kaspersky

Kaspersky Endpoint Security 14.1 voor Windows

© 2026 AO Kaspersky Lab

Inhoud

Kaspersky Endpoint Security voor Windows-help
- Nieuwigheden
- Opgeloste problemen
- Veelgestelde vragen

Kaspersky Endpoint Security voor Windows
- Modi van het programma: Standaard, EDR-agent, Light Agent
- 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 oude versie van het programma upgraden
  - Het programma upgraden zonder een herstart
  - SMU-update van het programma
- Programma verwijderen

Licentie van het programma activeren
- Over de Gebruiksrechtovereenkomst
- Over de licentie
- Over 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
- Een licentiesleutel verwijderen
- Licentie-informatie bekijken
- Een licentie aanschaffen
- Abonnement verlengen

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
- Het programma klaarmaken voor gebruik
- Beleid beheren
  - Een beleid aanmaken
  - Een beleid exporteren en importeren
  - Indicator voor beschermingsniveau
- 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
- 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

Malware-scan
- Computer scannen
- Verwisselbare schijven scannen wanneer ze op de computer zijn aangesloten
- Achtergrondscan
- Scannen vanuit contextmenu
- Programma Integriteitscontrole
- 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
- Programmamodules updaten
- Een proxyserver voor updates gebruiken
- Laatste update terugdraaien

Geavanceerde desinfectietechnologie
- Desinfectie van actieve dreigingen op werkstations
- Desinfectie van actieve dreigingen op servers

Onverwerkte dreigingen elimineren

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
Container Scan
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
BadUSB Attack Prevention
BadUSB Attack Prevention inschakelen en uitschakelen
Schermtoetsenbord gebruiken voor autorisatie van USB-apparaten
Autorisatie van barcodescanner
AMSI-bescherming
AMSI-bescherming inschakelen en uitschakelen
Scannen van bestanden optimaliseren door AMSI Protection
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
E-mails scannen in Thunderbird, MyOffice, R7-Office

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
- Network Threat Protection configureren op type

Firewall
- Firewall inschakelen en uitschakelen
- Type 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
  - Regels voor netwerkpakketten definiëren in XML
- 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

Exploit-preventie
- Exploit-preventie inschakelen en uitschakelen
- Bescherming voor systeemprocessen in geheugen

Gedragsdetectie

Anti-Cryptor
- Bescherming van gedeelde mappen tegen externe encryptie inschakelen en uitschakelen
- De blokkeringsperiode van een niet-vertrouwde computer configureren
- beschermd bereik bewerken
- Vertrouwde computers toevoegen voor externe gegevensencryptie
- Een lijst van uitzonderingen die niet moeten worden beschermd tegen externe encryptie exporteren en importeren:

Remediation Engine

Kaspersky Security Network
- Het gebruik van Kaspersky Security Network inschakelen en uitschakelen
- Beperkingen van Kaspersky Private Security Network
- 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
- Kaspersky-certificaat toevoegen aan het eigen certificatenarchief
- Versleutelde verbindingen uitsluiten van scannen

Gegevens wissen

- Computerbeheer
  - Webcontrole
    - Een toegangsregel voor webbronnen toevoegen
    - Filteren op adressen van webbronnen
    - Filteren op inhoud van webbronnen
    - Toegangsregels voor webbronnen testen
    - Regels voor webcontrole exporteren en importeren
    - Adressen van webbronnen van de webcontrole-regel exporteren en importeren
    - Activiteit van gebruikers op internet bewaken
    - Berichtsjablonen van Webcontrole bewerken
    - Maskers voor adressen van webbronnen bewerken
    - Webcontrole voor virtuele machines
    - Variabelen in de berichtsjablonen van Webcontrole
  - Apparaatcontrole
    - Over toegangsregels
    - Toegang tot apparaten beheren op type
    - Toegang tot apparaten beheren via de verbindingsbus
    - Differentiatie van gebruikersrechten voor apparaten
    - Toegang tot mobiele apparaten beheren
    - Toegang tot Bluetooth apparaten beheren
    - Afdrukbeheer
    - Controle van Wifi-verbindingen
    - 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 verbindingsregel wijzigen
      - De prioriteit van een verbindingsregel wijzigen
  - Adaptieve controle op afwijkingen
    - Adaptieve controle op afwijkingen trainen
    - 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
    - Monitoring van de bewerkingen van Adaptieve controle op afwijkingen

- Programmacontrole
  - Beperkingen van de functionaliteit van Programmacontrole
  - Informatie over geïnstalleerde programma's op computers van gebruikers ontvangen
  - De modus Geblokkeerde programma's inschakelen
  - Programmacontrole op basis van een basiscomputer
  - Regels van programmacontrole beheren
    - Een activeringsvoorwaarde voor een regel van Programmacontrole toevoegen
    - 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
    - De status van een regel van Programmacontrole wijzigen via Kaspersky Security Center
    - Regels voor programmabeheer exporteren en importeren
    - Gebeurtenissen die zich voordeden tijdens de werking van het onderdeel Programmacontrole weergeven
    - Een rapport over geblokkeerde programma's weergeven
  - Regels van Programmacontrole testen
    - In- en uitschakelen van testen van regels van Programmacontrole
    - Zo geeft u het rapport over geblokkeerde programma's in de testmodus weer
    - Gebeurtenissen die zich voordeden tijdens de geteste werking van het onderdeel Programmacontrole weergeven
  - Bewaking van programma-activiteit
  - Regels voor het maken van naammaskers voor bestanden of mappen
  - Berichtsjablonen van Programmacontrole bewerken
  - Variabelen in berichtsjablonen van Programmacontrole
  - 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
- Netwerkpoorten bewaken
  - Bewaking van alle netwerkpoorten inschakelen
  - Een lijst met bewaakte netwerkpoorten aanmaken
  - Een lijst met programma's aanmaken waarvoor alle netwerkpoorten worden gemonitord
  - Lijsten met bewaakte poorten exporteren en importeren
- Log Inspectie
  - Voorgedefinieerde regels configureren
  - Aangepaste regels toevoegen
- Systeemintegriteitscontrole
  - Over regels voor Systeemintegriteitscontrole
  - Realtime systeemintegriteitscontrole
  - On-demand systeemintegriteitscontrole
  - Regels voor Systeemintegriteitscontrole exporteren en importeren
  - Rapporten over Systeemintegriteitscontrole bekijken
  - Reset status van Systeemintegriteit
- Cloud Discovery

Vertrouwde zone
- Een scanuitzondering aanmaken
- Een uitzondering maken op type gedetecteerde objecten
- De lijst met vertrouwde programma's bewerken
- Een lokale vertrouwde zone creëren

- De vertrouwde zone importeren en exporteren
- Programma's met een vertrouwde digitale handtekening gebruiken
- Appendix. Vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's
  - SQL-server
  - Microsoft Exchange-server
  - System Center Configuration Manager
  - Citrix
  - VMware
- 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 van programmaservices tegen extern beheer
  - Ondersteuning voor programma's voor extern beheer
  - Wachtwoordbeveiliging
    - Wachtwoordbeveiliging inschakelen
    - Machtigingen aan individuele gebruikers of groepen verlenen
    - Een tijdelijk wachtwoord gebruiken om machtigingen te verlenen
    - Tijdelijk wachtwoord intrekken
    - Aandachtspunten bij machtigingen met wachtwoordbeveiliging
    - Het KL Admin-wachtwoord resetten
  - Administration Server verbindingsbeveiliging
- Gegevensencryptie
  - Beperkingen van de encryptiefunctionaliteit
  - 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:
    - Eenmalige 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 encryptiefunctionaliteit verhelpen
- De authenticatie-agent traceren
- 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
  - MDR en EDR Optimum-licenties
  - Compatibiliteit met oplossingen van derden EDR
  - Kaspersky Endpoint Agent
    - De [KES+KEA]-configuratie migreren naar [KES+built-in agent]
    - Migratie van beleid en taken voor Kaspersky Endpoint Agent
  - Endpoint Detection and Response Agent (EDR Agent)
    - EDR-agent installeren
    - EDR-agent integreren met MDR

- EDR-agent integreren met EDR (KATA)
- EDR-agent integreren met NDR (KATA)
- EDR-agent integreren met EDR Expert (on-premises)
- Compatibiliteit met toepassingen van derden EPP

Managed Detection and Response
- Integratie van de ingebouwde agent met MDR
- Migratiegids van KEA naar KES voor MDR

Endpoint Detection and Response
- Integratie van de ingebouwde agent met EDR Optimum / EDR Expert
- Scannen op indicatoren van compromis (standaard taak)
- Uitgebreide telemetrie voor IOC-scan
- Bestand in Quarantaine plaatsen
- Bestand ophalen
- Bestand verwijderen
- Proces starten
- Proces beëindigen
- Preventie van uitvoering
- Computer isoleren van netwerk
- Cloud Sandbox
- Migratiegids van KEA naar KES voor EDR Optimum

Kaspersky Sandbox
- Integratie van de ingebouwde agent met Kaspersky Sandbox
- Scannen op indicatoren van compromis (stand-alone taak)
- Migratiegids van KEA naar KES voor Kaspersky Sandbox

Kaspersky Anti Targeted Attack Platform
- Integratie van de ingebouwde agent met EDR / NDR (KATA)
- EDR (KATA)-telemetrie configureren
- EDR (KATA) telemetrie-uitzonderingen
  - Voorbeeld 1. Uitgesloten processen
  - Voorbeeld 2. Uitgesloten netwerkcommunicaties
  - Voorbeeld 3. Uitgesloten bestandsbewerkingen
  - Voorbeeld 4. Uitgesloten registerwijzigingen
- KATA Sandbox
  - Integratie van de ingebouwde agent met KATA Sandbox
  - Threat Response-acties configureren
- Migratiegids van KEA naar KES voor EDR (KATA)

Endpoint Detection and Response Expert (on-premises)
- Integratie van de ingebouwde agent met EDR Expert (on-premises)
- Instellingen voor EDR Expert (on-premises) telemetrie configureren
- Uitzonderingen voor telemetrie van EDR Expert (on-premises)
- EDR Expert (on-premises) gebeurtenisfilters exporteren en importeren
- Speciale overwegingen bij het gebruik van beleidsprofielen voor de configuratie van de integratie met EDR Expert (on-premises) en EDR (KATA)

Endpoint Detection and Response Expert (cloud)
- Integratie van de ingebouwde agent met EDR Expert (cloud)
- Instellingen voor EDR Expert (cloud) telemetrie configureren

Uitzonderingen voor telemetrie van EDR Expert (cloud)
EDR Expert (cloud) gebeurtenisfilters exporteren en importeren
Quarantaine beheren
De maximale quarantainegrootte configureren
Gegevens over in quarantaine geplaatste bestanden verzenden naar Kaspersky Security Center
Bestanden terugzetten vanuit quarantaine
EDR-acties bewaken
Kaspersky Unified Monitoring and Analysis Platform (KUMA)
Integratie van Kaspersky Endpoint Security met KUMA
Gebeurtenissen filteren die naar KUMA moeten worden verzonden
KUMA gebeurtenisfilters exporteren en importeren
Gids voor migratie van KSWS naar KES
Correspondentie van KSWS- en KES-onderdelen
Correspondentie van KSWS- en KES-instellingen
KSWS-componenten migreren
KSWS-taken en -beleid migreren
De vertrouwde KSWS-zone migreren
Migreren van KSWS-programma's Launch Control-regels
KES installeren in plaats van de KSWS.
De [KSWS+KEA]-configuratie migreren naar [KES+built-in agent]
Ervoor zorgen dat Kaspersky Security for Windows Server met succes is verwijderd
KES activeren met een KSWS-sleutel
Speciale overwegingen voor het migreren van zwaarbelaste servers
Het programma beheren op een server in Server Core-modus
Migreren van [KSWS+KEA] naar [KES+built-in agent]
Light Agent-modus om virtuele machines te beschermen
Speciale overwegingen voor de Light Agent-modus
Voorlopige configuratie van de virtuele machine
Compatibiliteit met Citrix App Layering-technologie
Compatibiliteit met Citrix Provisioning (Citrix Provisioning Services) technologie
Compatibiliteit met Omnissa App Volumes-technologie
Light Agent installeren
Light Agent verbinden met SVM
SVM-detectie
Het SVM-selectiealgoritme voor Light Agent configureren
Distribueren van de verbindingen van Light Agents naar SVM's (tags)
Bescherming van de verbinding tussen een Light Agent en SVM
Light Agent activeren
Migratiegids van KSVLA Light Agent naar KES Light Agent
KES Light Agent installeren in plaats van KSVLA Light Agent
Correspondentie van KSVLA Light Agent en KES Light Agent onderdelen
Taken en beleid van KSVLA Light Agent migreren
Migreren van [KSVLA Light Agent+KEA] configuratie naar [KES Light Agent+ingebouwde agent] configuratie
Het programma vanaf de opdrachtregel beheren
Setup. Het programma installeren
Setup /x. Programma verwijderen
msiexec /i. Het programma herstellen

AVP-opdrachten
- SCAN. Malware-scan
- UPDATE. Databases en softwaremodules van het programma bijwerken
- ROLLBACK. Laatste update terugdraaien
- TRACES. Tracing
- START. Een profiel starten
- 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. Het programma afsluiten
- EXITPOLICY. Beleid uitschakelen
- STARTPOLICY. Beleid inschakelen
- DISABLE. Bescherming uitschakelen
- SPYWARE. Detectie van spyware
- KSN. Schakelen tussen KSN / KPSN
- SERVERBINDINGDISABLE. Schakel de verbindingsbeveiliging van de server uit

KESCLI-opdrachten
- Scan. Malware-scan
- 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. Bepalen van de laatste updatedatum en -tijd van de databases
- EnableRTP. Beveiliging inschakelen
- GetRealTimeProtectionState. Status van bescherming bestanden
- GetEncryptionState. Schijfversleuteling status
- Version. De versie van het programma bepalen

Opdrachten voor beheer van Detection and Response
- SANDBOX. Sandbox beheren
- PREVENTION. Preventie van uitvoering beheren
- ISOLATION. Netwerkisolatie beheren
- RESTORE. Bestanden terugzetten vanuit quarantaine
- IOCSCAN. Scannen op IoC's (Indicators of Compromise)
- MDRLICENSE. MDR-activering
- EDRKATA. Integratie met EDR (KATA)
- KUMA. Integratie met KUMA
- YARA. YARA-scan starten
- TELEMETRIEFILTERS. Gebeurtenissen filteren die naar KUMA moeten worden verzonden

- Opdrachten voor beheer van Light Agent
  - KSVLAINFO. De Light Agent-modus bepalen
  - VIISINFO. Status van de Light Agent-verbinding met de Integrationserver
  - SVMINFO. Status van de Light Agent-verbinding met de Protection Server
- 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
- Gegevens van het besturingssysteem verkrijgen (Kaspersky Get System Info)

Beperkingen en waarschuwingen

Woordenlijst
- Actieve licentie
- Antivirusdatabases
- Archief
- Authenticatie-agent
- Beheergroep
- Beschermd bereik
- Cloud Discovery
- Database met phishing-webadressen
- Database met schadelijke webadressen
- Desinfectie
- Geïnfecteerd bestand
- Genormaliseerde notatie van het adres van een webbron
- Infecteerbaar bestand
- Integratieserver
- IOC
- IOC-bestand
- Kerberos-authenticatie
- Licentiecertificaat
- Light Agent
- Masker
- Netwerkagent
- OLE-object
- OpenIOC
- Portable bestandsbeheer
- Scanbereik
- SVM
- 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
  - Log Inspectie
  - Anti-Cryptor
  - Webcontrole
  - Apparaatcontrole
  - Programmacontrole
  - Adaptieve controle op afwijkingen
  - Systeemintegriteitscontrole
  - Endpoint Sensor
  - Sandbox
  - Managed Detection and Response
  - Endpoint Detection and Response
  - Endpoint Detection and Response Expert (on-premises)
  - Network Detection and Response (KATA)
  - Integratie met KUMA
  - 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
Kritiek
Functionele fout
Waarschuwing
Informatieve berichten.
Appendix 7. Ondersteunde bestandsextensies voor Preventie van uitvoering
Appendix 8. Ondersteunde scriptinterprekers voor Preventie van uitvoering
Appendix 9. IOC-scanbereik in het register (RegistryItem)
Appendix 10. IOC-bestandsvereisten
Appendix 11. API voor EDR Threat Response
Appendix 12. Gebruikersaccounts in regels voor programma-onderdelen
Juridische informatie
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
Kaspersky Endpoint Detection and Response Expert (on-premises)
Kaspersky Network Detection and Response (KATA)
Integratie met Kaspersky Unified Monitoring and Analysis Platform (KUMA)
Naleving van de wetgeving van de Europese Unie (AVG)
Kennisgevingen over handelsmerken
Informatie over code van derden

Kaspersky Endpoint Security voor Windows-help

Nieuwigheden

Update 14.1

Kaspersky Endpoint Security 14.1 voor Windows introduceert de volgende functies en verbeteringen:

1. Er is ondersteuning voor het besturingssysteem Windows Server 2025 toegevoegd.

2. De limiet voor het aantal filterregels voor telemetriegebeurtenissen voor Endpoint Detection and Response Expert (on-premises) en Kaspersky Endpoint Detection and Response Expert (cloud) is verhoogd. Kaspersky Endpoint Security ondersteunt nu in totaal 10.000 inclusieve en exclusieve filterregels.

3. U kunt nu taken zo instellen dat ze alleen op specifieke dagen van de week worden uitgevoerd, met een opgegeven interval in weken. Het schema is beschikbaar in Kaspersky Security Center 16.1 of nieuwer.

4. Voor de taak *Malware-scan*, kunt u nu een tijdsinterval opgeven waarin de taak wordt gepauzeerd, bijvoorbeeld om de impact op de computerprestaties tijdens periodes van verhoogde belasting te minimaliseren.

5. De prestaties van het subsysteem van de harde schijf op de beschermde computer zijn geoptimaliseerd door het aantal I/O-bewerkingen te verminderen.

6. Bij de ontwikkeling van deze versie van Kaspersky Endpoint Security hebben we de wijzigingen doorgevoerd die zijn opgenomen in de volgende privépatches: PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF14071, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF18057, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF20081, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF21062, PF21063, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF22059, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF23063, PF24005, PF24011, PF24013, PF24014, PF24017, PF24019, PF25013, PF25016, PF25019.

Update 14.0

Kaspersky Endpoint Security 14.0 voor Windows introduceert de volgende functies en verbeteringen:

1. Op ARM gebaseerde computers worden nu ondersteund. U kunt het programma installeren in de standaardmodus of in de EDR Agent-modus. Het programma heeft echter verscheidene beperkingen (zo wordt bijvoorbeeld van de gegevensversleutelingstechnologieën alleen BitLocker ondersteund).

2. Uitgebreide beleidsaudit wordt ondersteund in Kaspersky Security Center Web Console versie 15.0 of hoger. U kunt nu beleidsherzieningen bekijken en ze in een bestand opslaan. Een *revisie* is een set gewijzigde parameters die door de gebruiker is opgeslagen. Met revisies kunt u wijzigingen in beleidsparameters vergelijken en terugdraaien.

3. Nieuwe telemetriegebeurtenissen zijn nu beschikbaar voor gebruikers van Kaspersky Endpoint Detection and Response. Deze nieuwe gebeurtenissen verbeteren de detectie van dreigingen van Kaspersky EDR-oplossingen.

4. Bij de ontwikkeling van deze versie van Kaspersky Endpoint Security voor Windows hebben we de wijzigingen doorgevoerd die zijn opgenomen in de volgende privépatches: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF24005, PF24011.

Update 12.12

Kaspersky Endpoint Security 12.12 voor Windows introduceert de volgende functies en verbeteringen:

1. De bescherming van gedeelde mappen tegen externe versleuteling die vroeger deel uitmaakte van het onderdeel Gedragsdetectie is nu een apart onderdeel. Anti-Cryptor.

2. Ondersteuning voor het Kerberos-protocol is toegevoegd om het programma te verifiëren via a proxyserver voor internettoegang.

3. U kunt nu een bestandshash opgeven voor a vertrouwd programma en niet alleen een volledig pad.

4. Meer *IOC-scan* taakfuncties zijn beschikbaar voor gebruikers van Endpoint Detection and Response (EDR)-oplossingen. Retrospectieve IOC-scan functionaliteit is nu beschikbaar. *Retrospectieve IOC-scan* is een modus van de *IOC-scan* taak waarbij Kaspersky Endpoint Security gedurende een bepaalde periode scant op indicatoren van besmetting met behulp van gegevens. Deze modus is bedoeld voor het detecteren van indicatoren van besmetting in de gegevens van de netwerkactiviteit van de computer. Kaspersky Endpoint Security analyseert gegevens in logboeken van het besturingssysteem en browserlogboeken op de computer.

5. Gebruikers van Kaspersky Endpoint Detection and Response (EDR) kunnen de maximale grootte in quarantaine verwijderen. Dit kan nodig zijn voor YARA-scans omdat het programma een groot geheugendumpbestand kan opslaan. Nu kunt u al uw vrije schijfruimte gebruiken voor de quarantaine.

6. HTTPS-compressie wordt nu ondersteund voor het optimaliseren van de export van gebeurtenissen naar Kaspersky Unified Monitoring and Analysis Platform (KUMA). Dit helpt het uitgaand verkeer te verminderen.

7. Bij de ontwikkeling van deze versie van Kaspersky Endpoint Security voor Windows hebben we de wijzigingen doorgevoerd die zijn opgenomen in de volgende privépatches: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF24005, PF24011.

Update 12.11

Kaspersky Endpoint Security 12.11 voor Windows beschikt over de volgende functies en verbeteringen:

1. Het programma controleert de configuratie van de besturingsonderdelen voordat de instellingen worden opgeslagen. De controle is toegevoegd voor de onderdelen Programmacontrole, Apparaatcontrole en System Integrity Monitoring. Het programma toont nu een waarschuwing als de huidige instellingen van het besturingsonderdeel de belasting van de computer verhogen of systeemstoringen veroorzaken. Als u bijvoorbeeld in Programmacontrole de modus hebt geselecteerd die alle programma's blokkeert, behalve de toegestane, en u geen enkele toestaanssregel hebt toegevoegd, toont het programma een waarschuwing omdat een dergelijke configuratie systeemstoringen kan veroorzaken.

2. Ondersteuning toegevoegd voor het automatisch insturen van bestanden naar KATA Sandbox voor review. *KATA Sandbox* is een onderdeel van Kaspersky Anti Targeted Attack Platform dat bestanden uitvoert op virtuele afbeeldingen van besturingssystemen. Sandbox analyseert het gedrag van objecten om schadelijke activiteit en activiteit kenmerkend voor doelgerichte aanvallen op de IT-infrastructuur van het bedrijf te detecteren. Sandbox analyseert en scant objecten op speciale servers met geïmplementeerde virtuele kopieën van Microsoft Windows-besturingssystemen (Sandbox-servers). Om KATA Sandbox in de automatische modus te laten werken, moet Kaspersky Anti Targeted Attack Platform 8.0 of hoger zijn geïmplementeerd.

3. Versturing van EDR-telemetrie geoptimaliseerd. Nu kunt u de maximale pakketlengte opgeven.

4. Verbeterde diagnose van verbinding naar Kaspersky Security Network. Uitgebreide details over verbindingsfouten voor Kaspersky Security Network om mogelijke problemen op te lossen.

5. Ondersteuning toegevoegd voor de configuratie van gebeurtenistlijsten die naar Kaspersky Unified Monitoring and Analysis Platform (KUMA) worden verzonden. Naast de vooraf gedefinieerde gebeurtenislijsten in KUMA kunt u nu handmatig gebeurtenissen toevoegen aan telemetrie of gebeurtenissen uitsluiten op basis van hun ID in het Windows Gebeurtenislogboek.

6. Beleidsinterface in Webconsole bijgewerkt. De lay-out van beleidsgedeeltes is gewijzigd voor snellere toegang tot essentiële functies.

7. Ondersteuning voor Windows 11 25H2.

8. Bij de ontwikkeling van deze versie van Kaspersky Endpoint Security voor Windows hebben we de wijzigingen doorgevoerd die zijn opgenomen in de volgende privépatches: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF22004, PF22008, PF22014.

Update 12.10

Kaspersky Endpoint Security 12.10 voor Windows beschikt over de volgende functies en verbeteringen:

1. Voor het onderdeel BadUSB Attack Prevention is de optie toegevoegd om barcodescanners te autoriseren door een streepjescode van het scherm te lezen. U hoeft nu geen code met het schermtoetsenbord in te voeren om barcodescanners te autoriseren.

2. De volgende functies en verbeteringen zijn beschikbaar voor gebruikers van Endpoint Detection and Response (EDR)-oplossingen van Kaspersky:

   - U kunt nu de netwerkisolatie van de computer beheren in de details van de waarschuwing. Bovendien kunt u in de details van de waarschuwing de periode opgeven voor de netwerkisolatie van de computer en uitzonderingen toevoegen.

   - Details van de waatschuwing invullen met nieuwe gegevens. De details van de waarschuwing bevatten nu meer informatie over de dreiging, inclusief hoe het programma reageert op EDR-dreigingen.

   - De verwerking van IOC-bestanden is verbeterd. U kunt nu de inhoud van IOC-bestanden bekijken en bewerken in de Webconsole van Kaspersky Security Center interface. Na het laden van een IOC-bestand toont het programma een rapport over het programma IOC-termen.

   - Verbeterde reactie op gedetecteerde IOC's. Nu kunt u bestanden die zijn gedetecteerd door de *IOC-scan*taak rechtstreeks in IOC-detectie resulteert in taakeigenschappen. U kunt ook computers isoleren van het netwerk in de taakeigenschappen.

   - Nu kunt u IOC-bestanden rechtstreeks aanmaken in de eigenschappen van de *IOC Scan* taak op basis van lijsten met bestandshashes, IP-adressen of DNS-namen die in een TXT-bestand zijn gegenereerd.

   - Uitgebreid scanbereik voor de *IOC-scan*taak. U kunt nu een bereik voor de IOC-scan van het register definiëren (**Windows-register – Registeritem**). In eerdere versies van het programma kon u alleen een vooraf gedefinieerd IOC-scanbereik in het register gebruiken.

3. Nieuwe machtiging voor wachtwoordbeveiliging toegevoegd, *Instellingen exporteren*. Standaard kan alleen de KLAdmin-gebruiker een configuratiebestand maken met de instellingen van Kaspersky Endpoint Security in de programma-interface. Als u andere gebruikers toegang wilt verlenen, moet u ze de overeenkomstige machtiging geven.

4. Bij de ontwikkeling van deze versie van Kaspersky Endpoint Security voor Windows hebben we de wijzigingen doorgevoerd die zijn opgenomen in de volgende privépatches: PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF13120, PF13123, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF15062, PF16052, PF16053, PF16055, PF16056, PF16057, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF21007.

Update 12.9

Kaspersky Endpoint Security 12.9 voor Windows beschikt over de volgende functies en verbeteringen:

1. De nieuwe functionaliteit voor *tijdelijke wachtwoorden beheren* is toegevoegd. Met een tijdelijk wachtwoord kunt u een aparte computer toegang verlenen tot Kaspersky Endpoint Security met Wachtwoordbescherming ingeschakeld. Met het beheer van tijdelijke wachtwoorden kunt u de geschiedenis van het wachtwoord opslaan (tot 30 dagen), de status van het tijdelijke wachtwoord bewaken (*Actief*, *Verlopen*, *Ingetrokken*) en trek tijdelijke wachtwoorden in.

2. De optie om de verbinding met webbronnen te beëindigen die verboden zijn door de regels van Webcontrole onmiddellijk nadat het beleid is toegepast, is toegevoegd. In eerdere versies van het programma beperkte Webcontrole alleen nieuwe verbindingen tot verboden webbronnen.

3. Voor gebruikers van Kaspersky Anti Targeted Attack Platform is een optie toegevoegd om de YARA-controle lokaal op de computer uit te voeren. Hiervoor moet u een bestand met YARA-regels downloaden en de opdracht in CMD uitvoeren.

4. Het gedrag van het programma opgelost wanneer BitLocker is ingeschakeld op computers waarop stations al worden beschermd door BitLocker met hulpprogramma's van derden. Kaspersky Endpoint Security start de herstelprocedure om de herstelsleutel naar Kaspersky Security Center te versturen. Het BitLocker-beheer wordt dus overgedragen naar de console van Kaspersky Security Center.

5. Een nieuwe sectie, **Response history**, is beschikbaar voor gebruikers van Detection and Response-oplossingen van Kaspersky. Deze sectie bevat informatie over de acties die op de computer worden uitgevoerd als reactie op dreigingen. Dergelijke acties omvatten bijvoorbeeld het uitvoeren van de taak *Proces beëindigen* of het isoleren van de computer van het netwerk. Reactiegeschiedenis is alleen beschikbaar voor gebruikers van de volgende Kaspersky-oplossingen: MDR, EDR, KATA.

6. Voor gebruikers van Kaspersky Unified Monitoring and Analysis Platform geldt dat de ondersteuning voor EDR-acties voor de respons op dreigingen is nu beschikbaar. Bij het reageren op dreigingen voert KUMA scripts uit die overeenkomstige EDR-taken aanmaken. Om EDR-taken uit te voeren, moet u een antwoordregel voor het aangepaste script in de KUMA-console maken en gebeurtenissen selecteren.

7. Bij de ontwikkeling van deze versie van Kaspersky Endpoint Security voor Windows hebben we de wijzigingen doorgevoerd die zijn opgenomen in de volgende privépatches: PF10360, PF10362, PF10363, PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF16052, PF16053, PF16055, PF16056, PF17027, PF17029, PF17039, PF17041, PF17043, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF20011, PF20016, PF20017, PF20020, PF20021.

Update 12.8

Kaspersky Endpoint Security 12.8 voor Windows beschikt over de volgende functies en verbeteringen:

1. Het programma ondersteunt nu de Light Agent-modus voor het beschermen van virtuele omgevingen. Nu kunt u het programma implementeren als Light Agent als onderdeel van de Kaspersky Security for Virtualization Light Agent 6.2 oplossing.

2. Onderschepping van bestandsbewerkingen in Docker-containers op servers wordt nu ondersteund. Een *container* is een geïsoleerde omgeving waarin een programma kan draaien zonder directe interactie met het besturingssysteem. Kaspersky Endpoint Security scant de bestanden in containers waartoe de gebruiker toegang krijgt. Wanneer een bedreiging wordt gedetecteerd, blokkeert het programma deze kwaadaardige activiteit en probeert het bestand in de container te desinfecteren. Als het bestand niet kan worden gedesinfecteerd, stopt het programma de container.

3. Nu kunt u een beschermd bereik definiëren voor de bescherming van gedeelde mappen tegen externe encryptie (onderdeel Gedragsdetectie). Nu kunt u gedeelde mappen opgeven die het programma moet controleren op bestandsactiviteit. U kunt ook bestanden uitsluiten van het Beschermd bereik. In eerdere versies van het programma controleerde het onderdeel Gedragsdetectie alle gedeelde mappen op bestandsactiviteit.

4. Nu kunt u verschillende sets onderdelen configureren voor verschillende soorten besturingssystemen in het installatiepakket. Dat wil zeggen dat u het programma op werkstations en servers kunt implementeren met hetzelfde installatiepakket. Onderdelen die niet beschikbaar zijn voor een bepaald type besturingssysteem worden automatisch uitgesloten in de eigenschappen van het installatiepakket.

5. De optie om vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's te selecteren is toegevoegd. Met vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's kunt u snel de vertrouwde zone voor het programma configureren in een virtuele omgeving (Citrix, VMware). Dergelijke uitzonderingen omvatten bijvoorbeeld VHD- en VHDX-bestanden van virtuele machines. Uitsluitingen kunnen worden toegevoegd bij het maken van een programma-installatiepakket, het maken van een beleid of bij de installatie van Kaspersky Endpoint Security.

6. De EDR-telemetrie omvat nu gebeurtenissen voor bewerkingen met via USB aangesloten apparaten. U kunt deze gebeurtenissen ook toevoegen aan uitzonderingen van EDR-telemetrie.

7. De optie om netwerkverbindingen via het verouderde TLS 1.0-protocol blokkeren is toegevoegd. TLS 1.0 heeft een laag beveiligingsniveau, dus het wordt aanbevolen om dit protocol uit te schakelen en nieuwere versies van TLS 1.2 of TLS 1.3 te gebruiken. Kaspersky Endpoint Security blokkeert standaard TLS 1.0-verbindingen. Na het updaten van de programmaversie kan de werking van services van derden die gebruikmaken van het TLS 1.0-protocol mislukken. Om problemen met de werking van services van derden te voorkomen, kunt u: gebruik van het TLS 1.0-protocol in groepsbeleid toestaan voordat u de programmaversie update.

8. Bij de ontwikkeling van deze versie van Kaspersky Endpoint Security voor Windows hebben we de wijzigingen doorgevoerd die zijn opgenomen in de volgende privépatches: PF10053, PF10054, PF10360, PF10362, PF10363, PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF16052, PF16053, PF16055, PF16056, PF17027, PF17029, PF17039, PF17041, PF17043, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF19003, PF19016, PF19018.

Update 12.7

Kaspersky Endpoint Security 12.7 voor Windows beschikt over de volgende functies en verbeteringen:

1. Nu kunt u het gebruik van CPU-bronnen beperken voor: *Malware-scan* taken. Om dit te doen, in de programma-instellingen, specificeer het maximale CPU-belastingspercentage voor alle kernen die kunnen worden gebruikt tijdens het scannen van de computer.

2. Nu kunt u handmatig bestanden verzenden om te scannen in KATA Sandbox. *KATA Sandbox* is een onderdeel van Kaspersky Anti Targeted Attack Platform dat bestanden uitvoert op virtuele afbeeldingen van besturingssystemen. Sandbox analyseert het gedrag van objecten om schadelijke activiteit en activiteit kenmerkend voor doelgerichte aanvallen op de IT-infrastructuur van het bedrijf te detecteren. Sandbox analyseert en scant objecten op speciale servers met geïmplementeerde virtuele kopieën van Microsoft Windows-besturingssystemen (Sandbox-servers). Om een bestand voor scannen naar KATA Sandbox te sturen, selecteer de relevante opdracht in het contextmenu van het bestand.

3. Nu kunt u integratie instellen met de oplossing die het bedrijfsnetwerk beschermt, *Kaspersky Network Detection and Response*. Kaspersky Network Detection and Response (NDR) maakt deel uit van Kaspersky Anti Targeted Attack Platform. U kunt de interactie met NDR zowel in de standaardmodus als in de EDR Agent-modus configureren.

4. Ondersteuning voor Microsoft Office Outlook e-mailprogramma versie 2021 is toegevoegd aan de Mail Threat Protection-extensie. Met de extensie kunnen berichten worden gescand op het niveau van een e-mailclient in plaats van op protocolniveau. Naast berichten kunt u met de extensie ook objecten scannen die via de MAPI-interface zijn ontvangen vanuit Microsoft Exchange-opslagplaatsen (bijvoorbeeld objecten in de kalender). Dit scannen vindt plaats in de e-mailprogramma's.

5. Bij het ontwikkelen van deze versie van Kaspersky Endpoint Security for Windows hebben we de wijzigingen opgenomen in de volgende privépatches: PF10049, PF10355, PF12114, PF13109, PF14056, PF15038, PF15045, PF16037, PF16042, PF16047, PF17014, PF17018, PF17021, PF17024, PF18006, PF18007.

Update 12.6

Kaspersky Endpoint Security 12.6 voor Windows beschikt over de volgende functies en verbeteringen:

1. De functionaliteit voor integratie met Kaspersky SIEM-oplossing – *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* – is toegevoegd. Het is nu mogelijk om gebeurtenissen vanuit Windows-gebeurtenislogboeken naar de KUMA-verzamelaar te sturen. Hierdoor kan KUMA Windows-gebeurtenissen ontvangen (een beperkte set EventID's wordt ondersteund) van alle computers waarop Kaspersky Endpoint Security is geïnstalleerd, zonder KUMA-agents op deze computers te installeren.

2. Er is een nieuw *Systeemintegriteitscontrole* toegevoegd ter vervanging van het onderdeel Bestandsintegriteitsmonitor. Het onderdeel Systeemintegriteitscontrole omvat alle functionaliteit van Bestandsintegriteitsmonitor en maakt het bovendien mogelijk om registerwijzigingen en de aansluiting van externe apparaten te monitoren. Het onderdeel Systeemintegriteitscontrole bewaakt veranderingen in het besturingssysteem die kunnen wijzen op inbreuken op de beveiliging van de computer. Wanneer dergelijke wijzigingen worden gedetecteerd, genereert Kaspersky Endpoint Security overeenkomstige gebeurtenissen en waarschuwt de beheerder. Bestandsintegriteitsmonitor maakt geen deel meer uit van het programma. De instellingen van Bestandsintegriteitsmonitor migreren automatisch naar Systeemintegriteitscontrole wanneer u het programma bijwerkt. Om een correcte werking van Systeemintegriteitscontrole te garanderen, moeten zowel het Kaspersky Endpoint Security-programma als de beheerplug-in worden bijgewerkt naar versie 12.6.

3. De status van de geïnstalleerde ingebouwde EDR-agent (KATA) is toegevoegd aan de computereigenschappen in de Kaspersky Security Center-console. Als u nu een ingebouwde EDR-agent (KATA) hebt geïnstalleerd, **Endpoint Sensor status** kolom geeft de huidige status van het onderdeel weer (bijv. *Uitvoeren*, *Gestopt*, *Niet ondersteund door licentie*, enz.).

4. De optie om vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's te selecteren is toegevoegd. Vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's helpen bij het snel configureren van de vertrouwde zone bij gebruik van het programma op SQL-servers, Microsoft Exchange-servers en System Center Configuration Manager. Dergelijke uitzonderingen omvatten bijvoorbeeld MDF- en LDF-databasebestanden. Uitzonderingen kunnen worden toegevoegd wanneer u een nieuw beleid maakt, een bestaand beleid wijzigt of wanneer u Kaspersky Endpoint Security installeert.

5. De weergave van waarschuwingsdetails voor Kaspersky Endpoint Detection and Response Optimum is verplaatst van de Kaspersky Endpoint Security beheerplug-in naar een afzonderlijke Kaspersky Endpoint Detection and Response beheerplug-in. De beheerplug-in van EDR is een enkele plug-in voor het werken met agents op Windows-, Mac- en Linux-besturingssystemen. Als u nu met EDR Optimum werkt, hebt u de beheerplug-in van Kaspersky Endpoint Security nodig om responstaken op bedreigingen te creëren en de beheerplug-in van EDR om waarschuwingsdetails te bekijken.

6. Ondersteuning voor Windows 11 24H2.

7. Bij het ontwikkelen van deze versie van Kaspersky Endpoint Security voor Windows hebben we de wijzigingen opgenomen in de volgende privépatches: pf10048, pf10353, pf12106, pf12107, pf12108, pf13090, pf13100, pf15031, pf15034, pf15036, pf16021, pf16023, pf16029, pf17002.

Update 12.5

Kaspersky Endpoint Security 12.5 voor Windows beschikt over de volgende functies en verbeteringen:

1. De optie om telemetrie uitzonderingen te configureren is toegevoegd. *Telemetrie* is een lijst met gebeurtenissen die hebben plaatsgevonden op de beveiligde computer. Telemetriegegevens worden gebruikt door Kaspersky Anti Targeted Attack Platform (EDR) om de IT-infrastructuur van een organisatie te controleren en beschermen. Configuratie van telemetrie-uitzonderingen helpen om de computerprestaties verbeteren en de gegevensoverdracht naar de Telemetrieverzamelingsserver optimaliseren.

2. De interface van de vertrouwde zone van het programma is verbeterd. Kaspersky Endpoint Security verbergt nu vertrouwde zone objecten voor de gebruiker als de beheerder het toevoegen van hun eigen (lokale) scanuitzonderingen en vertrouwde programma's voor de gebruiker heeft verboden. Dit voorkomt onbevoegde toegang tot de vertrouwde zone door een indringer, wat de beveiliging van de computer verbeterd.

3. De optie om verkeer te scannen voor MyOffice Mail en R7-Office Organizer e-mailprogramma's is toegevoegd. Het onderdeel Mail Threat Protection scant nu niet alleen bijlages van berichten bij downloaden, maar ook maar ook verzonden en ontvangen berichten.

4. Er is een nieuwe categorie van webbronnen *Generatieve AI-tools* toegevoegd. U kunt toegang tot websites instellen vanuit de nieuwe categorie Webcontrole.

5. Nu kunt u de locatie van regels voor netwerkpakketten selecteren in de Firewall-lijst. De locatie van regels voor een netwerkpakket in de lijst bepaalt de prioriteit ervan. In eerdere versies van het programma kon een nieuwe regel alleen aan het einde van de lijst worden toegevoegd, waarna u de regel handmatig door de lijst moest verplaatsen om er prioriteit aan te geven. Wanneer u nu een regel toevoegt, kunt u kiezen of de regel aan het begin, aan het einde van de lijst of naast de geselecteerde regel moet worden geplaatst.

6. In de regels van Kaspersky Endpoint Security onderdelen, kun je nu niet alleen gebruikers selecteren uit je Active Directory, maar ook van de lijst van gebruikers in Kaspersky Security Center. U kunt ook handmatig lokale gebruikersaccountgegevens invoeren. Deze mogelijkheid is toegevoegd voor de regels van de volgende onderdelen: Programmacontrole, Apparaatcontrole, Webcontrole, Adaptieve controle op afwijkingen en Log Inspectie.

7. Het detectierapport voor netwerkaanvallen bevat nu een kolom met het MAC-adres van de aanvallende computer (het onderdeel Network Threat Protection). Nu kunt u naast het IP-adres ook het MAC-adres van de aanvallende computer in het rapport zien. Dit is nuttig bij het onderzoeken van incidenten. Rapporten met het MAC-adres van de aanvallende computer zullen ook beschikbaar zijn in de Kaspersky Security Center Linux-console versie 15.1 en nieuwer.

8. Het niveau van de computerbeveiligingseisen is verhoogd. Het beschermingsniveau hoog vereist nu het inschakelen van Bescherming van programmaservices tegen extern beheer. Controleer de indicator voor het beveiligingsniveau in het bovenste gedeelte van het beleidsvenster. Als je een gemiddeld of laag beveiligingsniveau hebt, kun je nu Bescherming van programmaservices tegen extern beheer inschakelen in het aanbevelingsvenster van de beveiligingsniveau-indicator.

9. Ondersteuning voor nieuwe gebeurtenissen van objectdetectie wanneer het programma wordt uitgevoerd in de Endpoint Detection and Response Agent (EDR Agent)-configuratie is toegevoegd. Deze gebeurtenissen werden al ondersteund in de configuratie [KES+ingebouwde agent].

10. Bij het ontwikkelen van deze versie van Kaspersky Endpoint Security voor Windows hebben we de wijzigingen opgenomen in de volgende privépatches: pf9640, pf9830, pf9831, pf10047, pf10351, pf12102, pf12105, pf13084, pf13089, pf14040, pf14047, pf15026, pf15028, pf16013.

Update 12.4

Kaspersky Endpoint Security 12.4 voor Windows beschikt over de volgende functies en verbeteringen:

1. Nieuwe functionaliteit toegevoegd om de verbinding van de computer met Kaspersky Security Center te beschermen. Met de nieuwe *Administration Server verbindingsbescherming* taak kunt u een wachtwoord instellen voor verbinding met een vertrouwde server. Dit betekent dat het zonder dit wachtwoord niet mogelijk is om de computer opnieuw te verbinden en opdrachten uit te voeren vanaf een andere server.

2. Voor het onderdeel Wachtwoordbeveiliging is de mogelijkheid toegevoegd om gebruikers handmatig te selecteren en niet alleen uit Active Directory. Dat wil zeggen dat u handmatig een gebruikersnaam en wachtwoord kunt opgeven en toegangsrechten tot Kaspersky Endpoint Security voor dit account kunt toewijzen. Op deze manier hoeft u uw KLAdmin-wachtwoord niet met andere gebruikers te delen of nieuwe Active Directory-accounts aan te maken om de toegang tot het programma te controleren.

3. Ondersteuning voor Windows 11 23H2.

Update 12.3

Kaspersky Endpoint Security 12.3 voor Windows beschikt over de volgende functies en verbeteringen:

1. Nu kunt u het programma installeren in de Endpoint Detection and Response Agent-configuratie. Met deze configuratie kan het programma worden geïnstalleerd met een reeks onderdelen die vereist zijn voor Detection and Response-oplossingen van Kaspersky: Kaspersky Managed Detection and Response en Kaspersky Anti Targeted Attack Platform (EDR). U kunt het programma in deze configuratie installeren naast oplossingen van derden (bijvoorbeeld Dr.Web, Dallas Lock, ESET). Hierdoor kunt u hulpmiddelen voor infrastructuurbeveiliging van derden gebruiken naast Detection and Response van Kaspersky.

2. De werking van Kaspersky Endpoint Security met Bluetooth apparaten is verbeterd. Nu kunt u uitzonderingen configureren en de toegang beperken tot alle Bluetooth apparaten, behalve invoerapparaten (draadloze toetsenborden, muizen, enz.).

3. De werking van het Programmacontrole-onderdeel met de database met uitvoerbare bestanden is geoptimaliseerd. Kaspersky Endpoint Security verwijdert nu automatisch bestandsinformatie uit de database als het bestand van de computer wordt verwijderd. Hierdoor kan de database up-to-date worden gehouden en kunnen bronnen van Kaspersky Security Center worden bespaard.

4. Het niveau van de computerbeveiligingseisen is verhoogd. Het hoge beveiligingsniveau vereist nu inschakelen van wachtwoordbeveiliging. Controleer de indicator voor het beveiligingsniveau in het bovenste gedeelte van het beleidsvenster. Als je een gemiddeld of laag beschermingsniveau hebt, kunt je wachtwoordbeveiliging inschakelen in het aanbevelingsvenster van de beveiligingsniveau-indicator.

5. Ondersteuning voor het HTTPS-protocol is toegevoegd om het programma te laten werken met Kaspersky Security Network. Schakel HTTPS-gebruik in bij de eigenschappen van Administration Server in de KSN proxyserver instellingen.

Update 12.2

Kaspersky Endpoint Security 12.2 voor Windows beschikt over de volgende functies en verbeteringen:

1. WPA3-protocolondersteuning is toegevoegd om verbindingen met wifinetwerken te beheren (apparaatcontrole). Nu kunt u het WPA3-protocol selecteren in de vertrouwde wifi-netwerkinstellingen en de verbinding met het netwerk te weigeren met behulp van een minder goed beveiligd protocol.

2. U kunt nu een protocol en poorten kiezen voor Network Threat Protection-uitzonderingen. Naast het specificeren van IP-adressen van vertrouwde apparaten, kunt u nu ook een poort en protocol selecteren. Hiermee kunt u individuele gegevensstromen uitsluiten en netwerkaanvallen van vertrouwde IP-adressen voorkomen.

3. Andere volgorde van updatebronnen voor de lokale taak *Update van databases en programmamodules* als een beleid op de computer wordt toegepast. De Kaspersky Security Center-server wordt nu standaard gebruikt als de eerste updatebron in plaats van de Kaspersky-servers. Dit helpt verkeer te besparen wanneer de gebruiker de lokale taak *Update van databases en programmamodules* uitvoert.

Update 12.1

Kaspersky Endpoint Security 12.1 voor Windows beschikt over de volgende functies en verbeteringen:

1. Een ingebouwde agent voor de Kaspersky Anti Targeted Attack Platform-oplossing is toegevoegd. U hebt Kaspersky Endpoint Agent niet langer nodig om EDR (KATA) te gebruiken. Alle functies van Kaspersky Endpoint Agent worden uitgevoerd door Kaspersky Endpoint Security. Om Kaspersky Endpoint Agent-beleid te migreren, gebruikt u de Migratiewizard. Na het bijwerken van het programma schakelt Kaspersky Endpoint Security over op het gebruik van de ingebouwde agent en wordt Kaspersky Endpoint Agent verwijderd. Kaspersky Endpoint Agent is toegevoegd aan de lijst met incompatibele software. Kaspersky Endpoint Security heeft ingebouwde agenten voor alle Detection and Response-oplossingen, daarom is het niet langer nodig om Kaspersky Endpoint Agent te installeren om met deze oplossingen te integreren.

2. Azure WVD-compatibiliteitsmodus wordt nu ondersteund. Deze functie garandeert een correcte weergave van de status van de Azure virtuele machine in de console van Kaspersky Anti Targeted Attack Platform. Met de Azure WVD-compatibiliteitsmodus kunt u een permanente unieke sensor-id toewijzen aan deze virtuele machines.

3. Nu kunt u gebruikerstoegang tot mobiele apparaten configureren in iTunes of vergelijkbare applicaties. Zo kunt u bijvoorbeeld toestaan dat het mobiele apparaat alleen in iTunes wordt gebruikt en het gebruik van het mobiele apparaat als een verwijderbare schijf blokkeren. Het programma ondersteunt deze regels ook voor het programma Android Debug Bridge (ADB).

4. Kaspersky Security Center versie 11 wordt niet meer ondersteund. Upgrade Kaspersky Security Center naar de nieuwste versie.

Opgeloste problemen

De onderstaande tabel toont alle problemen die zijn ontdekt in eerdere versies van Kaspersky Endpoint Security en opgelost in de huidige versie.

Lijst met opgeloste problemen in versie 14.1

Probleem-ID	Beschrijving van het probleem
10140523	Het inschakelen van Native NVMe in Windows 11 kan leiden tot onstabiel gedrag van programma's.
9340076	Op een apparaat waarop het programma is geïnstalleerd en het onderdeel Bestandsversleuteling is ingeschakeld, vernieuwt Windows Verkenner de inhoud van een netwerkmap niet automatisch nadat deze is gewijzigd vanaf een ander apparaat.
9722863	Het rapport Apparaatcontrole bevat geen gebeurtenis voor het loskoppelen van USB-token.
10006481	Na het toepassen van een regel die inkomend verkeer weigert, kunnen actieve TCP-verbindingen met externe services voortijdig worden beëindigd vanwege een onjuiste berekening van de time-out.
10140912	Het programma detecteert het BHT1100B PDA-apparaat niet.

Probleem-ID	Beschrijving van het probleem
10157563	Folder Redirection werkt mogelijk niet na een herstart op VDI -werkstations.
10158494	Apparaatbeheer registreert meerdere gebeurtenissen voor het verbinden en verbreken van een verwisselbaar apparaat zonder dat het fysiek opnieuw wordt verbonden.

Veelgestelde vragen

GENERAL

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?

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 malware-scan 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?

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?

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.

Het programma is niet bedoeld voor gebruik in technologische processen waarbij geautomatiseerde controlesystemen betrokken zijn. Om apparaten in dergelijke systemen te beschermen, wordt het aanbevolen om Kaspersky Industrial CyberSecurity for Nodes programma te gebruiken.

Technologieën voor detectie van dreigingen



Machine learning

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).



Cloud- analyse

Kaspersky Endpoint Security krijgt van het Kaspersky Security Network gegevens over dreigingen. *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.



Geavanceerde analyse

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.



Gedrags- analyse

Kaspersky Endpoint Security analyseert de activiteit van een object in realtime.



Automatische analyse

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.



Sandbox

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 Kaspersky Sandbox-oplossing gebruikt.



Cloud Sandbox

Kaspersky Endpoint Security scant objecten in een geïsoleerde omgeving aangeboden door Kaspersky. Cloud Sandbox-technologie is permanent ingeschakeld en is beschikbaar voor alle gebruikers van Kaspersky Security Network, ongeacht het type licentie dat ze gebruiken. Als u Endpoint Detection and Response Optimum-oplossingen al heeft geïmplementeerd, kunt u een aparte teller inschakelen voor door Cloud Sandbox gedetecteerde dreigingen.

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
Essential Threat Protection 	**File Threat Protection** Met het onderdeel File Threat Protection kunt u infectie van het bestandssysteem van een computer voorkomen. Het onderdeel File Threat Protection bevindt zich standaard permanent in het RAM van de computer en scant alle bestanden die worden geopend, opgeslagen en uitgevoerd in realtime. Dit onderdeel scant bestanden op alle computerschijven, inclusief aangesloten schijven. Het onderdeel biedt computerbescherming met behulp van antivirusdatabases, de Kaspersky Security Network-cloudservice en heuristische analyse. **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. **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 • Windows Mail • MyOffice Mail • R7-Office Organizer Om verkeer in Mozilla Thunderbird, MyOffice Mail en R7-Office Organizer e-mailprogramma's te scannen, moet u het Kaspersky-certificaat toevoegen aan het certificaatarchief en het eigen certificaatarchief selecteren. 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 Mail Threat Protection-extensie ondersteunt de 32-bit en 64-bit versies van Outlook 2010, 2013, 2016, 2019, 2021, 2024 en 365. Op Arm-computers ondersteunt de Mail Threat Protection-extensie de 32-bit en 64-bit versies van Outlook 2016, Outlook 2021, Outlook 2024 en Outlook 365 voor Arm64. **Network Threat Protection** Het onderdeel *Network Threat Protection* (ook wel Intrusion Detection System (IDS) genoemd) controleert inkomend netwerkverkeer op activiteiten die kenmerkend zijn voor netwerkaanvallen. Wanneer het programma 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 het programma 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** Het onderdeel Firewall blokkeert ongeautoriseerde verbindingen met een 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.

Gedeelte	Onderdeel
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 het Kaspersky Security Network, voorzien de KSN-services Kaspersky Endpoint Security van informatie over de reputatie van gescande webadressen, evenals informatie over de categorie en reputatie van gescande bestanden. **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 is gebaseerd op de definities van gedragspatronen en levert een proactieve bescherming voor de computer. Het onderdeel Gedragsdetectie bewaakt bovendien netwerkpoorten op processen van programma's die de beveiliging van de computer kunnen bedreigen. Het programma verkrijgt informatie over dergelijke processen met antivirusdatabases. **Anti-Cryptor** Het onderdeel Anti-Cryptor 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. **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. Het onderdeel Exploit-preventie bewaakt bovendien netwerkpoorten op processen van programma's die de beveiliging van de computer kunnen bedreigen. Het programma verkrijgt informatie over dergelijke processen met antivirusdatabases. **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 het onderdeel Remediation Engine kan Kaspersky Endpoint Security acties van malware in het besturingssysteem terugdraaien.

Gedeelte	Onderdeel
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 een computer (bijvoorbeeld harde schijven, camera's of wifi-apparaten). Met dit onderdeel kunt u de computer beschermen tegen infecties wanneer zulke apparaten worden aangesloten, en verlies van gegevens of gegevenslekken voorkomen. **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. **Log Inspectie** Log Inspectie bewaakt de integriteit van de beschermde omgeving op basis van de inspectiere van het Windows-gebeurtenislogboek. Wanneer het programma tekenen van atypisch gedrag in het systeem detecteert, informeert het de beheerder, omdat dit gedrag kan wijzen op een poging tot cyberaanval. **Systeemintegriteitscontrole** Het onderdeel Systeemintegriteitscontrole bewaakt veranderingen in het besturingssysteem die kunnen wijzen op inbreuken op de beveiliging van de computer. Wanneer dergelijke wijzigingen worden gedetecteerd, genereert Kaspersky Endpoint Security overeenkomstige gebeurtenissen en waarschuwt de beheerder.
Taken 	**Malware-scan** Kaspersky Endpoint Security scant de computer op virussen en andere bedreigingen. De Malwarescan helpt malware te vermijden die niet is gedetecteerd door beschermingsonderdelen, bijvoorbeeld wegens een laag ingesteld beveiligingsniveau. **Update van databases en programmamodules** 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. **Programma 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. **Encryptie van verwisselbare schijven** Met dit onderdeel kunt u gegevens op verwisselbare schijven beschermen. U kunt Full Disk Encryption (FDE) of File Level Encryption (FLE) gebruiken.

Gedeelte	Onderdeel
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* 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. **Endpoint Detection and Response Expert (on-premises)** en **Network Detection and Response (KATA)** Ingebouwde agents voor het beheer van het Endpoint Detection and Response en Network Detection and Response-onderdelen dat deel uitmaken 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 drie functionele eenheden: • Kaspersky Anti Targeted Attack Platform (*KATA*) • Kaspersky Endpoint Detection and Response (*EDR (KATA)*) • Network Detection and Response (*NDR (KATA)*) U kunt alle functionele eenheden of afzonderlijke functionele eenheden afzonderlijk kopen. Voor informatie over de oplossing raadpleegt u de Help van Kaspersky Anti Targeted Attack Platform. **Sandbox** Ingebouwde agent voor Sandbox. Het *Sandbox*-onderdeel detecteert en blokkeert automatisch geavanceerde dreigingen op computers. Sandbox analyseert het gedrag van objecten om schadelijke activiteit en activiteit kenmerkend voor doelgerichte aanvallen op de IT-infrastructuur van het bedrijf te detecteren. Sandbox analyseert en scant objecten op speciale servers met geïmplementeerde virtuele kopieën van Microsoft Windows-besturingssystemen (Sandbox-servers). Voor informatie over de oplossing raadpleeg de Help van Kaspersky Sandbox en Help van Kaspersky Anti Targeted Attack Platform. **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.

Modi van het programma: Standaard, EDR-agent, Light Agent

Kaspersky Endpoint Security voor Windows maakt deel uit van veel Kaspersky-oplossingen. Afhankelijk van de oplossing moet u een modus voor het programma selecteren.



Standaardmodus

Dit is de hoofd- en standaardmodus van het programma. U kunt het programma in deze modus installeren als onderdeel van Kaspersky EPP (Endpoint Protection Platform)-oplossingen. Kaspersky Endpoint Security in de Standaardmodus maakt bijvoorbeeld deel uit van Kaspersky Endpoint Security for Business. Kaspersky Endpoint Security biedt uitgebreide bescherming van werkstations en servers tegen verschillende bedreigingen, netwerkaanvallen en oplichting. In de standaardmodus zijn ook ingebouwde agents beschikbaar voor integratie met Kaspersky Detection and Response-oplossingen, waaronder EDR, MDR, KUMA en andere.



EDR Agent

In deze modus kunt u Kaspersky Detection and Response-oplossingen samen met EPP-oplossingen van derden implementeren. Detectie- en responsoplossingen omvatten Kaspersky Managed Detection and Response (MDR) en Kaspersky Anti Targeted Attack Platform (KATA). EDR Agent ondersteunt ook de Kaspersky SIEM-oplossing, Kaspersky Unified Monitoring and Analysis Platform (KUMA).

In deze modus zijn standaard beschermingsonderdelen zoals File Threat Protection of Web Threat Protection niet beschikbaar. De standaard bescherming van de computer wordt verzorgd door de externe EPP-oplossing. EDR Agent controleert voortdurend de processen die op deze computers worden uitgevoerd, open netwerkverbindingen en gewijzigde bestanden. Daarnaast communiceert de EDR Agent met Detection and Response-oplossingen.



Light Agent

Deze modus wordt gebruikt om virtuele omgevingen te beschermen. Kaspersky Endpoint Security in Light Agent-modus maakt deel uit van de Kaspersky Hybrid Cloud Security-oplossing. Light Agent beschermt virtuele machines met gastbesturingssystemen voor werkstations en servers. In deze modus zijn dezelfde beschermings- en besturingsonderdelen beschikbaar als in de Standaardmodus. Het verschil is dat objecten worden gescand op virussen en andere malware door een speciaal oplossingsonderdeel dat op een aparte virtuele machine is geïnstalleerd, SVM (Secure Virtual Machine). De Light Agent gebruikt dus de bronnen van SVM om de beveiliging van de infrastructuur te garanderen in plaats van de bronnen van de virtuele machine.

Software pakket

Het softwarepakket bevat de volgende distributiepakketten:

- **AES256**

  Dit distributiepakket is bedoeld voor installatie op computers met x86/x64-architectuur. Dit distributiepakket bevat cryptografische tools die het AES-encryptiealgoritme (Advanced Encryption Standard) met een effectieve sleutellengte van 256 bits implementeren.

- **AES56**

  Dit distributiepakket is bedoeld voor installatie op computers met x86/x64-architectuur. Dit distributiepakket bevat cryptografische tools die het AES-encryptiealgoritme met een effectieve sleutellengte van 56 bits implementeren.

- **Arm64**

  Dit distributiepakket is bedoeld voor installatie op Arm-gebaseerde computers. Dit distributiepakket is niet bedoeld voor installatie op servers.

Controleer vóór de installatie of het distributiepakket overeenkomt met de architectuur van uw processor. Als het distributiepakket niet overeenkomt met de processorarchitectuur, beëindigt het installatieprogramma de installatie met een fout.

Het distributiepakket is een zelfuitpakkend archief in EXE-indeling. Om de inhoud van het distributiepakket te bekijken, moet u het archief uitpakken in een aparte map. Elk distributiepakket bevat de volgende bestanden:

`kes_win.msi`	Installatiepakket van Kaspersky Endpoint Security
`setup_kes.exe`	Benodigde bestanden voor de installatie van het programma via een van de beschikbare methoden.
`kes_win.kud`	Bestand voor het maken van installatiepakketten voor Kaspersky Endpoint Security.
`klcfginst.msi`	Installatiepakket voor de plug-in voor programmabeheer in de Kaspersky Security Center Administration Console.
`bases.cab`	Bestanden van het updatepakket die tijdens de installatie worden gebruikt.
`cleaner_v2.cab` `cleanerapi_v2.cab`	Bestanden voor de verwijdering van incompatibele software.
`incompatible.txt`	Bestand met de lijst met software die compatibiliteitsproblemen met Kaspersky Endpoint Security kan veroorzaken. Kaspersky garandeert niet de compatibiliteit van Kaspersky Endpoint Security met software uit de lijst.
`ksn_<language ID>.txt`	Bestand waarin u de voorwaarden voor deelname aan Kaspersky Security Network kunt lezen.
`license.txt`	Bestand waarin u de Gebruiksrechtovereenkomst en het Privacybeleid kunt lezen.
`installer.ini`	Bestand met de interne instellingen van het distributiepakket.
`kes.cab`	Bestanden voor de grafische interface van het programma.
`aes256.cab` / `aes56.cab`	Bestanden voor het cryptografische AES-algoritme (niet inbegrepen in het Arm64-distributiepakket).
`package.kcat`	Bestand met handtekeningen van de distributiekit van het programma. De digitale handtekening garandeert de authenticiteit en integriteit van de distributiekit van het programma.

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

In dit artikel vindt u de softwareversies waarop het programma is getest en waarvoor het gegarandeerd correct werkt. Het programma werkt mogelijk ook met andere softwareversies, maar die configuraties hebben geen volledige testcyclus ondergaan en zijn niet opgenomen in de lijst met gegarandeerd ondersteunde versies.

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

Om het programma te installeren heeft u beheerdersrechten op de computer nodig.

Minimale algemene vereisten

Minimumvereisten	Werkstation (x86)	Server (x86/x64)	Arm
Opslag	2 GB	2 GB	2 GB
CPU	1 GHz, Ondersteuning voor SSE2-instructies.	1.4 GHz, Ondersteuning voor SSE2-instructies.	1 GHz, Armv8.1-architectuur
RAM	Werkstation (x86): 1 GB Werkstation (x64): 2 GB	2 GB Let op: De server heeft 8 GB geheugen nodig om het programma te installeren met de ingebouwde agent voor integratie met Kaspersky Anti Targeted Attack Platform.	4 GB
Microsoft .NET Framework	4 of hoger	4 of hoger	4,8 of hoger

Werkstations

Ondersteunde besturingssystemen voor werkstations:

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1
- 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
- Windows 11 for Arm64 Home / Pro / Pro for Workstations / Education / Enterprise

Windows-besturingssystemen, vanaf versie 11 24H2, ondersteunen de UDP Receive Segment Coalescing Offload (URO) technologie. De technologie is standaard ingeschakeld als een compatibele netwerkkaart en drivers op de computer zijn geïnstalleerd. Het uitschakelen van URO op de computer van een gebruiker kan de prestaties van het programma aanzienlijk verminderen.

Voor een correcte werking van Kaspersky Endpoint Security moet de service Windows Security Center (wscsvc) actief zijn op de computer van de gebruiker.

Kaspersky Endpoint Security kan niet geïnstalleerd worden op Microsoft Windows 7 zonder geïnstalleerde updates voor besturingssysteem: KB4490628 (12 maart, 2019) en KB4474419 (23 september, 2019). Raadpleeg de Knowledge Base van de Technische Support voor gedetailleerde informatie.

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 for Windows Server op servers en clusters van uw organisatie (Cluster Mode). Het programma ondersteunt ook Server Core Mode (zie bekende problemen).

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
- Windows Web Server 2008 R2 Service Pack 1
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter (including Server Core mode)
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (including Server Core mode)
- Windows Server 2016 Essentials / Standard / Datacenter (including Server Core mode)
- Windows Server 2019 Essentials / Standard / Datacenter (including Server Core mode)
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (including Server Core mode)
- Windows Server 2025 Standard / Datacenter

Kaspersky Endpoint Security kan niet geïnstalleerd worden op Microsoft Windows Server 2008 R2 zonder geïnstalleerde updates voor besturingssysteem: KB4490628 (12 maart, 2019) en KB4474419 (23 september, 2019).

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.

Niet ondersteunde besturingssystemen voor servers:

- Windows Server 2003 Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 2

- Windows Server 2008 Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2008 Core Standard / Enterprise / Datacenter Service Pack 2
- Microsoft Small Business Server 2008 Standard / Premium Service Pack 2

Virtuele platforms

Ondersteunde virtuele platforms voor de werking van programma's in de standaardmodus:

- VMware Workstation Pro 26H1
- VMware ESXi 8.0 Update 3i
- Windows Server 2025
- Citrix Virtual Apps and Desktops 7 2507 LTSR
- Citrix Provisioning 2507 LTSR
- XenServer 8.4

Het programma ondersteunt virtuele machines met Windows 11 Pro Arm64 die zijn gemaakt met Hyper-V.

Virtuele machines voor de installatie van Light Agent

De installatie van Kaspersky Endpoint Security in de Light Agent-modus op virtuele machines met Arm wordt niet ondersteund.

Het BIOS op virtuele machines moet de SMBIOS-specificatie versie 2.1 of nieuwer ondersteunen.

De volgende pakketten en hulpprogramma's moeten op virtuele machines zijn geïnstalleerd:

- Bij gebruik van Microsoft Hyper-V – Integration Services-pakket.
- Bij gebruik van VMware vSphere – VMware Tools-pakket.
- Bij gebruik van XenServer – XenTools-pakket.
- Bij gebruik van HUAWEI FusionSphere – HUAWEI Tools-pakket.
- Bij gebruik van op KVM gebaseerde hypervisors – QEMU Guest Agent.

Zie de Help van Kaspersky Security for Virtualization Light Agent voor de vereisten voor virtuele infrastructuur om het programma in de Light Agent-modus uit te voeren.

Voor een correcte werking van het programma dient u een gevirtualiseerde netwerkinterface te gebruiken met een bandbreedte van ten minste 100 Mbit/s.

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
- Microsoft Remote Desktop Services gebaseerd op Windows Server 2022
- Microsoft Remote Desktop Services gebaseerd op Windows Server 2025
- Citrix RDSH van Citrix Virtual Apps and Desktops 7 2507 LTSR

Kaspersky Security Center ondersteuning

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

- Kaspersky Security Center 14.2
- Kaspersky Security Center Linux 14.2
- Kaspersky Security Center Linux 15
- Kaspersky Security Center Windows 15.1
- Kaspersky Security Center Linux 15.1
- Kaspersky Security Center Linux 15.2
- Kaspersky Security Center Linux 15.3
- Kaspersky Security Center Linux 15.4
- Kaspersky Security Center Linux 16

- Kaspersky Security Center Linux 16.1
- Kaspersky Security Center Linux 16.2

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).

Vanaf Kaspersky Endpoint Security 12.8 voor Windows kunt u in het installatiepakket verschillende sets onderdelen voor verschillende typen besturingssystemen configureren. Dat wil zeggen dat u het programma op werkstations en servers kunt implementeren met hetzelfde installatiepakket.

De installatie van Kaspersky Endpoint Security in de Light Agent-modus op virtuele machines met Arm wordt niet ondersteund.

Vergelijking van Kaspersky Endpoint Security-functies

Functie	Werkstation	Arm-gebaseerd werkstation	Server	Server Core-modus
Advanced Threat Protection				
Kaspersky Security Network	✓	✓	✓	✓
Gedragsdetectie	✓	✓	✓	✓
Anti-Cryptor	✓	✓	✓	✓
Exploit-preventie	✓	✓	✓	✓
Host Intrusion Prevention	✓	✓	–	–
Remediation Engine	✓	✓	✓	✓
Essential Threat Protection				
File Threat Protection	✓	✓	✓	✓
Web Threat Protection	✓	✓	✓	–
Mail Threat Protection	✓	✓	✓	–
Firewall	✓	✓	✓	✓
Network Threat Protection	✓	✓	✓	✓
BadUSB Attack Prevention	✓	✓	✓	–
AMSI-bescherming	✓	✓	✓	✓
Security Controls				
Log Inspectie	–	–	✓	–
Programmacontrole	✓	✓	✓	✓
Apparaatcontrole	✓	✓	✓	✓
Webcontrole	✓	✓	✓	–
Adaptieve controle op afwijkingen	✓	✓	–	–
Systeemintegriteitscontrole	–	–	✓	–
Cloud Discovery	✓	✓	–	–

Functie	Werkstation	Arm-gebaseerd werkstation	Server	Server Core-modus
Gegevensencryptie				
Kaspersky Disk Encryption	✓	–	–	–
BitLocker-stationsversleuteling	✓	✓	✓	✓
File Level Encryption	✓	–	–	–
Encryptie van verwisselbare schijven	✓	–	–	–
Detection and Response				
Endpoint Detection and Response Optimum	✓	✓	✓	✓
Endpoint Detection and Response Expert (cloud)	✓	–	✓	✓
Endpoint Detection and Response (KATA)	✓	✓	✓	✓
Network Detection and Response (KATA)	✓	✓	✓	✓
Sandbox	✓	✓	✓	✓
Managed Detection and Response (MDR)	✓	✓	✓	✓
KUMA-integratie	✓	✓	✓	✓

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.

Kaspersky Endpoint Security maakt deel uit van de Kaspersky Next Pro View-oplossing. Raadpleeg Kaspersky Next Help voor meer informatie over de beschikbare functies van het programma wanneer deze als onderdeel van deze oplossing werkt.

Vergelijking van Kaspersky Endpoint Security-functies

Functie	Kaspersky Security Center		Kaspersky Security Center
	Beheerconsole	Webconsole	Cloudconsole
Advanced Threat Protection			
Kaspersky Security Network	✓	✓	✓
Kaspersky Private Security Network	✓	✓	–

Functie	Kaspersky Security Center		Kaspersky Security Center
	Beheerconsole	Webconsole	Cloudconsole
Gedragsdetectie	✓	✓	✓
Anti-Cryptor			
Exploit-preventie	✓	✓	✓
Host Intrusion Prevention	✓	✓	✓
Remediation Engine	✓	✓	✓
Essential Threat Protection			
File Threat Protection	✓	✓	✓
Web Threat Protection	✓	✓	✓
Mail Threat Protection	✓	✓	✓
Firewall	✓	✓	✓
Network Threat Protection	✓	✓	✓
BadUSB Attack Prevention	✓	✓	✓
AMSI-bescherming	✓	✓	✓
Security Controls			
Log Inspectie	✓	✓	✓
Programmacontrole	✓	✓	✓
Apparaatcontrole	✓	✓	✓
Webcontrole	✓	✓	✓
Adaptieve controle op afwijkingen	✓	✓	✓
Systeemintegriteitscontrole	✓	✓	✓
Cloud Discovery	–	–	✓
Gegevensencryptie			
Kaspersky Disk Encryption	✓	✓	–
BitLocker-stationsversleuteling	✓	✓	✓
File Level Encryption	✓	✓	–
Encryptie van verwisselbare schijven	✓	✓	–
Detection and Response			
Endpoint Detection and Response Optimum	–	✓	✓
Endpoint Detection and Response Expert (cloud)	–	–	✓
Endpoint Detection and Response (KATA)	✓	✓	–
Network Detection and Response (KATA)	✓	✓	–
Sandbox	–	✓	–
Managed Detection and Response (MDR)	✓	✓	✓
KUMA-integratie	✓	✓	✓
Taken			
Licentie toevoegen	✓	✓	✓
Programmaonderdelen wijzigen	✓	✓	✓
Inventarisatie	✓	✓	✓
Update	✓	✓	✓
Update terugdraaien	✓	✓	✓

Functie	Kaspersky Security Center		Kaspersky Security Center
	Beheerconsole	Webconsole	Cloudconsole
Malware-scan	✓	✓	✓
Programma 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)	–	✓	✓
Process starten (EDR)	–	✓	✓
Proces beëindigen (EDR)	–	✓	✓

Compatibiliteit met andere programma's

Kaspersky Endpoint Security is incompatibel met sommige Kaspersky-programma's en ook met sommige programma's van derden. Daarom moet u vóór de installatie de programmaversie bijwerken, en de programmaonderdelen wijzigen, Kaspersky Endpoint Security scant de computer om te zien of dergelijke programma's aanwezig zijn.

Compatibiliteit met toepassingen van derden

Kaspersky Endpoint Security is incompatibel met programma's die deel uitmaken van endpoint protection-systemen van derden (Endpoint Protection Platform, EPP). Kaspersky Endpoint Security kan ook compatibiliteitsproblemen met andere programma's ervaren. Om de compatibiliteit te bepalen raadpleegt Kaspersky Endpoint Security een lijst met software die door Kaspersky is opgesteld. Deze lijst bevindt zich in het bestand incompatible.txt. Dit bestand is opgenomen in de distributiekit.

Kaspersky garandeert niet de compatibiliteit van Kaspersky Endpoint Security met software uit de lijst. Als een programma uit de lijst wordt ontdekt, stopt het installatieprogramma de implementatie van Kaspersky Endpoint Security. Het installatieprogramma kan sommige programma's automatisch uit de lijst verwijderen. Als u bereid bent de risico's te negeren en Kaspersky Endpoint Security en een stukje software uit de lijst op dezelfde computer wilt installeren, kunt u de computercontrole overslaan (zie onderstaande instructies).

DOWNLOAD HET INCOMPATIBELE BESTAND TXT

Compatibiliteit met Kaspersky-programma's

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

- Kaspersky Standard | Plus | Premium.
- Kaspersky Small Office Security.
- Kaspersky Internet Security.
- Kaspersky Anti-Virus.
- Kaspersky Total Security.
- Kaspersky Safe Kids.
- Kaspersky Free.
- Kaspersky Anti-Ransomware Tool.
- Endpoint Sensor als onderdeel van Kaspersky Anti Targeted Attack Platform en Kaspersky Endpoint Detection and Response-oplossingen.
- Kaspersky Endpoint Agent als onderdeel van de Detection and Response-oplossingen van Kaspersky.

  Kaspersky schakelt alle Detection and Response over op het werken met de ingebouwde agent van Kaspersky Endpoint Security in plaats van Kaspersky Endpoint Agent. Vanaf versie 12.1 ondersteunt het programma alle Detection and Response-oplossingen.

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

  Vanaf Kaspersky Endpoint Security 12.0 kunt u migreren van Kaspersky Security for Windows Server naar Kaspersky Endpoint Security voor Windows en dezelfde oplossing gebruiken om werkstations en servers te beschermen.

- 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.

De controle overslaan op software die compatibiliteitsproblemen kan veroorzaken

Als Kaspersky Endpoint Security software uit de lijst incompatible.txt detecteert, wordt de installatie van het programma beëindigd. Om door te gaan met de installatie, moet u dat programma verwijderen. Als de leverancier van software van derden echter in zijn documentatie heeft aangegeven dat zijn software compatibel is met Endpoint Protection Platform (EPP), kunt u Kaspersky Endpoint Security installeren op een computer die een programma van deze leverancier bevat. De leverancier van de Endpoint Detection and Response (EDR)-oplossing kan bijvoorbeeld verklaren dat deze compatibel is met EPP-systemen van derden. Als dit het geval is, moet u de installatie van Kaspersky Endpoint Security starten zonder een geïnstalleerde softwarecontrole uit te voeren. Geef hiervoor de volgende parameters door aan de installateur:

- `SKIPPRODUCTCHECK=1` Controle op geïnstalleerde software uitschakelen. De lijst met software die compatibiliteitsproblemen kan veroorzaken, vindt u in het bestand incompatible.txt in het distributiepakket. Als er geen waarde is ingesteld voor deze parameter en er wordt software uit de lijst gedetecteerd, wordt de installatie van Kaspersky Endpoint Security beëindigd.

- `SKIPPRODUCTUNINSTALL=1` Schakel de automatische verwijdering van gedetecteerde software uit de lijst incompatible.txt uit. Als er geen waarde is ingesteld voor deze parameter, probeert Kaspersky Endpoint Security de software te verwijderen die compatibiliteitsproblemen kan veroorzaken.

- `CLEANERSIGNCHECK=0` Schakel de verificatie van digitale handtekening uit van programma's die door de controle worden gevonden. Als deze parameter niet is ingesteld, is de verificatie van digitale handtekeningen uitgeschakeld bij de implementatie van het programma via Kaspersky Security Center. Wanneer het programma lokaal is geïnstalleerd, is verificatie van digitale handtekeningen standaard ingeschakeld.

U kunt parameters in de opdrachtregel doorgeven wanneer u het programma lokaal installeert.

Als u tijdens het installatieproces de scan op software die compatibiliteitsproblemen kan veroorzaken hebt overgeslagen, kan Kaspersky Endpoint Security deze controle opnieuw uitvoeren wanneer de programmaonderdelen worden gewijzigd. Als u de scan naar geïnstalleerde software wilt overslaan, moet u de *Programmaonderdelen wijzigen* taak overslaan.

Voorbeeld:

```
C:\KES\setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0 /s
```

Om Kaspersky Endpoint Security op afstand te installeren, moet u de juiste parameters toevoegen aan het installatiepakket-generatiebestand met de naam `kes_win.kud` in `[Setup]` (zie hieronder). Het bestand `kes_win.kud` is inbegrepen in de distributiekit.

kes_win.kud

```
[Setup]
UseWrapper=1
ExecutableRelPath=EXEC
Params=/s /pAKINSTALL=1 /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0
Executable=setup_kes.exe
RebootDelegated = 1
RebootAllowed=1
ConfigFile=installer.ini
RelPathsToExclude=klcfginst.msi
```

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).
- 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.
4. Instellingen ontvangen uit het configuratiebestand (install.cfg).

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

Bij het installeren van Kaspersky Endpoint Security kan het besturingssysteem zijn eigen berichten weergeven. Netwerk- en internetverbindingen kunnen ook worden onderbroken wanneer het programma wordt geïnstalleerd.

Bij het installeren, bijwerken of verwijderen van Kaspersky Endpoint Security kunnen fouten optreden. Raadpleeg voor meer informatie over het oplossen van deze fouten de Knowledge Base van de Technische Support.

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. Voordat u het programma installeert, moet u ervoor zorgen dat Kaspersky Security Center Network Agent op de computer is geïnstalleerd. *Netwerkagent* vereenvoudigt de interactie tussen Administration Server en een clientcomputer.

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.

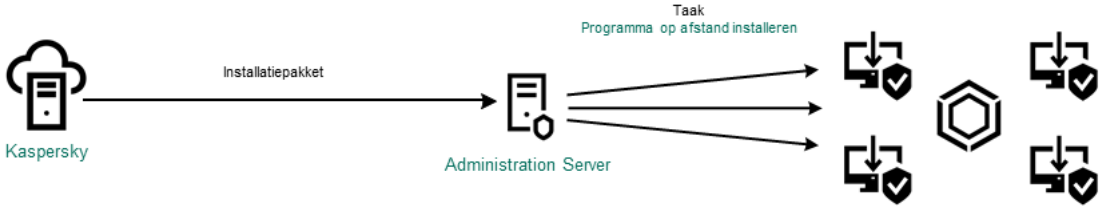
Standaardinstallatie van het programma

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 *Install application remotely* maken in de Administration Server van Kaspersky Security Center.



Kaspersky Endpoint Security implementeren

De wizard Bescherming implementeren uitvoeren in de Beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de beheerconsole **Advanced** → **Remote installation**.
3. Klik op de koppeling **Deploy installation package on managed devices (workstations)**.

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. De bron van het installatiepakket selecteren

Selecteer de bron **Deploy Kaspersky Security Center package**.

Stap 3. 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 4: Instellingen voor installatietaken op afstand definiëren

Configureer de volgende aanvullende programma-instellingen:

- **Force installation package download**. Selecteer de installatiemethode voor het programma:
  - **Using Network Agent**. De Network Agent is verantwoordelijk voor de levering van het installatiepakket van Kaspersky Endpoint Security op de clientcomputers. Als de netwerkagent niet is geïnstalleerd, eindigt de taak met een fout. Voeg in dit geval het installatiepakket van Network Agent toe aan de taak *Install application remotely* en schakel de levering van bestanden via bronnen van het besturingssysteem in. Vervolgens wordt de Network Agent geïnstalleerd met gebruikmaking van de bronnen van het besturingssysteem. Kaspersky Endpoint Security wordt vervolgens geïnstalleerd via de tools van de netwerkagent.
  - **Using operating system resources through distribution points**. 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.
  - **Using operating system resources through 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.
- **Behavior for devices managed through other 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.
- **Do not re-install application if it is already installed**. Schakel dit selectievakje uit als u bijvoorbeeld een oudere versie van het programma wilt installeren.
- **Assign Network Agent installation in Active Directory group policies**. Networkagent 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 5: 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 distributiefunctionaliteit heeft, wordt de licentie later automatisch toegevoegd. U kunt ook later het programma activeren met de taak *Add key*.

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. 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 9. De installatie starten

Verlaat de wizard verlaten. Schakel indien nodig het selectievakje **Run the task after the wizard finishes** 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 distributiefunctionaliteit heeft, wordt de licentie later automatisch toegevoegd. U kunt ook later het programma activeren met de taak *Add key*.

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:

- **Force installation package download**. Selecteer de installatiemethode voor het programma:
  - **Using Network Agent**. De Network Agent is verantwoordelijk voor de levering van het installatiepakket van Kaspersky Endpoint Security op de clientcomputers. Als de netwerkagent niet is geïnstalleerd, eindigt de taak met een fout. Voeg in dit geval het installatiepakket van Network Agent toe aan de taak *Install application remotely* en schakel de levering van bestanden via bronnen van het besturingssysteem in. Vervolgens wordt de Network Agent geïnstalleerd met gebruikmaking van de bronnen van het besturingssysteem. Kaspersky Endpoint Security wordt vervolgens geïnstalleerd via de tools van de netwerkagent.
  - **Using operating system resources through distribution points**. 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.
  - **Using operating system resources through 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.
- **Do not re-install application if it is already installed**. Schakel dit selectievakje uit als u bijvoorbeeld een oudere versie van het programma wilt installeren.
- **Assign package installation in Active Directory group policies**. 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 **Unassigned devices**.

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 **Run the task after the wizard finishes** 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 → Advanced → Remote installation → Installation packages**.

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

2. Klik op **Create installation package**.

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

Stap 1. Het type installatiepakket selecteren

Selecteer de optie **Create an installation package for a Kaspersky application**.

Stap 2. De naam van het installatiepakket definiëren

Voer de naam van het installatiepakket in, bijvoorbeeld *Kaspersky Endpoint Security voor Windows 14.1*.

Stap 3: Het distributiepakket voor installatie selecteren

Klik op de knop **Browse** en selecteer het bestand `kes_win.kud` dat in het distributiepakket zit.

Werk indien nodig de antivirusdatabases in het installatiepakket bij met het selectievakje **Copy updates from repository to installation package**.

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 programmaonderdelen voor verschillende typen besturingssystemen selecteren. Dat wil zeggen dat het installatiepakket twee sets onderdelen bevat: voor werkstations en voor servers. Voordat het installatiepakket wordt geïmplementeerd, detecteert het installatieprogramma het type besturingssysteem en installeert het alleen de programmaonderdelen die u voor dat type besturingssysteem hebt geselecteerd. Op deze manier kunt u hetzelfde installatiepakket gebruiken voor werkstations en servers.

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.

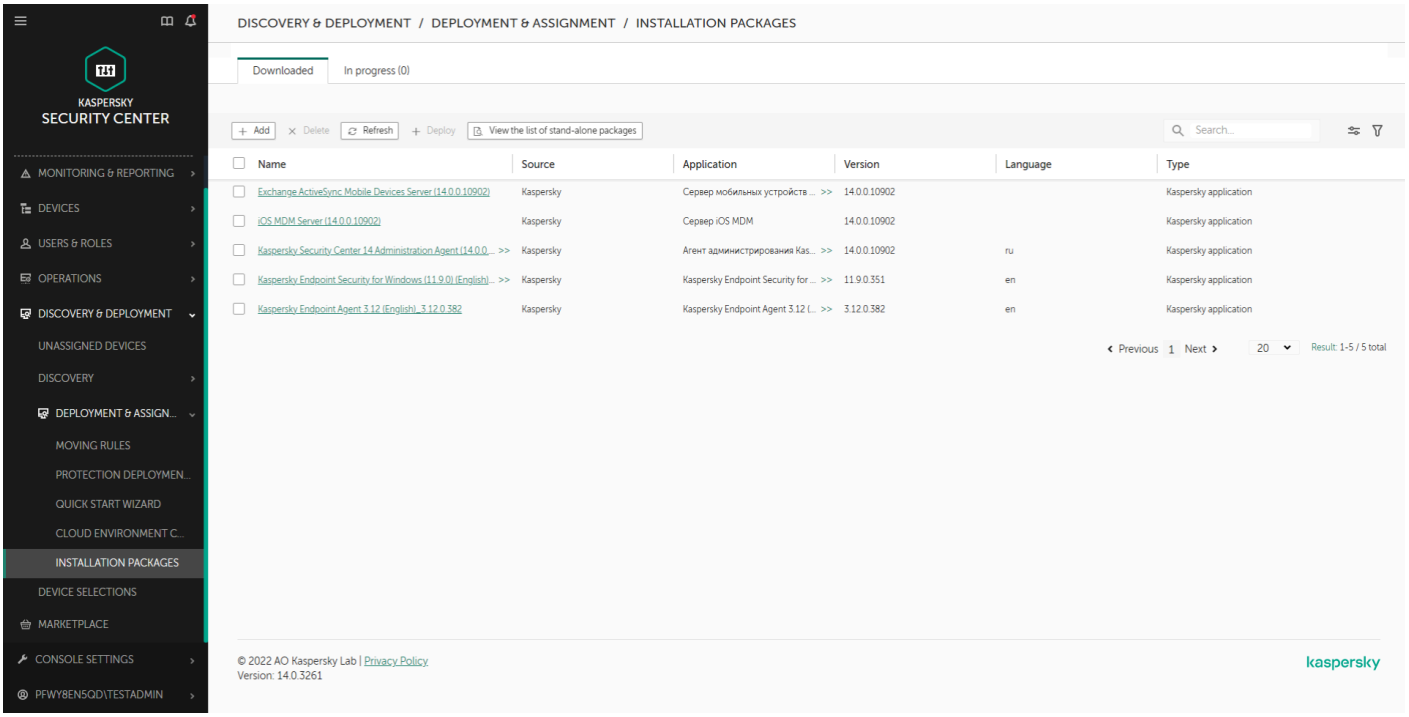
Een installatiepakket maken in de Webconsole en Cloudconsole

1. Selecteer 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 **Add**.

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



Lijst van installatiepakketten

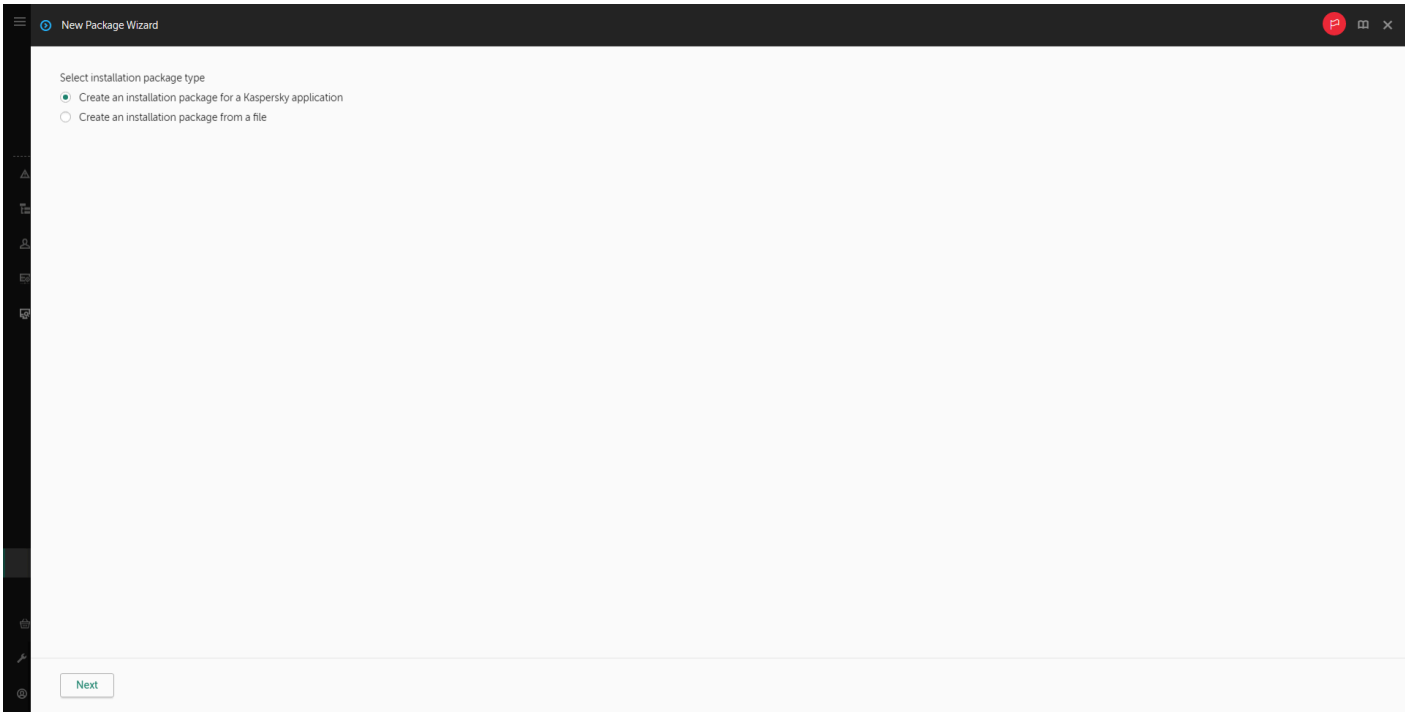
Stap 1. Het type installatiepakket selecteren

Selecteer de optie **Create an installation package for a Kaspersky application**.

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 gereleaset. 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.

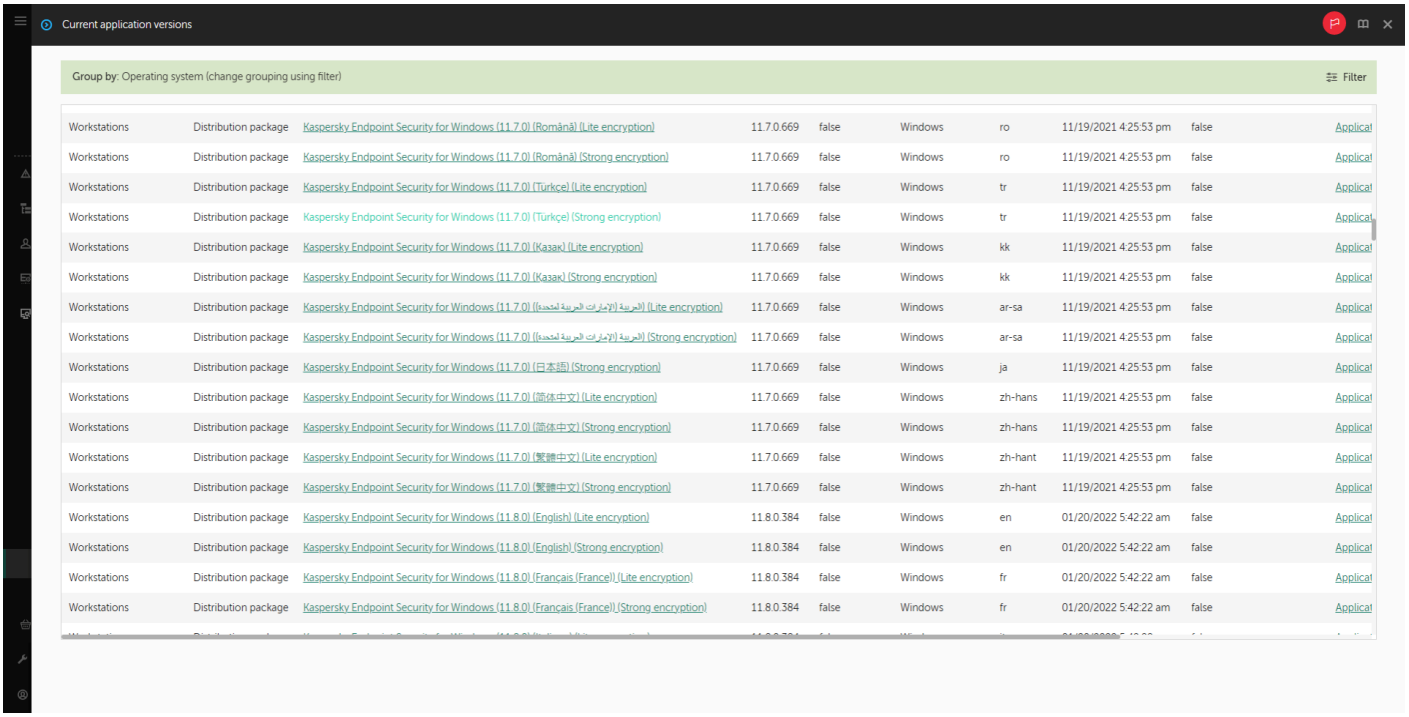
Een installatiepakket maken voor Kaspersky Endpoint Security vanuit een bestand is alleen beschikbaar in Kaspersky Security Center Web Console.



Types installatiepakketten

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.

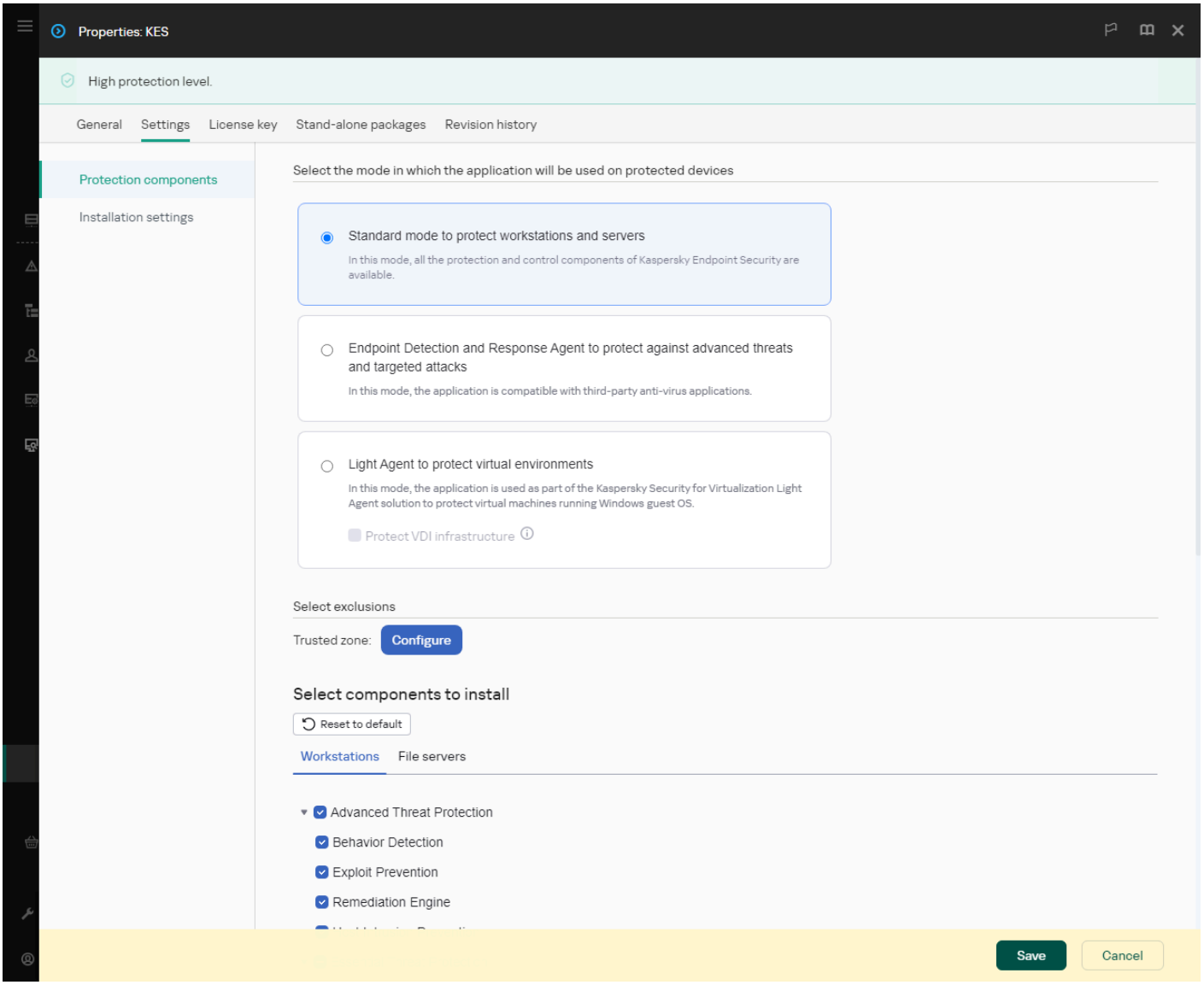


Lijst van installatiepakketten op Kaspersky servers

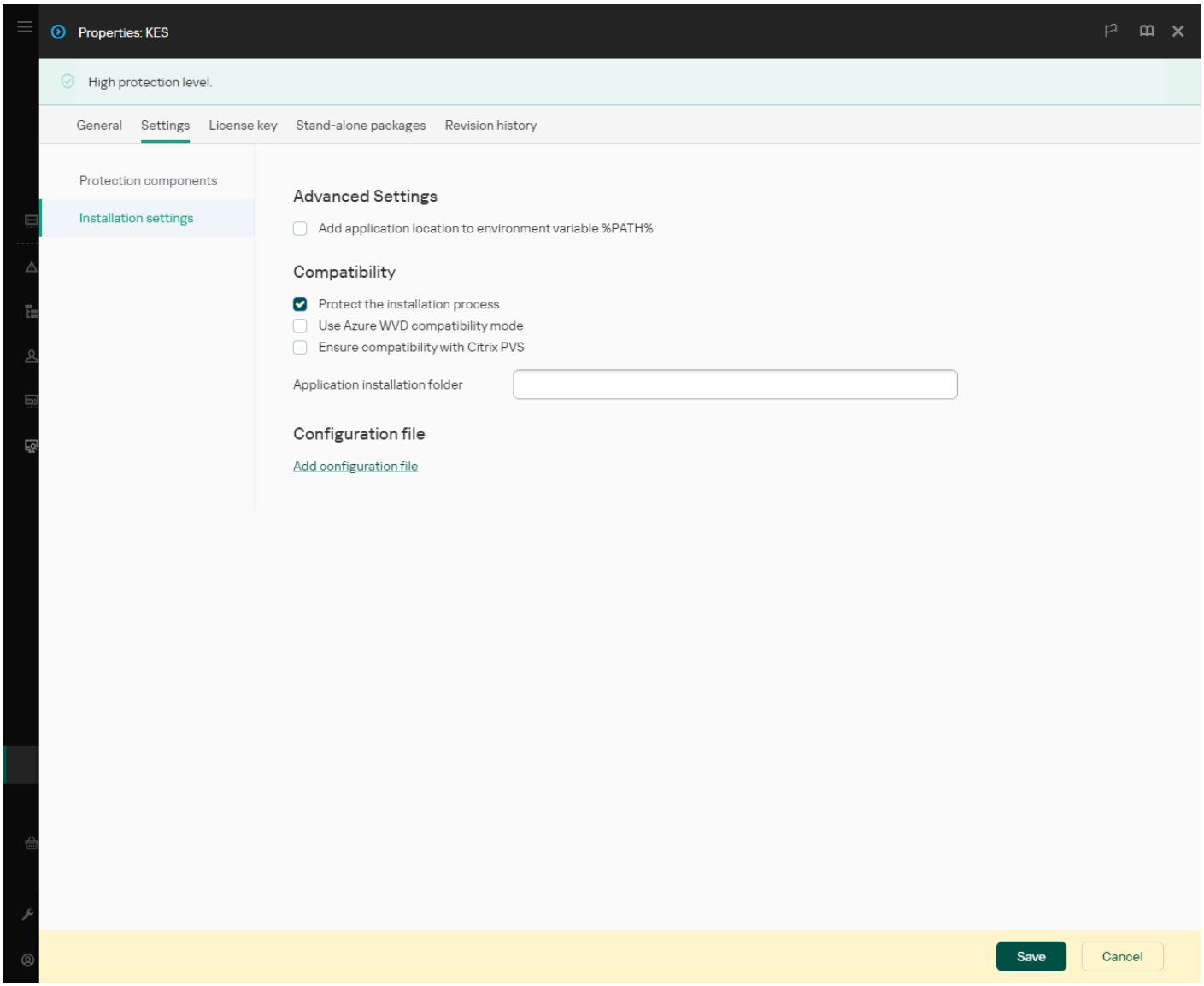
Het installatiepakket wordt gemaakt en toegevoegd aan Kaspersky Security Center. Met het installatiepakket kunt u Kaspersky Endpoint Security installeren op computers in het bedrijfsnetwerk of de programmaversie updaten.

In de instellingen van het installatiepakket kunt u programmaonderdelen voor verschillende typen besturingssystemen selecteren. Dat wil zeggen dat het installatiepakket twee sets onderdelen bevat: voor werkstations en voor servers. Voordat het installatiepakket wordt geïmplementeerd, detecteert het installatieprogramma het type besturingssysteem en installeert het alleen de programmaonderdelen die u voor dat type besturingssysteem hebt geselecteerd. Op deze manier kunt u hetzelfde installatiepakket gebruiken voor werkstations en servers.

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.



Onderdelen opgenomen in het installatiepakket



Installatie-instellingen van het installatiepakket

Instellingen van het installatiepakket

Gedeelte	Beschrijving
Beschermingsonderdelen	**Standaardmodus**. De standaardconfiguratie. Met deze configuratie kunt u alle onderdelen van het programma gebruiken, inclusief onderdelen die ondersteuning bieden voor Detection and Response-oplossingen. Deze configuratie wordt gebruikt voor uitgebreide bescherming van de computer tegen verschillende bedreigingen, netwerkaanvallen en fraude. **Endpoint Detection and Response Agent**. In deze configuratie kunt u alleen de onderdelen installeren die ondersteuning bieden voor Detection and Response-oplossingen: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), evenals KUMA. Deze configuratie is nodig als een Endpoint Protection Platform (EPP) van derden wordt geïmplementeerd in uw organisatie naast een Kaspersky Detection and Response-oplossing. Hierdoor is Kaspersky Endpoint Security in de Endpoint Detection and Response Agent-configuratie compatibel met EPP-programma's van derden. **Light Agent om virtuele omgevingen te beschermen**. Deze configuratie is bedoeld voor het programma die wordt gebruikt als onderdeel van de Kaspersky Security for Virtualization Light Agent-oplossing. Light Agent moet worden geïnstalleerd op elke virtuele machine die met de oplossing moet worden beschermd. In deze configuratie kunt u geen Onderdelen voor gegevensencryptie of Adaptieve controle op afwijkingen gebruiken. Als u Light Agent installeert op een virtuele machinesjabloon die zal worden gebruikt om *niet-permanente virtuele machines* te maken, schakel dan het selectievakje **Bescherm de VDI-infrastructuur** (VDI staat voor Virtual Desktop Infrastructure). De VDI-beschermingsmodus helpt de prestaties van Kaspersky Endpoint Security op niet-permanente virtuele machines te optimaliseren. In deze modus weigert Light Agent programma-updates waarvoor de virtuele machine opnieuw moet worden opgestart. Bij het ontvangen van programma-updates die een herstart vereisen, genereert Light Agent een event over de noodzaak om de template van de beschermde virtuele machines bij te werken.

Gedeelte	Beschrijving
Uitzonderingen	Beginnend met Kaspersky Endpoint Security 12.6 voor Windows, uitzonderingen scannen en vertrouwde programma's worden toegevoegd aan de vertrouwde zone. Vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's helpen bij het snel configureren van Kaspersky Endpoint Security op SQL-servers, Microsoft Exchange-servers en System Center Configuration Manager. Dit betekent dat u niet handmatig een vertrouwde zone voor het programma op servers hoeft in te stellen. Vanaf Kaspersky Endpoint Security 12.8 voor Windows kun je het programma in Light Agent-modus installeren om virtuele omgevingen te beschermen. Met voorgedefinieerde uitzonderingen van scans en vertrouwde programma's kunt u Kaspersky Endpoint Security snel configureren in Citrix- en VMware-virtuele omgevingen. U kunt de vertrouwde zone ook later configureren in de beleidseigenschappen: scanuitzonderingen en vertrouwde programma's.
Selecteer de onderdelen die u wilt installeren	In dit gedeelte kunt u selecteren welke programmaonderdelen beschikbaar zullen zijn. U kunt later de selectie van programmaonderdelen wijzigen met de taak *Programmaonderdelen wijzigen*. U kunt afzonderlijke sets onderdelen voor werkstations en servers maken. Voordat het installatiepakket wordt geïmplementeerd, detecteert het installatieprogramma het type besturingssysteem en installeert het alleen de programmaonderdelen die u voor dat type besturingssysteem hebt geselecteerd. Op deze manier kunt u hetzelfde installatiepakket gebruiken voor werkstations en servers. De set beschikbare onderdelen is afhankelijk van de configuratie van het programma: **Standaardmodus** 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. **Endpoint Detection and Response Agent** In deze configuratie zijn alleen ingebouwde agenten voor Kaspersky Detection and Response-oplossingen beschikbaar. **Light Agent om virtuele omgevingen te beschermen** In deze configuratie kunt u vrijwel alle programmaonderdelen gebruiken die beschikbaar zijn in de **Standaardmodus** configuratie, met uitzondering van onderdelen voor gegevensencryptie en Adaptieve controle op afwijkingen.
License key	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 Help van Kaspersky Security Center.
Incompatible applications	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.
Installation settings	**Voeg het pad naar het bestand avp.com toe aan de systeemvariabele %PATH%**. U kunt het pad voor de installatie toevoegen aan de variabele %PATH% om de opdrachtregel-interface eenvoudig te gebruiken. **Protect the installation process**. 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 Remote Desktop), wordt u aanbevolen de bescherming van het installatieproces uit te schakelen. **Zorg voor compatibiliteit met Citrix PVS**. U kunt de ondersteuning voor Citrix Provisioning Services inschakelen om Kaspersky Endpoint Security op een virtuele machine te installeren. **Azure WVD compatibiliteitsmodus gebruiken**. Deze functie garandeert een correcte weergave van de status van de Azure virtuele machine in de console van Kaspersky Anti Targeted Attack Platform. Om de prestaties van de computer te controleren, verzendt Kaspersky Endpoint Security telemetrie naar KATA-servers. Telemetrie omvat een ID van de computer (Sensor ID). Met de Azure WVD-compatibiliteitsmodus kunt u een permanente unieke Sensor ID toewijzen aan deze virtuele machines. Als de compatibiliteitsmodus is uitgeschakeld, kan de Sensor ID veranderen nadat de computer opnieuw is opgestart vanwege de manier waarop virtuele Azure-machines werken. Dit kan er voor zorgen dat duplicaten van virtuele machines op de console worden weergegeven. **Application installation folder**. U kunt het pad voor de installatie van Kaspersky Endpoint Security op een clientcomputer wijzigen. Standaard wordt het programma geïnstalleerd in de map `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.1`. **Configuration file**. Het programma installeren met vooraf gedefinieerde instellingen. Om dit te doen, moet u een bestand uploaden dat de instellingen van Kaspersky Endpoint Security definieert. U kunt een configuratiebestand in de lokale interface van het programma maken.

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 *Download updates to the Administration Server repository* 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. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de consolestructuur de map **Advanced** → **Remote installation** → **Installation packages**.

   Er wordt een lijst geopend met installatiepakketten die zijn gedownload naar Kaspersky Security Center.
3. Open de eigenschappen van het installatiepakket.
4. Klik in het gedeelte **General** op **Update databases**.

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. Selecteer 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 **General information** op de koppeling **Update databases**.

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 *Install application remotely* is bedoeld om Kaspersky Endpoint Security op afstand te installeren. Met de taak *Install application remotely* 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. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de beheerconsole **Tasks**.

   De lijst met taken wordt geopend.
3. Klik op **New task**.

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

Stap 1. Een taaktype selecteren

Selecteer **Kaspersky Security Center Administration Server → Install application remotely**.

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:

- **Force installation package download**. Selecteer de installatiemethode voor het programma:

  - **Using Network Agent**. De Network Agent is verantwoordelijk voor de levering van het installatiepakket van Kaspersky Endpoint Security op de clientcomputers. Als de netwerkagent niet is geïnstalleerd, eindigt de taak met een fout. Voeg in dit geval het installatiepakket van Network Agent toe aan de taak *Install application remotely* en schakel de levering van bestanden via bronnen van het besturingssysteem in. Vervolgens wordt de Network Agent geïnstalleerd met gebruikmaking van de bronnen van het besturingssysteem. Kaspersky Endpoint Security wordt vervolgens geïnstalleerd via de tools van de netwerkagent.

  - **Using operating system resources through distribution points**. 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.

  - **Using operating system resources through 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.

- **Behavior for devices managed through other 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.

- **Do not re-install application if it is already installed**. 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 14.1 installeren*.

Stap 10. Aanmaak van de taak voltooien

Verlaat de wizard verlaten. Schakel indien nodig het selectievakje **Run the task after the wizard finishes** 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 **Asset management** → **Tasks**.

   De lijst met taken wordt geopend.

2. Klik op **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** de optie **Kaspersky Security Center**.
2. Selecteer in de vervolgkeuzelijst **Task type** de optie **Install application remotely**.
3. Typ in het veld **Task name** een korte omschrijving, zoals *Installatie van Kaspersky Endpoint Security voor managers*.
4. Selecteer in het gedeelte **Devices to which the task will be assigned** 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 (14.1) voor Windows.
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 **Force installation package download** de installatiemethode voor het programma:

   - **Using Network Agent**. De Network Agent is verantwoordelijk voor de levering van het installatiepakket van Kaspersky Endpoint Security op de clientcomputers. Als de netwerkagent niet is geïnstalleerd, eindigt de taak met een fout. Voeg in dit geval het installatiepakket van Network Agent toe aan de taak *Install application remotely* en schakel de levering van bestanden via bronnen van het besturingssysteem in. Vervolgens wordt de Network Agent geïnstalleerd met gebruikmaking van de bronnen van het besturingssysteem. Kaspersky Endpoint Security wordt vervolgens geïnstalleerd via de tools van de netwerkagent.

   - **Using operating system resources through distribution points**. 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.

   - **Using operating system resources through 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 number of concurrent 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 number of installation attempts** 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 **Do not re-install application if it is already installed** uit. Op deze manier kunt u bijvoorbeeld een oudere versie van het programma installeren.

7. Schakel indien nodig het selectievakje **Verify operating system type before downloading** 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 **Assign package installation in Active Directory group policies** 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 **Prompt users to close running applications** 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 **Behavior for devices managed through other 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 **Start** 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.

Het programma lokaal met de wizard installeren

De interface van de Installatiewizard van het programma bestaat uit een reeks vensters die de installatiestappen van het programma voorstellen. Zorg ervoor dat het gebruikersaccount waarmee u de installatiewizard uitvoert, deel uitmaakt van de beheerdersgroep.

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

1. Kopieer de distributiekit map naar de computer van de gebruiker.
2. Voer setup_kes.exe uit.

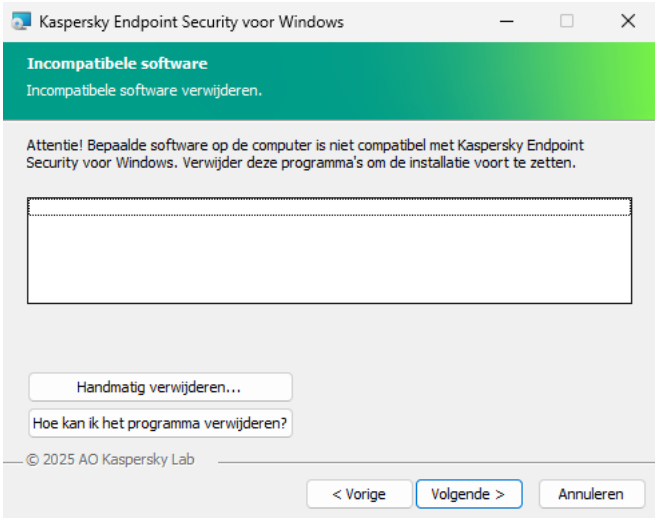
   De Installatiewizard wordt gestart.

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:

- Is er software geïnstalleerd die mogelijk compatibiliteitsproblemen heeft met Kaspersky Endpoint Security? (de lijst met software is beschikbaar in het bestand incompatible.txt dat is meegeleverd met de distributiekit).
- Of aan de hardware- en softwarevereisten is voldaan.
- Of Microsoft .NET Framework aanwezig is.
- 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. Bijvoorbeeld een melding over incompatibele software (zie onderstaande figuur).



Incompatibele software verwijderen

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 14.1 voor Windows. De vorige versie van het programma wordt automatisch verwijderd. Dit is van toepassing op de volgende programmaversies:

- Kaspersky Endpoint Security 12.1 voor Windows (build 12.1.0.506)
- Kaspersky Endpoint Security 12.2 voor Windows (build 12.2.0.462)
- Kaspersky Endpoint Security 12.3 voor Windows (build 12.3.0.493)
- Kaspersky Endpoint Security 12.4 voor Windows (build 12.4.0.467)
- Kaspersky Endpoint Security 12.5 voor Windows (build 12.5.0.539)
- Kaspersky Endpoint Security 12.6 voor Windows (build 12.6.0.438)
- Kaspersky Endpoint Security 12.7 voor Windows (build 12.7.0.533)
- Kaspersky Endpoint Security 12.8 voor Windows (build 12.8.0.505)
- Kaspersky Endpoint Security 12.9 voor Windows (build 12.9.0.384)
- Kaspersky Endpoint Security 12.10 voor Windows (build 12.10.0.466)
- Kaspersky Endpoint Security 12.11 voor Windows (build 12.11.0.637)
- Kaspersky Endpoint Security 12.12 voor Windows (build 12.12.0.522)
- Kaspersky Endpoint Security 14.0 voor Windows (build 14.0.0.504)

Configuratie van Kaspersky Endpoint Security



De configuratie van het programma kiezen

Standaardmodus. De standaardconfiguratie. Met deze configuratie kunt u alle onderdelen van het programma gebruiken, inclusief onderdelen die ondersteuning bieden voor Detection and Response-oplossingen. Deze configuratie wordt gebruikt voor uitgebreide bescherming van de computer tegen verschillende bedreigingen, netwerkaanvallen en fraude.

Endpoint Detection and Response Agent. In deze configuratie kunt u alleen de onderdelen installeren die ondersteuning bieden voor Detection and Response-oplossingen: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), evenals KUMA. Deze configuratie is nodig als een Endpoint Protection Platform (EPP) van derden wordt geïmplementeerd in uw organisatie naast een Kaspersky Detection and Response-oplossing. Hierdoor is Kaspersky Endpoint Security in de Endpoint Detection and Response Agent-configuratie compatibel met EPP-programma's van derden.

Light Agent om virtuele omgevingen te beschermen. Deze configuratie is bedoeld voor het programma die wordt gebruikt als onderdeel van de Kaspersky Security for Virtualization Light Agent-oplossing. Light Agent moet worden geïnstalleerd op elke virtuele machine die met de oplossing moet worden beschermd. In deze configuratie kunt u geen Onderdelen voor gegevensencryptie of Adaptieve controle op afwijkingen gebruiken. Als u Light Agent installeert op een virtuele machinesjabloon die zal worden gebruikt om *niet-permanente virtuele machines* te maken, schakel dan het selectievakje **Bescherm de VDI-infrastructuur** (VDI staat voor Virtual Desktop Infrastructure). De VDI-beschermingsmodus helpt de prestaties van Kaspersky Endpoint Security op niet-permanente virtuele machines te optimaliseren. In deze modus weigert Light Agent programma-updates waarvoor de virtuele machine opnieuw moet worden opgestart. Bij het ontvangen van programma-updates die een herstart vereisen, genereert Light Agent een event over de noodzaak om de template van de beschermde virtuele machines bij te werken.

Kaspersky Endpoint Security-onderdelen

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



Programmaonderdelen selecteren voor installatie

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 (cloud)
- Alleen Endpoint Detection and Response Expert (on-premises)
- Alleen Network Detection and Response (KATA)
- Alleen Sandbox
- Endpoint Detection and Response Optimum en Sandbox
- Endpoint Detection and Response Expert (cloud) en Sandbox
- Endpoint Detection and Response Expert (on-premises) en Sandbox

- Network Detection and Response (KATA) en Endpoint Detection and Response Expert (on-premises)
- Network Detection and Response (KATA) en Managed Detection and Response

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.

De map selecteren voor het installeren van het programma

U kunt het pad voor de installatie van Kaspersky Endpoint Security op een clientcomputer wijzigen. Standaard wordt het programma geïnstalleerd in de map `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.1`.

De vertrouwde zone configureren

Beginnend met Kaspersky Endpoint Security 12.6 voor Windows, uitzonderingen scannen en vertrouwde programma's worden toegevoegd aan de vertrouwde zone. Vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's helpen bij het snel configureren van Kaspersky Endpoint Security op SQL-servers, Microsoft Exchange-servers en System Center Configuration Manager. Dit betekent dat u niet handmatig een vertrouwde zone voor het programma op servers hoeft in te stellen.

Vanaf Kaspersky Endpoint Security 12.8 voor Windows kun je het programma in Light Agent-modus installeren om virtuele omgevingen te beschermen. Met voorgedefinieerde uitzonderingen van scans en vertrouwde programma's kunt u Kaspersky Endpoint Security snel configureren in Citrix- en VMware-virtuele omgevingen.

U kunt de vertrouwde zone ook later configureren in de beleidseigenschappen: scanuitzonderingen en vertrouwde programma's.

Geavanceerde instellingen



Geavanceerde instellingen van programma-installatie

Bescherm het installatieproces van het programma. 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 Remote Desktop), wordt u aanbevolen de bescherming van het installatieproces uit te schakelen.

Zorg voor compatibiliteit met Citrix PVS. U kunt de ondersteuning voor Citrix Provisioning Services inschakelen om Kaspersky Endpoint Security op een virtuele machine te installeren.

Voeg het pad naar het bestand avp.com toe aan de systeemvariabele %PATH%. U kunt het pad voor de installatie toevoegen aan de variabele %PATH% om de opdrachtregel-interface eenvoudig te gebruiken.

Het programma op afstand installeren via System Center Configuration Manager

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

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

1. Open de console Configuratiebeheer.
2. Selecteer in het 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.

Gebruik het bestand setup.ini alleen wanneer je de applicatie in stille modus installeert.

U kunt geen pad toevoegen aan de install.cfg configuratiebestand in het bestand setup.ini. Het programma slaat ook de install.cfg configuratiebestand over als dit in dezelfde map staat als de distributiepakket van Kaspersky Endpoint Security. Om instellingen uit het configuratiebestand install.cfg toe te passen, moet u het pad naar het bestand opgeven in de volgende opdracht voor programma-installatie: `CONFIGPATH=<path to the configuration file>`.

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 in de standaardmodus moeten worden geïnstalleerd. 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.
- `[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`, `enabled`, en `true`. De alternatieven voor de waarde `0` zijn de waarden `no`, `off`, `disable`, `disabled`, en `false`.

Instellingen van het bestand 'setup.ini'

Gedeelte	Parameter	Beschrijving
`[Setup]`	`InstallDir`	Pad naar de installatiemap van het programma.
	`ActivationCode`	Activeringscode van Kaspersky Endpoint Security.
	`Eula`	Aanvaarding van de voorwaarden van de Gebruiksrechtovereenkomst. De tekst van de Gebruiksrechtovereenkomst vindt u in het distributiepakket van Kaspersky Endpoint Security. U moet akkoord gaan met de voorwaarden van Gebruiksrechtovereenkomst om het programma te installeren of de versie van het programma te upgraden.

Gedeelte	Parameter	Beschrijving
	`PrivacyPolicy`	Aanvaarding van het Privacybeleid. De tekst van het Privacybeleid wordt bij het distributiepakket van Kaspersky Endpoint Security meegeleverd. U moet akkoord gaan met het Privacybeleid om het programma te installeren of een upgrade voor de programmaversie uit te voeren.
	`KSN`	Aanvaarding of weigering van deelname aan Kaspersky Security Network (KSN). Als geen waarde voor deze parameter is ingesteld, wordt u door Kaspersky Endpoint Security gevraagd of u al dan niet wilt deelnemen aan KSN wanneer Kaspersky Endpoint Security voor het eerst wordt gestart. Beschikbare waarden: • `1` – Aanvaarding van de deelname aan KSN. • `0` – Weigering van de deelname aan KSN (standaardwaarde). Het distributiepakket van Kaspersky Endpoint Security is geoptimaliseerd voor gebruik met Kaspersky Security Network. Als u ervoor hebt gekozen om niet deel te nemen aan Kaspersky Security Network, moet u Kaspersky Endpoint Security meteen na de installatie bijwerken.
	`CLEANERSIGNCHECK`	Het verifiëren van digitale handtekeningen van de gedetecteerde softwarebestanden uit de lijst incompatible.txt. Om de software te verwijderen, voert Kaspersky Endpoint Security het software-installatiebestand uit. Als het installatiebestand geen digitale handtekening heeft, beschouwt Kaspersky Endpoint Security het bestand als onbetrouwbaar en stopt het de verwijdering van software om te voorkomen dat mogelijke schadelijke code wordt uitgevoerd. Als het programma de digitale handtekening van het gedetecteerde softwarebestand niet kan verifiëren, wordt de installatie van Kaspersky Endpoint Security gestopt met een foutmelding. De standaardwaarde is verschillend, afhankelijk van de software-installatiemethode: • `0` betekent dat verificatie van digitale handtekeningen is uitgeschakeld (standaardwaarde indien geïmplementeerd via Kaspersky Security Center). • `1` betekent dat verificatie van digitale handtekeningen is ingeschakeld (standaardwaarde als het programma lokaal wordt geïnstalleerd).
	`Login`	Stel de gebruikersnaam voor toegang tot functies en instellingen van Kaspersky Endpoint Security in (het onderdeel Wachtwoordbeveiliging). De gebruikersnaam wordt samen met de parameters `Password` en `PasswordArea` ingesteld. De gebruikersnaam 'KLAdmin' wordt standaard gebruikt.
	`Password`	Geef een wachtwoord op voor de toegang tot functies en instellingen van Kaspersky Endpoint Security (het wachtwoord wordt samen de parameters `Login` en `PasswordArea` opgegeven). Als u wel een wachtwoord hebt opgegeven maar geen gebruikersnaam bij de parameter `Login`, wordt de gebruikersnaam 'KLAdmin' standaard gebruikt.
	`PasswordArea`	Geef het bereik van het wachtwoord op voor toegang tot functies en instellingen van Kaspersky Endpoint Security. Wanneer een gebruiker een actie uit dit bereik probeert uit te voeren, vraagt Kaspersky Endpoint Security de accountgegevens van de gebruiker (de parameters `Login` en `Password`). Gebruik het teken `;` om meerdere waarden op te geven. Beschikbare waarden: • `SET` – voor het wijzigen van de programma-instellingen. • `EXIT` – voor het afsluiten van het programma. • `DISPROTECT` – voor het uitschakelen van beschermingsonderdelen en het stoppen van scantaken. • `DISPOLICY` – voor het uitschakelen van het Kaspersky Security Center-beleid. • `UNINST` – voor het verwijderen van het programma op de computer. • `DISCTRL` – voor het uitschakelen van de controleonderdelen. • `REMOVELIC` – voor het verwijderen van de licentie. • `REPORTS` – voor het bekijken van rapporten. • `EXPORT` – Programma-instellingen exporteren. Bijvoorbeeld `PasswordArea=SET;PasswordArea=UNINST;PasswordArea=EXIT`.

Gedeelte	Parameter	Beschrijving
	`SelfProtection`	Schakel het beschermingsmechanisme voor de installatie van het programma in of uit. Beschikbare waarden: • `1` – Het beschermingsmechanisme voor de installatie van het programma is ingeschakeld (standaardwaarde). • `0` – Het beschermingsmechanisme voor de installatie van het programma is uitgeschakeld. 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 Remote Desktop), wordt u aanbevolen de bescherming van het installatieproces uit te schakelen.
	`PROTECTOSSERVICES`	Bescherming van de functionaliteit van de besturingssysteemservices. De bescherming van besturingssysteemservices voorkomt dat programma's van derden de werking van besturingssysteemservices verstoren. Dergelijke services omvatten bijvoorbeeld de programma-autostartservice. • `1` betekent dat de bescherming van de besturingssysteemservices is ingeschakeld (standaardwaarde). • `0` betekent dat de bescherming van de besturingssysteemservices is uitgeschakeld.
	`EnableAzureSupport`	De Azure WVD-compatibiliteitsmodus in- of uitschakelen. Beschikbare waarden: • `1` – Azure WVD-compatibiliteitsmodus is ingeschakeld. • `0` – Azure WVD-compatibiliteitsmodus is uitgeschakeld (standaardwaarde). Deze functie garandeert een correcte weergave van de status van de Azure virtuele machine in de console van Kaspersky Anti Targeted Attack Platform. Om de prestaties van de computer te controleren, verzendt Kaspersky Endpoint Security telemetrie naar KATA-servers. Telemetrie omvat een ID van de computer (Sensor ID). Met de Azure WVD-compatibiliteitsmodus kunt u een permanente unieke Sensor ID toewijzen aan deze virtuele machines. Als de compatibiliteitsmodus is uitgeschakeld, kan de Sensor ID veranderen nadat de computer opnieuw is opgestart vanwege de manier waarop virtuele Azure-machines werken. Dit kan er voor zorgen dat duplicaten van virtuele machines op de console worden weergegeven.
	`Reboot`	Computer automatisch opnieuw opstarten, indien nodig na de installatie of upgrade van het programma. Als er geen waarde is ingesteld voor deze parameter, wordt het automatisch herstarten van de computer geblokkeerd. Opnieuw opstarten is niet nodig bij de installatie van Kaspersky Endpoint Security. Opnieuw opstarten is alleen nodig als u incompatibele programma's moet verwijderen alvorens u de installatie kunt starten. De computer opnieuw opstarten is mogelijk ook vereist wanneer u de programmaversie updatet.
	`AddEnvironment`	Voeg het pad naar de uitvoerbare bestanden in de installatiemap van Kaspersky Endpoint Security toe aan de systeemvariabele %PATH%. Beschikbare waarden: • `1` – De systeemvariabele %PATH% wordt toegevoegd aan het pad naar de uitvoerbare bestanden die zich in de installatiemap van Kaspersky Endpoint Security bevinden. • `0` – De systeemvariabele %PATH% wordt niet toegevoegd aan het pad naar de uitvoerbare bestanden die zich in de installatiemap van Kaspersky Endpoint Security bevinden.
	`AMPPL`	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 website van Microsoft. AM-PPL-technologie is beschikbaar voor de besturingssystemen Windows 10 versie 1703 (RS2) of hoger en Windows Server 2019. Beschikbare waarden: • `1` – Bescherming van de Kaspersky Endpoint Security-processen met AM-PPL-technologie is ingeschakeld. • `0` – Bescherming van de Kaspersky Endpoint Security-processen met AM-PPL-technologie is uitgeschakeld.

Gedeelte	Parameter	Beschrijving
	UPGRADEMODE	Upgrademodus programma: • Seamless betekent het upgraden van het programma met een herstart van de computer (standaardwaarde). • Force betekent het upgraden van het programma zonder een herstart. U kunt het programma upgraden zonder opnieuw te starten vanaf versie 11.10.0. Als u een eerdere versie van het programma wilt upgraden, moet u de computer opnieuw opstarten. U kunt patches installeren zonder opnieuw te starten vanaf versie 11.11.0. Opnieuw opstarten is niet nodig bij de installatie van Kaspersky Endpoint Security. De upgrademodus van het programma wordt dus gespecificeerd in de programma-instellingen. U kunt deze parameter veranderen in de programma-instellingen of in het beleid. Bij het upgraden van een reeds geïnstalleerd programma is de prioriteit van de parameter opgegeven in het bestand setup.ini hoger dan die van de parameter opgegeven in de programma-instellingen of in de opdrachtregel. Als bijvoorbeeld de upgrademodus Force is gespecificeerd in het bestand setup.ini en de modus Seamless gespecificeerd is in de programma-instellingen, dan wordt de upgrade geïnstalleerd zonder een heropstart van de computer (Force). Als u het setup.ini-bestand gebruikt, waar de parameter UPGRADEMODE niet is gespecificeerd, dan zal het installatieprogramma een standaardwaarde gebruiken (Seamless) en de upgrade installeren met een heropstart van de computer.
	SetupReg	Schakel het schrijven van registersleutels vanuit het bestand 'setup.reg' naar het register in. Waarde van de parameter SetupReg: setup.reg.
	EnableTraces	Programmatracing inschakelen of uitschakelen. Nadat Kaspersky Endpoint Security is gestart, worden de tracebestanden opgeslagen in de map %ProgramData%\Kaspersky Lab\KES.14.1\Traces. Beschikbare waarden: • 1 – tracing is ingeschakeld. • 0 – tracing is uitgeschakeld (standaardwaarde).
	TracesLevel	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.
	RESTAPI	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). Beschikbare waarden: • 1 – Beheer via de REST API is toegestaan. • 0 – Beheer via de REST API is niet toegestaan (standaardwaarde). 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.
	RESTAPI_User	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 <DOMAIN>\<UserName> in (bijvoorbeeld, RESTAPI_User=COMPANY\Administrator). U kunt slechts één gebruiker kiezen die met de REST API mag werken. Een gebruikersnaam toevoegen is een vereiste voor het beheer van het programma via de REST API.
	RESTAPI_Port	Poort die wordt gebruikt voor het beheer van het programma via de REST API. Poort 6782 wordt standaard gebruikt. Zorg ervoor dat de poort vrij is.
	RESTAPI_Certificate	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. Hiervoor moet u een certificaat installeren en vervolgens de payload van elk verzoek ondertekenen.

Gedeelte	Parameter	Beschrijving
	`StandaloneMode`	Het programma installeren in de modus Endpoint Detection and Response Agent (EDR Agent). *Endpoint Detection and Response Agent* is een programma dat wordt geïnstalleerd op individuele werkstations en servers in de IT-infrastructuur van de organisatie ter ondersteuning van de oplossingen Kaspersky Managed Detection and Response en Kaspersky Anti Targeted Attack Platform. EDR-agent compatibel met EPP-applicaties van derden. Hierdoor kunt u hulpmiddelen voor infrastructuurbeveiliging van derden gebruiken naast Detection and Response van Kaspersky. Om EDR Agent te installeren, in de sectie `[Components]`, selecteer `StandaloneKATA`, `StandaloneNDR` of `StandaloneMDR` onderdelen. EDR Agent ondersteunt geen andere programmaonderdelen. Beschikbare waarden: • `1` om het programma in de EDR Agent-modus te installeren. • `0` om het programma in de standaardmodus (standaard) te installeren.
	`KSVLAMode`	Het programma installeren in Light Agent mode. Deze configuratie is bedoeld voor het programma die wordt gebruikt als onderdeel van de Kaspersky Security for Virtualization Light Agent-oplossing. Light Agent moet worden geïnstalleerd op elke virtuele machine die met de oplossing moet worden beschermd. Beschikbare waarden: • `1` om het programma in de Light Agent-modus te installeren. • `0` om het programma in de standaardmodus (standaard) te installeren.
	`InstallOnVDI`	De VDI-beschermingsmodus inschakelen bij het installeren van het programma in de Light Agent-modus (`KSVLAMode=1`). De VDI-beschermingsmodus helpt de prestaties van Kaspersky Endpoint Security op niet-permanente virtuele machines te optimaliseren. In deze modus weigert Light Agent programma-updates waarvoor de virtuele machine opnieuw moet worden opgestart. Bij het ontvangen van programma-updates die een herstart vereisen, genereert Light Agent een event over de noodzaak om de template van de beschermde virtuele machines bij te werken. Beschikbare waarden: • `1` om de VDI-beschermingsmodus in te schakelen. • `0` om de VDI-beschermingsmodus uit te schakelen (standaard).
	`KESExclusions`	Voorgedefinieerde scanuitzonderingen en vertrouwde programma's toevoegen bij het installeren van het programma op de server. Vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's helpen bij het snel configureren van Kaspersky Endpoint Security op SQL-servers, Microsoft Exchange-servers en System Center Configuration Manager. Voorgedefinieerde scanuitzonderingen voor SQL-servers omvatten bijvoorbeeld MDF- en LDF-databasebestanden. Dit betekent dat u niet handmatig een vertrouwde zone voor het programma op servers hoeft in te stellen. Beschikbare waarden: • `1` maakt vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's • `0` schakelt vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's uit (standaard).
	`LAExclusions`	Voorgedefinieerde scanuitzonderingen en vertrouwde programma's toevoegen bij het installeren van het programma op een virtuele machine (Light Agent-modus). Met voorgedefinieerde uitzonderingen van scans en vertrouwde programma's kunt u Kaspersky Endpoint Security snel configureren in Citrix- en VMware-virtuele omgevingen. Beschikbare waarden: • `1` maakt vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's • `0` schakelt vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's uit (standaard).

Gedeelte	Parameter	Beschrijving
	`EnableUniqueSensorID`	Het aanmaken van een unieke computer-ID (Sensor ID) tijdens de installatie of update van het programma. (Sensor ID) wordt in de oplossing Kaspersky Anti Targeted Attack Platform gebruikt om computers te identificeren die telemetrie naar de server sturen. Bij het aanmaken van (Sensor ID) gebruikt het programma een algoritme dat rekening houdt met de configuratie van de computer, zoals het serienummer van het moederbord. In sommige gevallen, bijvoorbeeld wanneer het programma in een virtuele omgeving wordt gebruikt, kan (Sensor ID) worden gedupliceerd. Hierdoor kan het Kaspersky Anti Targeted Attack Platform niet identificeren vanaf welke computer de telemetrie wordt verzonden. Om een unieke (Sensor ID) te maken, moet u de parameter `EnableUniqueSensorID=1` instellen. Als gevolg hiervan zal de applicatie een ander algoritme gebruiken om de (Sensor ID) te maken, die rekening houdt met andere gegevens over de computer. Dit zorgt voor een unieke (Sensor ID). Standaard is de parameter niet ingesteld. Het programma erft de (Sensor ID) in de volgende gevallen: • De versie van het programma bijwerken; • de [KES+KEA]-configuratie migreren naar [KES+built-in agent]. Als onderdeel van het programmaherstel probeert het installatieprogramma de Sensor ID over te nemen. Als de Sensor ID niet kan worden hersteld, maakt het programma een nieuwe Sensor ID.
	`CitrixCompatibility`	Ondersteuning voor Citrix Provisioning Services inschakelen om Kaspersky Endpoint Security op een virtuele machine te installeren.
`[Components]`	`ALL`	Installatie van alle onderdelen. Als parameterwaarde `1` is opgegeven, worden alle onderdelen geïnstalleerd ongeacht de installatie-instellingen van individuele onderdelen. Vanwege de manier waarop Detection and Response-oplossingen worden ondersteund, Endpoint Detection and Response Optimum en Sandbox onderdelen op de computer zijn geïnstalleerd. Het Endpoint Detection and Response Expert (cloud) onderdeel is niet compatibel met deze configuratie.
	`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.
	`CloudDiscovery`	Cloud Discovery.
	`LogInspector`	Log Inspectie
	`AntiCryptor`	Anti-Cryptor
	`FileThreatProtection`	File Threat Protection.
	`SystemIntegrityMonitor`	Systeemintegriteitscontrole.
	`FileEncryption`	File Level Encryption-bibliotheken.
	`DiskEncryption`	Full Disk Encryption-bibliotheken.
	`MSBitLocker`	Beheerbibliotheken voor BitLocker-versleuteling.
	`BadUSBAttackPrevention`	BadUSB Attack Prevention.

Gedeelte	Parameter	Beschrijving
	`EDR`	Endpoint Detection and Response Optimum Het onderdeel is niet compatibel met de Endpoint Detection and Response Expert (cloud) (`EDRCloud`) en Endpoint Detection and Response Expert (on-premises) (`AntiAPT`) onderdelen.
	`EDRCloud`	Endpoint Detection and Response Expert (cloud) Het onderdeel is niet compatibel met de Endpoint Detection and Response Optimum (`EDR`) en Endpoint Detection and Response Expert (on-premises) (`AntiAPT`) onderdelen.
	`AntiAPT`	Endpoint Detection and Response Expert (on-premises) Het onderdeel is niet compatibel met de Endpoint Detection and Response Expert (cloud) (`EDRCloud`) en Endpoint Detection and Response Optimum (`EDR`) onderdelen.
	`SB`	Kaspersky Sandbox of KATA Sandbox. *Kaspersky Sandbox* is een zelfstandige Detection and Response-oplossing van Kaspersky. *KATA Sandbox* is een onderdeel van de Kaspersky Anti Targeted Attack Platform-oplossing.
	`MDR`	Managed Detection and Response
	`NDR`	Network Detection and Response (KATA) Het onderdeel is niet compatibel met de Endpoint Detection and Response Expert (cloud) (`EDRCloud`) en Endpoint Detection and Response Optimum (`EDR`) onderdelen.
	`AdminKitConnector`	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. Beschikbare waarden: • `1` – Programmabeheer met behulp van beheersystemen is toegestaan (standaardwaarde). • `0` – Programmabeheer is alleen via de lokale interface toegestaan.
	`KUMAIntegration`	Integratie met KUMA.
	`StandaloneKATA`	Het programma installeren in de Endpoint Detection and Response Agent (EDR Agent)-modus voor integratie met Kaspersky Anti Targeted Attack Platform (EDR).
	`StandaloneMDR`	Het programma installeren in de Endpoint Detection and Response Agent (EDR Agent)-modus voor integratie met Kaspersky Managed Detection and Response.
	`StandaloneNDR`	Het programma installeren in de Endpoint Detection and Response Agent (EDR Agent)-modus voor integratie met Kaspersky Anti Targeted Attack Platform (NDR).
	`StandaloneSiemTelemetry`	Het programma installeren in de Endpoint Detection and Response Agent (EDR Agent)-modus voor integratie met KUMA.
`[Tasks]`	`ScanMyComputer`	De taak Volledige Scan. Beschikbare waarden: • `1` – De taak wordt aan de lijst met taken van Kaspersky Endpoint Security toegevoegd. • `0` – De taak wordt niet aan de lijst met taken van Kaspersky Endpoint Security toegevoegd.
	`ScanCritical`	De taak Kritieke Gebiedenscan. Beschikbare waarden: • `1` – De taak wordt aan de lijst met taken van Kaspersky Endpoint Security toegevoegd. • `0` – De taak wordt niet aan de lijst met taken van Kaspersky Endpoint Security toegevoegd.

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

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.

  > Deze methode is niet beschikbaar als het programma is geïnstalleerd via Kaspersky Security Center. U kunt de selectie van programmaonderdelen in het Configuratiescherm alleen wijzigen nadat u het programma lokaal hebt geïnstalleerd.

- 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.

- Als het programma in de Light Agent-modus in een VDI-infrastructuur is geïnstalleerd, wordt het wijzigen van de ingestelde onderdelen niet ondersteund.

Programmaonderdelen toevoegen of verwijderen in de Beheerconsole (MMC)

1. Selecteer **Tasks** in de structuur van de Beheerconsole van Kaspersky Security Center.

   De lijst met taken wordt geopend.

2. Klik op **New task**.

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

Stap 1. Een taaktype selecteren

Selecteer **Kaspersky Endpoint Security voor Windows 14.1. → Selecteer de onderdelen die u wilt installeren**.

Stap 2: Taakinstellingen voor het wijzigen van programmaonderdelen

Selecteer de configuratie van het programma:

- **Standaardmodus om hosts te beschermen**. De standaardconfiguratie. Met deze configuratie kunt u alle onderdelen van het programma gebruiken, inclusief onderdelen die ondersteuning bieden voor Detection and Response-oplossingen. Deze configuratie wordt gebruikt voor uitgebreide bescherming van de computer tegen verschillende bedreigingen, netwerkaanvallen en fraude.

- **Endpoint Detection and Response Agent ter bescherming tegen geavanceerde bedreigingen en gerichte aanvallen**. In deze configuratie kunt u alleen de onderdelen installeren die ondersteuning bieden voor Detection and Response-oplossingen: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), evenals KUMA. Deze configuratie is nodig als een Endpoint Protection Platform (EPP) van derden wordt geïmplementeerd in uw organisatie naast een Kaspersky Detection and Response-oplossing. Hierdoor is Kaspersky Endpoint Security in de Endpoint Detection and Response Agent-configuratie compatibel met EPP-programma's van derden.

  Wanneer u de programmaconfiguratie voor de werking van de EDR-agent met MDR wijzigt, moet u ervoor zorgen dat de onderdelen die verantwoordelijk zijn voor het ontvangen van telemetrie zijn ingeschakeld.

- **Light Agent om virtuele omgevingen te beschermen**. Deze configuratie is bedoeld voor het programma die wordt gebruikt als onderdeel van de Kaspersky Security for Virtualization Light Agent-oplossing. Light Agent moet worden geïnstalleerd op elke virtuele machine die met de oplossing moet worden beschermd. In deze configuratie kunt u geen Onderdelen voor gegevensencryptie of Adaptieve controle op afwijkingen gebruiken. Als u Light Agent installeert op een virtuele machinesjabloon die zal worden gebruikt om *niet-permanente virtuele machines* te maken, schakel dan het selectievakje **Bescherm VDI-infrastructuur** (VDI staat voor Virtual Desktop Infrastructure). De VDI-beschermingsmodus helpt de prestaties van Kaspersky Endpoint Security op niet-permanente virtuele machines te optimaliseren. In deze modus weigert Light Agent programma-updates waarvoor de virtuele machine opnieuw moet worden opgestart. Bij het ontvangen van programma-updates die een herstart vereisen, genereert Light Agent een event over de noodzaak om de template van de beschermde virtuele machines bij te werken.

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

Stap 3. Geavanceerde instellingen

Configureer de geavanceerde instellingen voor de taak (zie onderstaande tabel).

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. Een taakstartschema configureren

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

Stap 6. Taaknaam definiëren

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

Stap 7. Aanmaak van de taak voltooien

Verlaat de wizard verlaten. Schakel indien nodig het selectievakje **Run the task after the wizard finishes** in. U kunt de voortgang van de taak volgen in de taakeigenschappen.

Programmaonderdelen toevoegen of verwijderen in de Webconsole en Cloudconsole

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

   De lijst met taken wordt geopend.

2. Klik op **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** de optie **Kaspersky Endpoint Security for Windows 14.1.0**.
2. Selecteer in de vervolgkeuzelijst **Task type** de optie **Change application components**.
3. Typ in het veld **Task name** een korte omschrijving, zoals *Het onderdeel Programmacontrole toevoegen*.
4. Selecteer in het gedeelte **Devices to which the task will be assigned** 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 **Open task details when creation is complete** in en voltooi de wizard.

Selecteer het tabblad **Application settings** in de taakeigenschappen. Vervolgens, selecteer de configuratie van het programma:

- **Standard mode to protect workstations and servers**. De standaardconfiguratie. Met deze configuratie kunt u alle onderdelen van het programma gebruiken, inclusief onderdelen die ondersteuning bieden voor Detection and Response-oplossingen. Deze configuratie wordt gebruikt voor uitgebreide bescherming van de computer tegen verschillende bedreigingen, netwerkaanvallen en fraude.

- **Endpoint Detection and Response Agent to protect against advanced threats and targeted attacks**. In deze configuratie kunt u alleen de onderdelen installeren die ondersteuning bieden voor Detection and Response-oplossingen: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), evenals KUMA. Deze configuratie is nodig als een Endpoint Protection Platform (EPP) van derden wordt geïmplementeerd in uw organisatie naast een Kaspersky Detection and Response-oplossing. Hierdoor is Kaspersky Endpoint Security in de Endpoint Detection and Response Agent-configuratie compatibel met EPP-programma's van derden.

  Wanneer u de programmaconfiguratie voor de werking van de EDR-agent met MDR wijzigt, moet u ervoor zorgen dat de onderdelen die verantwoordelijk zijn voor het ontvangen van telemetrie zijn ingeschakeld.

- **Light Agent to protect virtual environments**. Deze configuratie is bedoeld voor het programma die wordt gebruikt als onderdeel van de Kaspersky Security for Virtualization Light Agent-oplossing. Light Agent moet worden geïnstalleerd op elke virtuele machine die met de oplossing moet worden beschermd. In deze configuratie kunt u geen Onderdelen voor gegevensencryptie of Adaptieve controle op afwijkingen gebruiken. Als u Light Agent installeert op een virtuele machinesjabloon die zal worden gebruikt om *niet-permanente virtuele machines* te maken, schakel dan het selectievakje **Protect VDI infrastructure** (VDI staat voor Virtual Desktop Infrastructure). De VDI-beschermingsmodus helpt de prestaties van Kaspersky Endpoint Security op niet-permanente virtuele machines te optimaliseren. In deze modus weigert Light Agent programma-updates waarvoor de virtuele machine opnieuw moet worden opgestart. Bij het ontvangen van programma-updates die een herstart vereisen, genereert Light Agent een event over de noodzaak om de template van de beschermde virtuele machines bij te werken.

Selecteer de programmaonderdelen die beschikbaar zullen zijn op de computer van de gebruiker. Configureer de geavanceerde instellingen voor de taak (zie onderstaande tabel).

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.

Bij het installeren, bijwerken of verwijderen van Kaspersky Endpoint Security kunnen fouten optreden. Raadpleeg voor meer informatie over het oplossen van deze fouten de Knowledge Base van de Technische Support.

Parameter	Beschrijving
Taakinstellingen	**Controleer op incompatibele programma's van derden**. Standaard is Kaspersky Endpoint Security controleert geïnstalleerde programma's op compatibiliteit. De lijst met software die compatibiliteitsproblemen kan veroorzaken, is te vinden in het bestand incompatible.txt. Het bestand is inbegrepen in de distributiekit. Als de scan van geïnstalleerde software is ingeschakeld en een programma uit de lijst wordt gedetecteerd, stopt Kaspersky Endpoint Security de taak. U kunt de scan van geïnstalleerde software uitschakelen als de documentatie van de leverancier van de software van derden claimt dat deze compatibel is met: Endpoint Protection Platform (EPP). **Incompatibele programma's van derden verwijderen**. Programma's automatisch verwijderen die genoemd worden in het bestand incompatible.txt voordat u de set onderdelen wijzigt. Als deze functionaliteit is ingeschakeld, probeert Kaspersky Endpoint Security de programma's te verwijderen die compatibiliteitsproblemen kunnen veroorzaken om de taak voort te zetten. **Azure WVD compatibiliteitsmodus gebruiken**. Deze functie garandeert een correcte weergave van de status van de Azure virtuele machine in de console van Kaspersky Anti Targeted Attack Platform. Om de prestaties van de computer te controleren, verzendt Kaspersky Endpoint Security telemetrie naar KATA-servers. Telemetrie omvat een ID van de computer (Sensor ID). Met de Azure WVD-compatibiliteitsmodus kunt u een permanente unieke Sensor ID toewijzen aan deze virtuele machines. Als de compatibiliteitsmodus is uitgeschakeld, kan de Sensor ID veranderen nadat de computer opnieuw is opgestart vanwege de manier waarop virtuele Azure-machines werken. Dit kan er voor zorgen dat duplicaten van virtuele machines op de console worden weergegeven.
Uitzonderingen	Beginnend met Kaspersky Endpoint Security 12.6 voor Windows, uitzonderingen scannen en vertrouwde programma's worden toegevoegd aan de vertrouwde zone. Vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's helpen bij het snel configureren van Kaspersky Endpoint Security op SQL-servers, Microsoft Exchange-servers en System Center Configuration Manager. Dit betekent dat u niet handmatig een vertrouwde zone voor het programma op servers hoeft in te stellen. Vanaf Kaspersky Endpoint Security 12.8 voor Windows kun je het programma in Light Agent-modus installeren om virtuele omgevingen te beschermen. Met voorgedefinieerde uitzonderingen van scans en vertrouwde programma's kunt u Kaspersky Endpoint Security snel configureren in Citrix- en VMware-virtuele omgevingen. U kunt de vertrouwde zone ook later configureren in de beleidseigenschappen: scanuitzonderingen en vertrouwde programma's.
Aparte modus / Gecombineerde modus	U kunt afzonderlijke sets onderdelen voor werkstations en servers maken – **Aparte modus**. Voordat het installatiepakket wordt geïmplementeerd, detecteert het installatieprogramma het type besturingssysteem en installeert het alleen de programmaonderdelen die u voor dat type besturingssysteem hebt geselecteerd. Op deze manier kunt u hetzelfde installatiepakket gebruiken voor werkstations en servers. **Gecombineerde modus** biedt een algemene lijst met onderdelen voor werkstations en servers. De beschikbaarheid van afzonderlijke onderdelen is afhankelijk van het type besturingssysteem. In deze modus raden wij aan om een apart installatiepakket voor werkstations en een apart installatiepakket voor servers te maken. U kunt de algemene lijst met onderdelen in het installatiepakket alleen in de standaardmodus configureren.
Wachtwoord gebruiken voor het wijzigen van de set van programma-onderdelen	Beheerders schakelen doorgaans wachtwoordbeveiliging in om de toegang tot Kaspersky Endpoint Security te beperken. Dat wil zeggen, om de selectie van programmaonderdelen te wijzigen, moet u referenties invoeren van een gebruiker met de machtiging **Programma verwijderen/wijzigen/herstellen**. U kunt bijvoorbeeld het KL Admin-account gebruiken.
Gebruik het wachtwoord om Kaspersky Endpoint Agent en Kaspersky Security for Windows Server te verwijderen	Beheerders schakelen wachtwoordbeveiliging meestal in voor de instellingen van deze taken om de toegang tot Kaspersky Endpoint Agent (KEA) en Kaspersky Security for Windows Server (KSWS) te beperken. Dat wil zeggen, als u migreert van de [KES+KEA]-configuratie naar [KES+ingebouwde agent], of als u migreert van KSWS naar KES, moet u een wachtwoord invoeren om deze programma's te verwijderen.

Een oude versie van het programma upgraden

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

- De lokalisering van de nieuwe versie van Kaspersky Endpoint Security moet overeenkomen met de lokalisering van de geïnstalleerde versie van het programma. Als lokaliseringen van de programma's niet overeenkomen, zal de programma-update voltooien met een fout.
- We raden aan dat u alle actieve programma's afsluit voordat u met de installatie van de update begint.
- 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 12.1 voor Windows (build 12.1.0.506)
- Kaspersky Endpoint Security 12.2 voor Windows (build 12.2.0.462)
- Kaspersky Endpoint Security 12.3 voor Windows (build 12.3.0.493)
- Kaspersky Endpoint Security 12.4 voor Windows (build 12.4.0.467)
- Kaspersky Endpoint Security 12.5 voor Windows (build 12.5.0.539)
- Kaspersky Endpoint Security 12.6 voor Windows (build 12.6.0.438)
- Kaspersky Endpoint Security 12.7 voor Windows (build 12.7.0.533)
- Kaspersky Endpoint Security 12.8 voor Windows (build 12.8.0.505)
- Kaspersky Endpoint Security 12.9 voor Windows (build 12.9.0.384)
- Kaspersky Endpoint Security 12.10 voor Windows (build 12.10.0.466)
- Kaspersky Endpoint Security 12.11 voor Windows (build 12.11.0.637)
- Kaspersky Endpoint Security 12.12 voor Windows (build 12.12.0.522)
- Kaspersky Endpoint Security 14.0 voor Windows (build 14.0.0.504)

Bij het installeren, bijwerken of verwijderen van Kaspersky Endpoint Security kunnen fouten optreden. Raadpleeg voor meer informatie over het oplossen van deze fouten de Knowledge Base van de Technische Support.

Upgrademethodes programma

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

- Met Kaspersky-updateservice (Seamless Update – SMU).
- 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.

Het programma upgraden zonder een herstart

Het upgraden van de applicatie zonder herstarten zorgt voor een ononderbroken werking van de server tijdens het bijwerken van de programmaversie.

Het upgraden van het programma zonder een herstart heeft de volgende beperkingen:

- U kunt het programma upgraden zonder opnieuw te starten vanaf versie 11.10.0. Als u een eerdere versie van het programma wilt upgraden, moet u de computer opnieuw opstarten.
- U kunt patches installeren zonder herstarten vanaf versie 11.11.0. Om patches voor eerdere versies van het programma te installeren, kan het nodig zijn de computer opnieuw op te starten.
- Het programma upgraden zonder opnieuw te starten is niet beschikbaar op computers met ingeschakelde gegevensencryptie (Kaspersky-encryptie (FDE), BitLocker, File Level Encryption (FLE)). Om het programma te upgraden op computers met ingeschakelde gegevenscodering, moet de computer opnieuw worden opgestart.
- Het programma kan niet worden geüpgraded op een virtuele machine zonder een herstart. Als u het programma op een virtuele machine wilt upgraden, moet u de virtuele machine opnieuw opstarten.

Na de upgrade van het programma, de installatie van een patch, de wijziging van de set programma-onderdelen of de herstelbewerking, wordt Kaspersky Endpoint Security opnieuw gestart om de nieuwe versie te gebruiken. Het herstarten van Kaspersky Endpoint Security kan een minuut duren. Tijdens deze tijd is de computer minder beschermd. Na de herstart van het programma wordt het beschermingsniveau van de computer hersteld.

De upgrademodus van de programma-interface configureren in de Beheerconsole (MMC)

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.

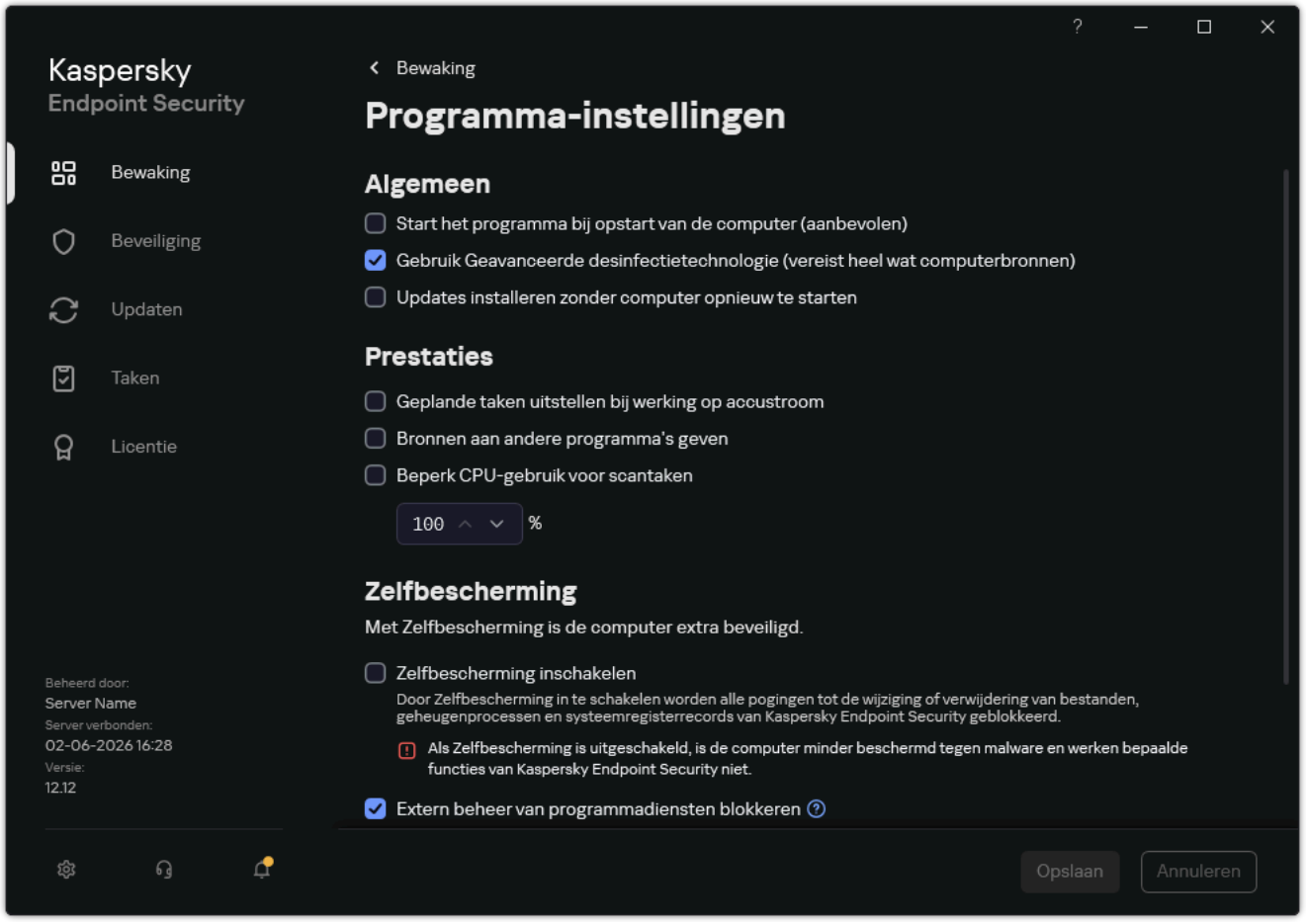
   U ziet nu het venster met de beleidseigenschappen.

3. Selecteer het tabblad **Application settings**.
4. Ga naar **General Settings** → **User Interaction**.
5. Schakel in het blok **Application update settings** het selectievakje **Install application updates without restart** in of uit om de upgrademodus voor het programma te configureren.
6. Sla uw wijzigingen op.

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Algemene instellingen** → **Programma-instellingen** in het beleidsvenster.
4. Schakel in het blok **Geavanceerde instellingen** het selectievakje **Installeer programma-updates zonder opnieuw op te starten** in of uit om de upgrademodus voor het programma te configureren.
5. Sla uw wijzigingen op.

De upgrademodus van het programma selecteren 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.



Instellingen Kaspersky Endpoint Security voor Windows

3. Schakel in het blok **Algemeen** het selectievakje **Updates installeren zonder computer opnieuw te starten** in of uit om de upgrademodus voor het programma te configureren.

4. Sla uw wijzigingen op.

Nadat de upgradeprocedure voor het programma zonder herstart is voltooid, is de nieuwe versie van Kaspersky Endpoint Security geïnstalleerd op de computer. De vorige versie van het programma wordt automatisch verwijderd.

U kunt geen programma-upgrade starten voordat de vorige upgrade volledig is voltooid.

U kunt de Kaspersky Endpoint Security-upgrade status controleren met behulp van het Kaspersky-programmaversierapport in de Kaspersky Security Center-console.

SMU-update van het programma

Om het programma bij te werken met de Kaspersky-updateservice Seamless Update; SMU), hoeft u het installatieprogramma niet uit te voeren, in tegenstelling tot andere updatemethoden. Kaspersky Endpoint Security ontvangt de nieuwe versie van het programma samen met antivirusdatabases van dezelfde bron.

Met een SMU-update kunt u het programma op alle computers in uw organisatie bijwerken naar de nieuwste versie. Voordat u een SMU-update toepast, raden wij u aan de nieuwe versie van het programma op een aantal computers te testen. Om dit te doen, moet u het programma op deze computers handmatig bijwerken (bijvoorbeeld lokaal met behulp van de Installatiewizard). U kunt geen afzonderlijke computers selecteren bij het uitvoeren van een SMU-update.

Het updateschema voor het programma wordt bepaald door medewerkers van Kaspersky. Om ervoor te zorgen dat de nieuwe versie van het programma soepel werkt, stelt Kaspersky updates stapsgewijs beschikbaar. Dit betekent dat u uw SMU-update maximaal twee maanden later kunt ontvangen dan de release van een nieuwe versie.

U kunt de SMU-update van het programma beheren met de taak *Update van databases en programmamodules*. Om de nieuwe versie van het programma in hetzelfde pakket als de antivirusdatabases op te nemen, moet u het bijwerken van *programmamodules* toestaan in de taakinstellingen *Update van databases en programmamodules*. Ook in de taakinstellingen voor het *Update van databases en programmamodules* kunt u toestaan dat het programma wordt bijgewerkt zonder dat deze opnieuw hoeft te worden opgestart.

Stappen van een SMU-update van het programma

1. **Zodra een nieuwe versie van het programma uitkomt, verspreidt Kaspersky de update.**

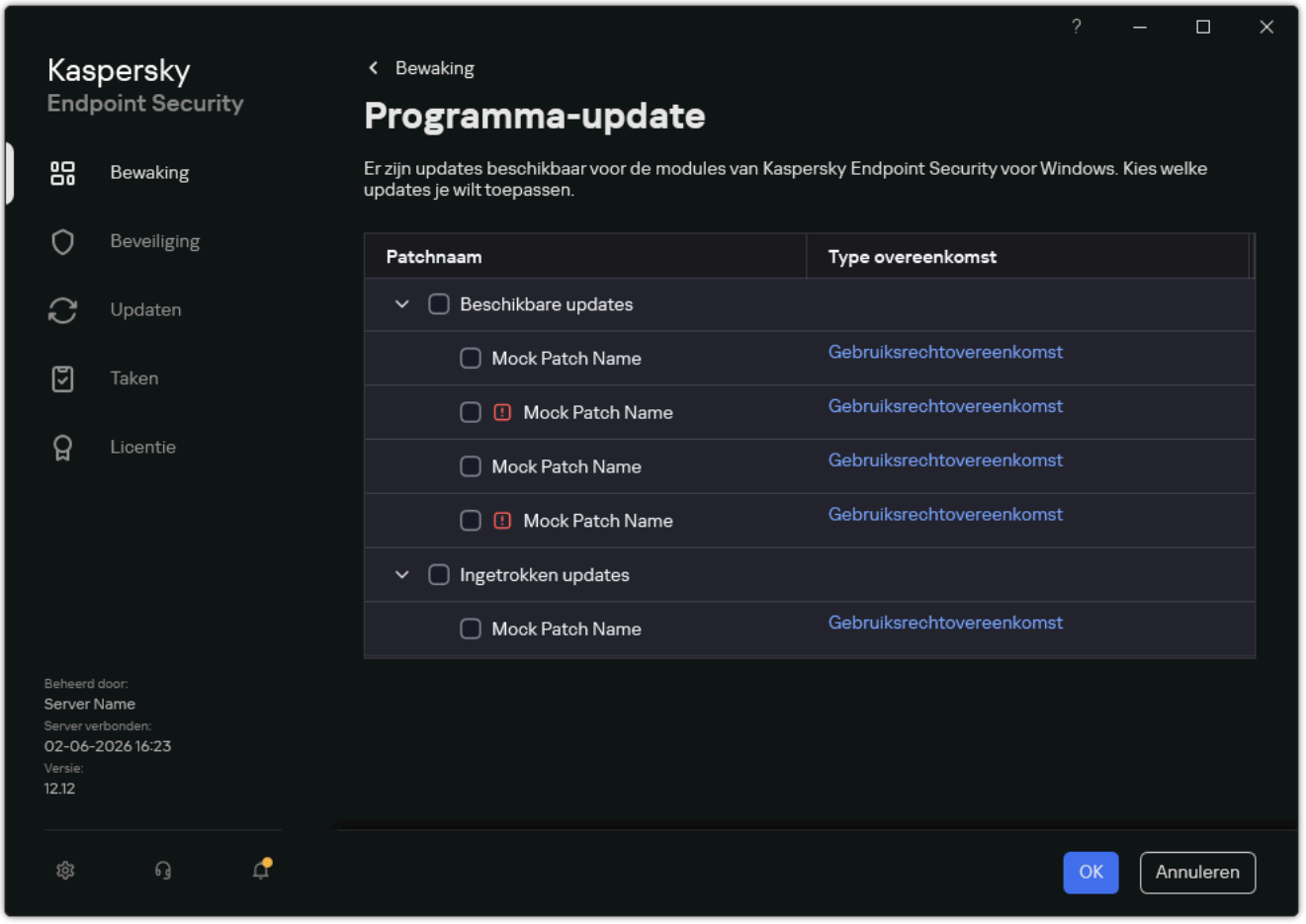
2. **De gebruiker keurt de update van het programma goed.**

   Als de computer is verbonden met Kaspersky Security Center, is de update beschikbaar in Kaspersky Security Center, in het gedeelte **Update of Kaspersky databases and application modules**. Voor meer informatie over selecties van gebeurtenissen raadpleegt u de Help van Kaspersky Security Center.

   Als de computer niet is verbonden met Kaspersky Security Center, is de update beschikbaar in het gedeelte voor meldingen van de interface van het programma: . Om de update goed te keuren, selecteer een versie van het programma en accepteer de algemene voorwaarden van de overeenkomsten (zie de onderstaande afbeelding).

3. **Kaspersky Endpoint Security voert de taak *Update van databases en programmamodules* uit volgens het geconfigureerde schema.**

Als gevolg hiervan werkt Kaspersky Endpoint Security het programma bij in "stille" modus.



Beschikbare programma-updates

Programma verwijderen

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

Bij het installeren, bijwerken of verwijderen van Kaspersky Endpoint Security kunnen fouten optreden. Raadpleeg voor meer informatie over het oplossen van deze fouten de Knowledge Base van de Technische Support.

Het programma op afstand verwijderen via Kaspersky Security Center:

U kunt het programma op afstand verwijderen met behulp van de taak *Uninstall application remotely*. 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. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de beheerconsole **Tasks**.

   De lijst met taken wordt geopend.
3. Klik op **New task**.

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

Stap 1. Een taaktype selecteren

Selecteer **Kaspersky Security Center Administration Server → Advanced → Uninstall application remotely**.

Stap 2: Het programma selecteren dat moet worden verwijderd

Selecteer **Uninstall application supported by Kaspersky Security Center**.

Stap 3: Taakinstellingen voor het verwijderen van programma's

Selecteer **Kaspersky Endpoint Security voor Windows (14.1)**.

Stap 4. Verwijder hulpprogramma-instellingen

Configureer de volgende aanvullende programma-instellingen:

- **Force download of the uninstallation utility**. Selecteer de leveringsmethode voor het hulpprogramma:
  - **Using Network Agent**. 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.
  - **Using operating system resources through 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.
  - **Using operating system resources through distribution points**. 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.
- **Verify operating system type before downloading**. 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. Selecteer het selectievakje **Use uninstallation password**.
2. Klik op de knop **Edit**.
3. Voer het wachtwoord van het KLAdmin-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 14.1 verwijderen*.

Stap 10. Aanmaak van de taak voltooien

Verlaat de wizard verlaten. Schakel indien nodig het selectievakje **Run the task after the wizard finishes** 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 **Tasks**.
   De lijst met taken wordt geopend.
2. Klik op **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** de optie **Kaspersky Security Center**.
2. Selecteer in de vervolgkeuzelijst **Task type** de optie **Uninstall application remotely**.
3. Typ in het veld **Task name** een korte omschrijving, zoals *Kaspersky Endpoint Security verwijderen op computers van Technische Support*.
4. Selecteer in het gedeelte **Devices to which the task will be assigned** 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 het type **Uninstall managed application**.
2. Selecteer **Kaspersky Endpoint Security for Windows**.

3. **Force download of the uninstallation utility**. Selecteer de leveringsmethode voor het hulpprogramma:

   - **Using Network Agent**. 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.

   - **Using operating system resources through 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.

   - **Using operating system resources through distribution points**. 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.

4. Stel in het veld **Maximum number of concurrent 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 number of uninstallation attempts** 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 **Verify operating system type before downloading** 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 **Start** 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 *Uninstall application remotely* in. Zonder het wachtwoord wordt de taak niet uitgevoerd.

Zo gebruikt u het wachtwoord van het KLAdmin-account met de taak Uninstall application remotely:

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

   De lijst met taken wordt geopend.

2. Klik op de taak **Uninstall application remotely** van Kaspersky Security Center.

   U ziet nu het venster met de taakeigenschappen.

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

4. Selecteer het selectievakje **Use uninstallation password**.

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

6. Sla uw wijzigingen op.

Start de computer opnieuw op om de verwijdering te voltooien. Om dit te doen, geeft netwerkagent een pop-upvenster weer.

De toepassing op afstand verwijderen met Active Directory

U kunt het programma op afstand verwijderen met behulp van een Microsoft Windows-groepsbeleid. Om het programma te verwijderen, moet u de groepsbeleidsbeheerconsole (gpmc.msc) openen en de groepsbeleid-editor gebruiken om een verwijderingstaak voor het programma te maken (ga voor meer informatie naar de website voor technische support van Microsoft).

Als het verwijderen van het programma met een wachtwoord is beveiligd, moet u het volgende doen:

1. Maak een BAT-bestand aan met de volgende inhoud:

   ```
   msiexec.exe /x<GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
   ```

   `<GUID>` is de unieke ID van het programma. U kunt de GUID van het programma vinden in de Knowledge Base van de Technische Support of de volgende opdracht te gebruiken:

   ```
   wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
   ```

   Voorbeeld

   ```
   msiexec.exe /x{6BB76C8F-365E-4345-83ED-6D7AD612AF76} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
   ```

2. Maak een nieuw Microsoft Windows-beleid voor de computers in de groepsbeleidbeheerconsole (gpmc.msc).

3. Gebruik het nieuwe beleid om het gemaakte BAT-bestand op de computers uit te voeren.

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.



Het verwijderen van programma selecteren

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 opgeeft, wordt het programma volledig verwijderd (zie onderstaande afbeelding).



Gegevens opslaan na verwijdering

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.

Kaspersky Endpoint Security slaat gegevens op in de map `C:\ProgramData\Kaspersky Lab\KES.14.1\QB`.

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\KES\Doc\<locale>\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. Het programma kan niet worden geactiveerd onder een proeflicentie nadat het is geactiveerd met een commerciële licentie.

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

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

Wanneer de commerciële licentie verloopt, 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 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:

- Licentie-ID 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.
- Haal een sleutelbestand op van een andere beheerserver.

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 de programmafunctionaliteit afhankelijk van het Kaspersky Next-licentietype, zie Kaspersky Next Help.

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 Optimum Security	Kaspersky Endpoint Detection and Response Expert	Ka S S
Advanced Threat Protection							
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	
Gedragsdetectie	✓	✓	✓	✓	✓	✓	
Anti-Cryptor	✓	✓	✓	✓	✓	✓	
Exploit-preventie	✓	✓	✓	✓	✓	✓	
Host Intrusion Prevention	✓	✓	✓	✓	✓	✓	
Remediation Engine	✓	✓	✓	✓	✓	✓	
Essential Threat Protection							
File Threat Protection	✓	✓	✓	✓	✓	✓	
Web Threat Protection	✓	✓	✓	✓	✓	✓	
Mail Threat Protection	✓	✓	✓	✓	✓	✓	
Firewall	✓	✓	✓	✓	✓	✓	
Network Threat Protection	✓	✓	✓	✓	✓	✓	
BadUSB Attack Prevention	✓	✓	✓	✓	✓	✓	
AMSI-bescherming	✓	✓	✓	✓	✓	✓	
Security Controls							
Log Inspectie	–	–	–	–	–	–	
Programmacontrole	✓	✓	✓	✓	✓	✓	
Apparaatcontrole	✓	✓	✓	✓	✓	✓	
Webcontrole	✓	✓	✓	✓	✓	✓	
Adaptieve controle op afwijkingen	–	✓	✓	✓	✓	✓	
Systeemintegriteitscontrole	–	–	–	–	–	–	
Gegevensencryptie							

Functie	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Ka S S
Kaspersky Disk Encryption	–	✓	✓	✓	✓	✓	
BitLocker-stationsversleuteling	–	✓	✓	✓	✓	✓	
File Level Encryption	–	✓	✓	✓	✓	✓	
Encryptie van verwisselbare schijven	–	✓	✓	✓	✓	✓	
Detection and Response							
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	
Endpoint Detection and Response Expert	–	–	–	–	–	✓	
Kaspersky Sandbox *(Kaspersky Sandbox-licentie moet afzonderlijk worden aangekocht)*	✓	✓	✓	✓	✓	✓	
Integratie met KUMA *(licentie voor KUMA-integratie moet apart worden aangeschaft)*	✓	✓	✓	✓	✓	✓	
Light Agent-modus *(om het programma te activeren, moet u een licentiesleutel toevoegen aan de SVM waarmee de Light Agent is verbonden)*	–	–	–	–	–	–	

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

Vergelijking van de programmafunctionaliteit afhankelijk van het Kaspersky Next-licentietype, zie Kaspersky Next Help.

Functie	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Ka
Advanced Threat Protection							
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	
Gedragsdetectie	✓	✓	✓	✓	✓	✓	
Anti-Cryptor	✓	✓	✓	✓	✓	✓	
Exploit-preventie	✓	✓	✓	✓	✓	✓	
Host Intrusion Prevention	–	–	–	–	–	–	
Remediation Engine	✓	✓	✓	✓	✓	✓	
Essential Threat Protection							
File Threat Protection	✓	✓	✓	✓	✓	✓	
Web Threat Protection	–	✓	✓	✓	✓	✓	
Mail Threat Protection	–	✓	✓	✓	✓	✓	
Firewall	✓	✓	✓	✓	✓	✓	
Network Threat Protection	✓	✓	✓	✓	✓	✓	
BadUSB Attack Prevention	✓	✓	✓	✓	✓	✓	
AMSI-bescherming	✓	✓	✓	✓	✓	✓	
Security Controls							
Log Inspectie	–	–	–	–	–	–	
Programmacontrole	–	✓	✓	✓	✓	✓	
Apparaatcontrole	–	✓	✓	✓	✓	✓	
Webcontrole	–	✓	✓	✓	✓	✓	
Adaptieve controle op afwijkingen	–	–	–	–	–	–	
Systeemintegriteitscontrole	–	–	–	–	–	–	
Gegevensencryptie							
Kaspersky Disk Encryption	–	–	–	–	–	–	
BitLocker-stationsversleuteling	–	✓	✓	✓	✓	✓	
File Level Encryption	–	–	–	–	–	–	
Encryptie van verwisselbare schijven	–	–	–	–	–	–	
Detection and Response							
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	
Endpoint Detection and Response Expert	–	–	–	–	–	✓	
Kaspersky Sandbox *(Kaspersky Sandbox-licentie moet afzonderlijk worden aangekocht)*	✓	✓	✓	✓	✓	✓	

Functie	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Ka S S
Integratie met KUMA *(licentie voor KUMA-integratie moet apart worden aangeschaft)*	✓	✓	✓	✓	✓	✓	
Light Agent-modus *(om het programma te activeren, moet u een licentiesleutel toevoegen aan de SVM waarmee de Light Agent is verbonden)*	–	–	–	–	–	–	

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, met behulp van de Activeringswizard. Op deze manier kunt u zowel de actieve licentie als de reservelicentie toevoegen.
- Op afstand met behulp van het Kaspersky Security Center-softwarepakket.
  - 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. Op deze manier kunt u zowel de actieve licentie als de reservelicentie toevoegen.
  - 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.

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

- 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.

- 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.

Als Kaspersky Endpoint Security in de Light Agent-modus wordt gebruikt om virtuele omgevingen te beschermen, hoeft u het programma niet afzonderlijk te activeren.

Programma activeren

Het programma activeren in de Beheerconsole (MMC)

1. Selecteer **Tasks** in de structuur van de Beheerconsole van Kaspersky Security Center.

   De lijst met taken wordt geopend.

2. Klik op **New task**.

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

Stap 1. Een taaktype selecteren

Selecteer **Kaspersky Endpoint Security voor Windows 14.1.** → **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 Kaspersky Security Center-opslagplaats raadpleegt u de Help van Kaspersky Security Center.

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 **Run the task after the wizard finishes** 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.

Het programma in de webconsole en cloudconsole activeren

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

   De lijst met taken wordt geopend.

2. Klik op **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** de optie **Kaspersky Endpoint Security for Windows 14.1.0**.
2. Selecteer in de vervolgkeuzelijst **Task type** de optie **Add key**.
3. Typ in het veld **Task name** een korte omschrijving, zoals *Activering van Kaspersky Endpoint Security voor Windows*.
4. Selecteer in het gedeelte **Devices to which the task will be assigned** 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 (**Operations → Licensing**).

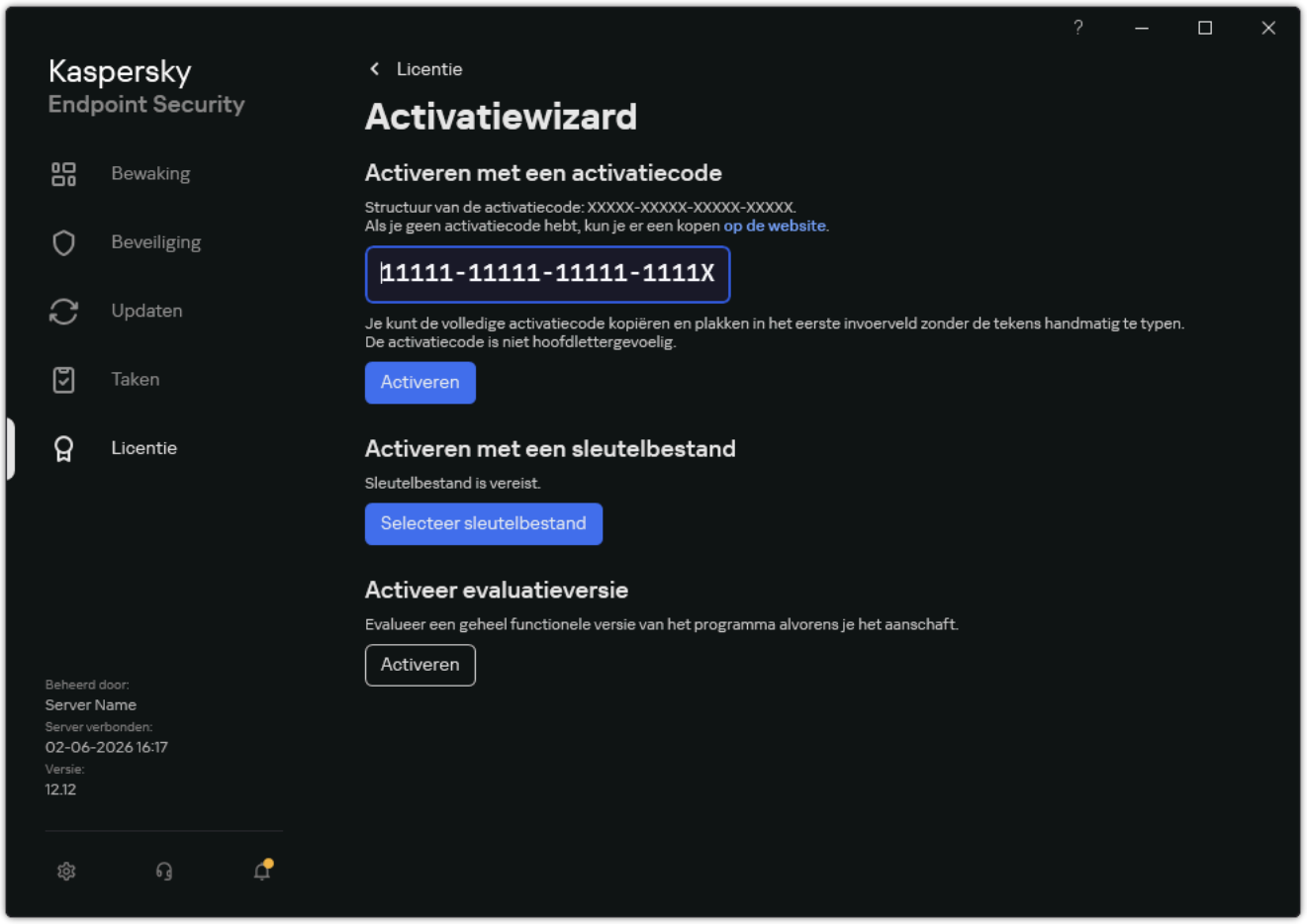
Stap 4. Aanmaak van de taak voltooien

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 **Start** te klikken. Kaspersky Endpoint Security wordt nu op de computers van de gebruikers geactiveerd in stille modus.

Het programma activeren in de programma-interface.

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.



Programma activeren

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. 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 **Kaspersky Licenses**.

   Er wordt een lijst met licentiesleutels geopend.

2. Open de eigenschappen van de licentiesleutel.

3. Schakel in het gedeelte **General** het selectievakje **Automatically distribute license key to managed devices** 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 **Devices** 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 **Operations → Licensing → Licenses**.

   Er wordt een lijst met licentiesleutels geopend.

2. Open de eigenschappen van de licentiesleutel.

3. Schakel op het tabblad **General** de **Automatically distribute license key to managed devices**-schakel 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. Op het tabblad **Devices** in de licentie-eigenschappen kunt u het aantal computers zien waaraan de licentie is toegevoegd, alsook andere gegevens.

Als je het programma met een *activeringscode* activeert, is internettoegang nodig om verbinding te maken met de activeringsservers van Kaspersky. Als je het programma met een *sleutelbestand* activeert, is internettoegang niet nodig. Als de computers zich in een geïsoleerd netwerksegment bevinden zonder internettoegang, moet je het toestaan om Kaspersky Sercurity Center Administration Server als een proxyserver.te gebruiken om het programma met een code te activeren. Dit houdt in dat het programma toegang kan krijgen tot de activeringsservers via de Administration Server die internettoegang heeft.

Het gebruik van de Administration Server als een proxyserver voor het activeren van het programma toestaan in de beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.

2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

3. Selecteer **Algemene instellingen → Programma-instellingen** in het beleidsvenster.

4. Selecteer het selectievakje **Kaspersky Security Center gebruiken als proxyserver voor activering**.

5. Sla uw wijzigingen op.

Het gebruik van de Administration Server als een proxyserver voor het activeren van het programma toestaan in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management → Policies**.

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 → KSC Integration**.

5. Selecteer het selectievakje **Use Kaspersky Security Center as proxy server for activation**.

6. Sla uw wijzigingen op.

Als je het programma niet met een *activatiecode* kunt activeren, kun je proberen een *sleutelbestand* te verkrijgen via de Kaspersky-oplossing en opnieuw proberen het programma te activeren met een andere methode.

Bewaking van licentiegebruik

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

- Bekijk het *Report on usage of license keys* in de infrastructuur van het bedrijf (**Monitoring** → **Reports**).
- Bekijk de status van computers op het tabblad **Managed devices** → **Devices**. Als het programma niet is geactiveerd, heeft de computer de status ⚠ *Programma is niet geactiveerd*.
- Bekijk licentie-informatie in de computereigenschappen.
- Bekijk sleuteleigenschappen (**Operations** → **Licensing**).

Bijzonderheden over het activeren van het programma als onderdeel van Kaspersky Security Center Cloud Console

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.

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.

Een licentiesleutel verwijderen

Om een licentiesleutel te verwijderen, moet u een speciale taak op uw computer uitvoeren. U kunt een licentiesleutel verwijderen, bijvoorbeeld om de licentie-eenheden opnieuw te ordenen. Bovendien ontvangt u van Kaspersky Endpoint Security een melding wanneer de licentie verloopt. Als u een licentiesleutel hebt toegevoegd met een korte looptijd om het programma uit te proberen (bijvoorbeeld EDR Optimum Add-on), kunt u deze licentiesleutel verwijderen om meldingen te verwijderen en de status van uw computer te herstellen.

De taak *Sleutel verwijderen* kunt u alle licentiesleutels van de computer verwijderen. U kunt actieve licentiesleutels verwijderen en licentiesleutels reserveren. Naast de activeringslicentiesleutel van Kaspersky Endpoint Security kunt u afzonderlijke licentiesleutels van Kaspersky Detection and Response-oplossingen verwijderen (bijvoorbeeld EDR Optimum Add-on).

Een licentiesleutel verwijderen in de beheerconsole (MMC)

1. Selecteer **Tasks** in de structuur van de Beheerconsole van Kaspersky Security Center.

   De lijst met taken wordt geopend.

2. Klik op **New task**.

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

Stap 1. Een taaktype selecteren

Selecteer **Kaspersky Endpoint Security voor Windows 14.1.** → **Sleutel verwijderen**.

Stap 2. Een licentie selecteren

Selecteer de licentiesleutel die u wilt verwijderen. U kunt een licentiesleutel selecteren uit de sleutelopslag van Kaspersky Security Center of een sleutelbestand selecteren.

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: *Verwijder sleutel voor bèta*.

Stap 6. Aanmaak van de taak voltooien

Verlaat de wizard verlaten. Schakel indien nodig het selectievakje **Run the task after the wizard finishes** in. U kunt de voortgang van de taak volgen in de taakeigenschappen.

Verwijder een licentiesleutel in de Webconsole

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

   De lijst met taken wordt geopend.

2. Klik op **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** de optie **Kaspersky Endpoint Security for Windows 14.1.0**.
2. Selecteer in de vervolgkeuzelijst **Task type** de optie **Remove key**.
3. Voer in het veld **Task name** een korte omschrijving, zoals *Sleutel voor bèta verwijderen*.
4. Selecteer in het gedeelte **Devices to which the task will be assigned** 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 licentiesleutel die u wilt verwijderen. U kunt een licentiesleutel selecteren uit de sleutelopslag van Kaspersky Security Center of een sleutelbestand selecteren. Ga naar de volgende stap.

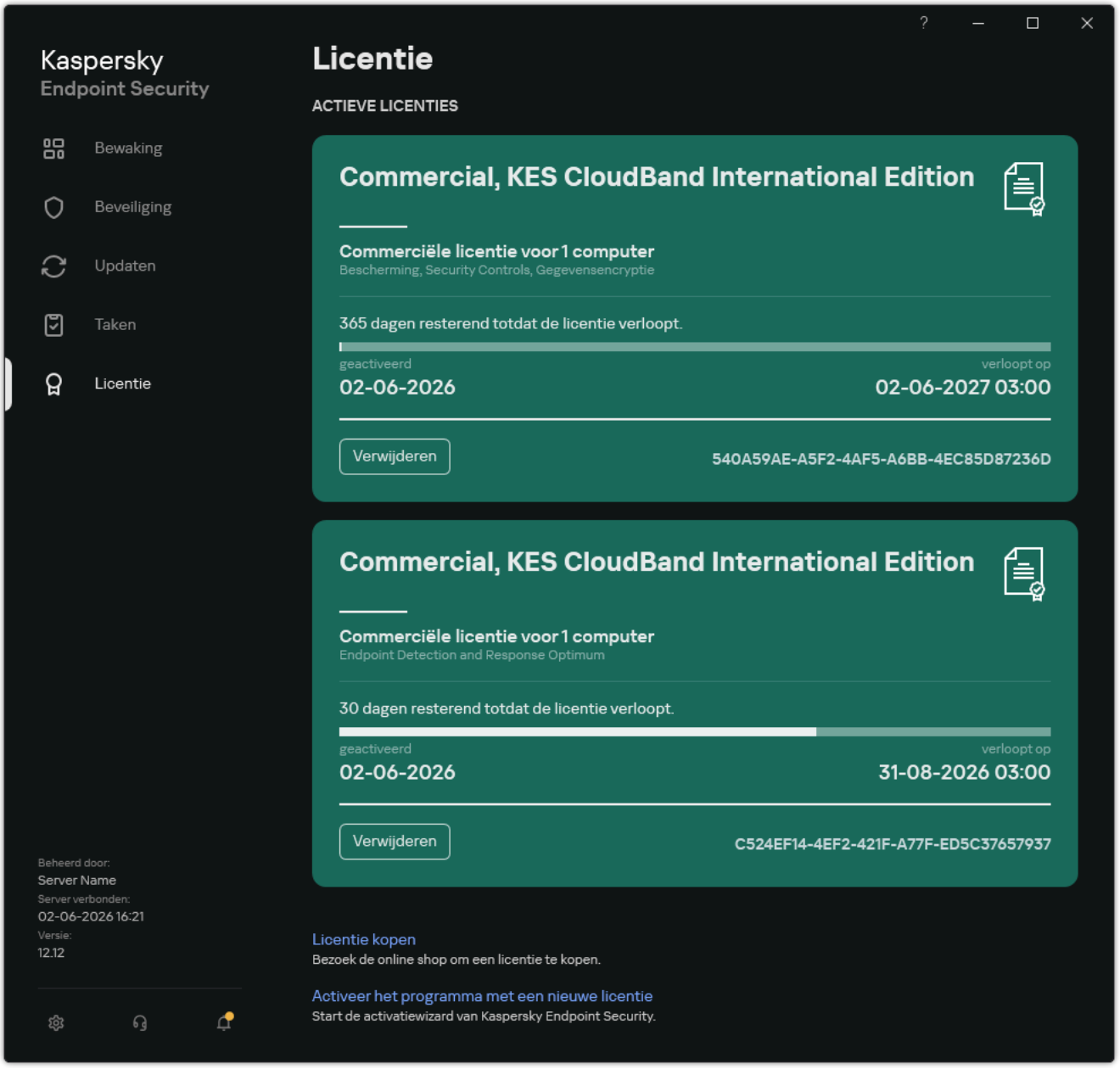
Stap 4. Aanmaak van de taak voltooien

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 **Start** te klikken.

Een aangepaste regel maken in de programma-interface

1. Ga in het hoofdvenster van het programma naar het gedeelte **Licentie**.

2. Selecteer de sleutel die u wilt verwijderen en klik op **Verwijderen**.



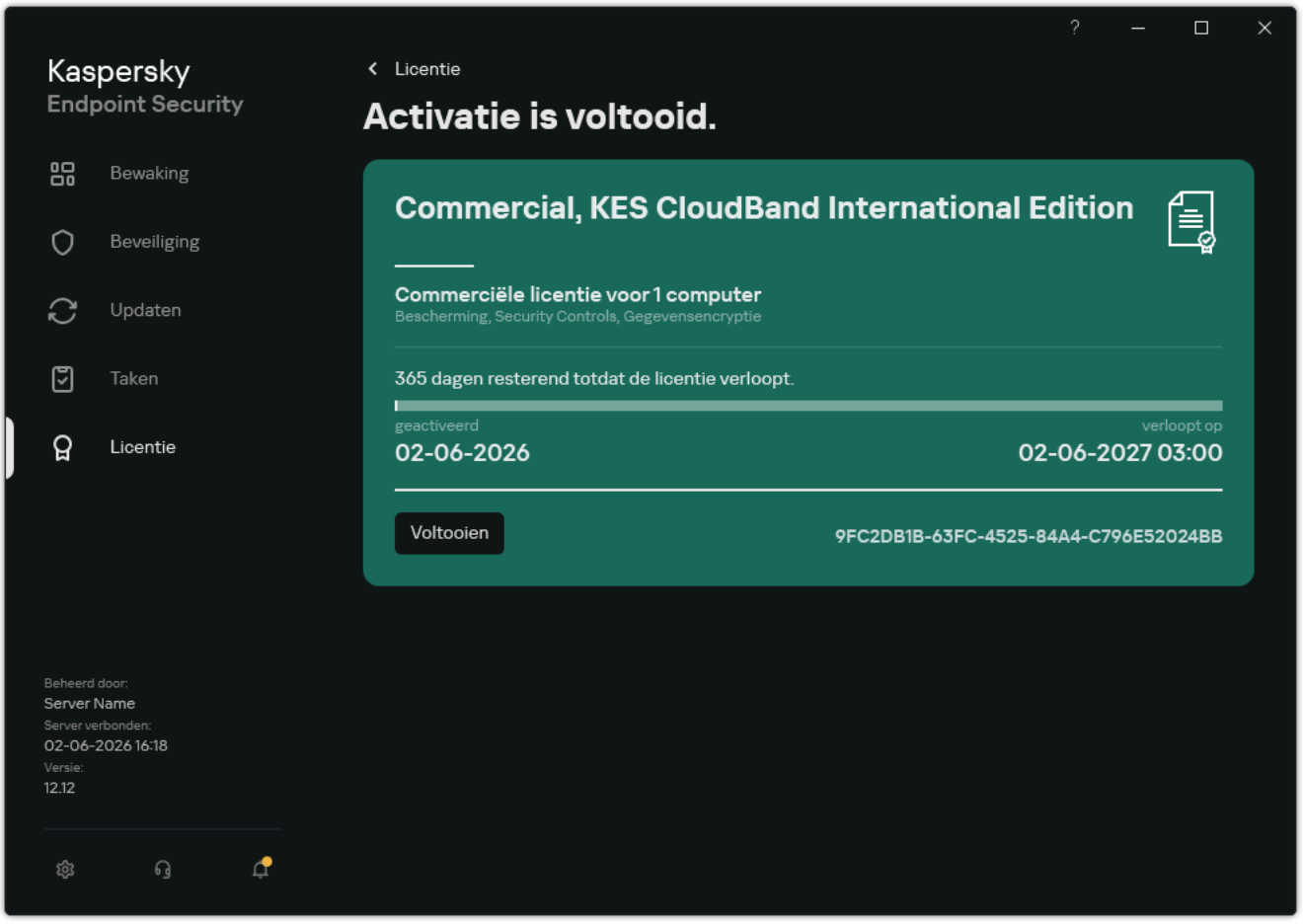
Het venster Licentiebeheer

U kunt een licentiesleutel ook via de opdrachtregel verwijderen.

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 reservelicentie 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.

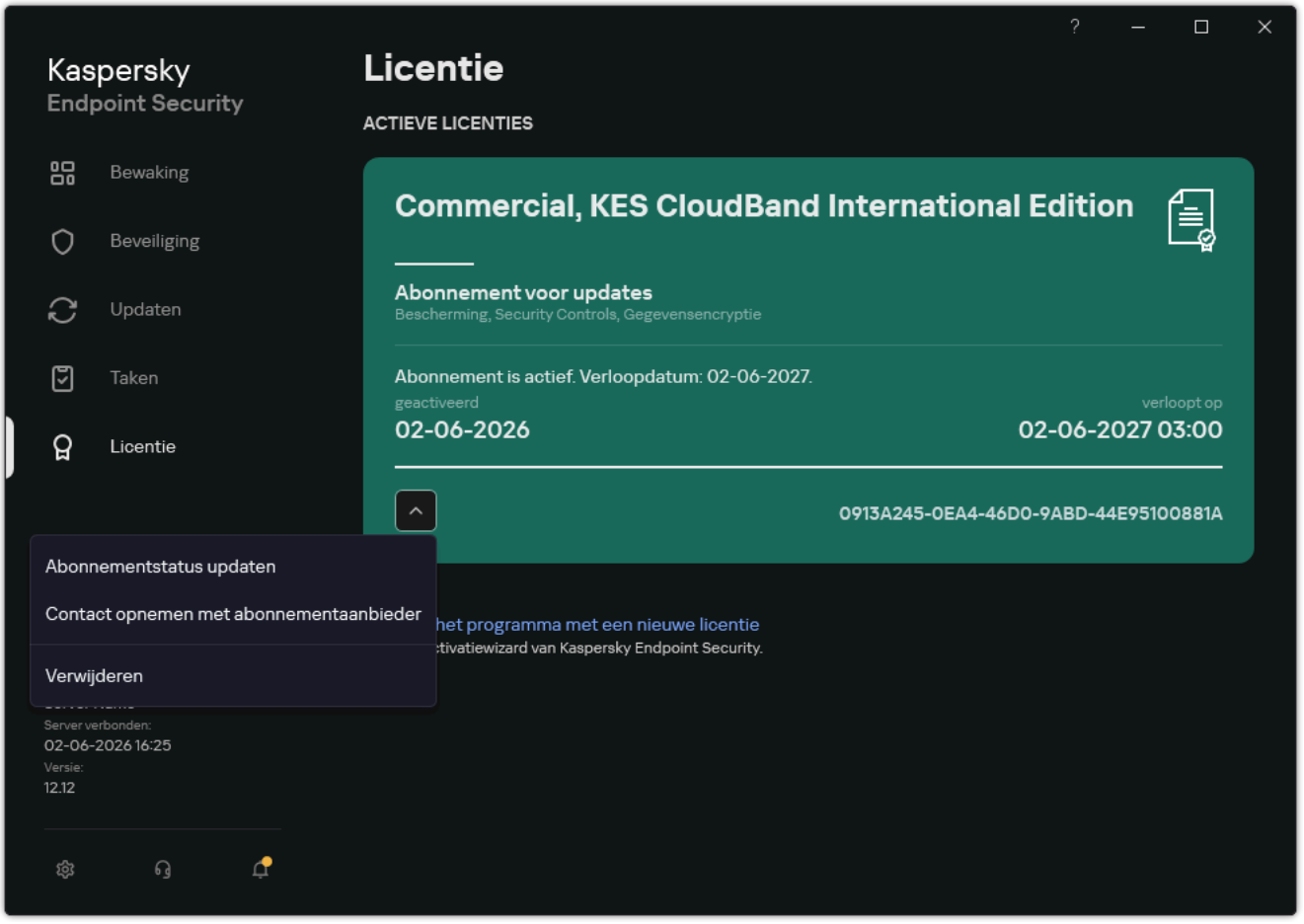
Als u het programma met een beperkt abonnement gebruikt, meldt Kaspersky Endpoint Security u dit op de verloopdatum van het abonnement (of op de verloopdatum van de respijtperiode) en worden geen nieuwe pogingen ondernomen om het abonnement automatisch te verlengen. In dit geval werkt Kaspersky Endpoint 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 abonnementaanbieder**.

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



Abonnement verlengen

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 beheren 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. De webplug-in moet zijn geïnstalleerd op een computer waarop Kaspersky Security Center Web Console 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.

Als u Kaspersky Endpoint Security gebruikt als onderdeel van de Kaspersky Endpoint Detection and Response Optimum-oplossing, moet u de Kaspersky Endpoint Detection and Response beheerplug-in installeren. Om waarschuwingsdetails weer te geven, hebt u de beheerplug-in nodig. *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. Om taken voor reactie op bedreigingen te maken, hebt u de beheerplug-in van Kaspersky Endpoint Security nodig. Om waarschuwingsdetails te bekijken, hebt u de beheerplug-in van EDR nodig.

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 gereleaset.

- Download het distributiepakket naar de Webconsole vanaf een externe bron.

  Voeg het ZIP-archief 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.

Vanaf Kaspersky Endpoint Security 12.11 voor Windows is de installatieprocedure voor de webplug-in gewijzigd. Het distributiepakket bevat nu twee webplug-ins: *Kaspersky Endpoint Security for Windows 14.1.0* en de *Unified Protection and Management Plug-in*. Dit komt door de overgang naar één enkele webplug-in voor het beheer van Kaspersky-programma's. Met de geïntegreerde webplug-in kunt u één beleid maken voor het beheer van meerdere Kaspersky-programma's (bijvoorbeeld Kaspersky Endpoint Security voor Windows, macOS en Linux). De overgang naar de geïntegreerde webplug-in kan meerdere releases duren. Nadat de overgang is voltooid, bevat het distributiepakket alleen de *Unified Protection and Management Plug-in*.

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-archief 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.

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

- De vorige versie van de Beheerplug-in voor Kaspersky Endpoint Security wordt verwijderd.
- De nieuwe versie van de Beheerplug-in voor Kaspersky Endpoint Security biedt ondersteuning voor het beheer van de vorige versie van Kaspersky Endpoint Security 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.

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.

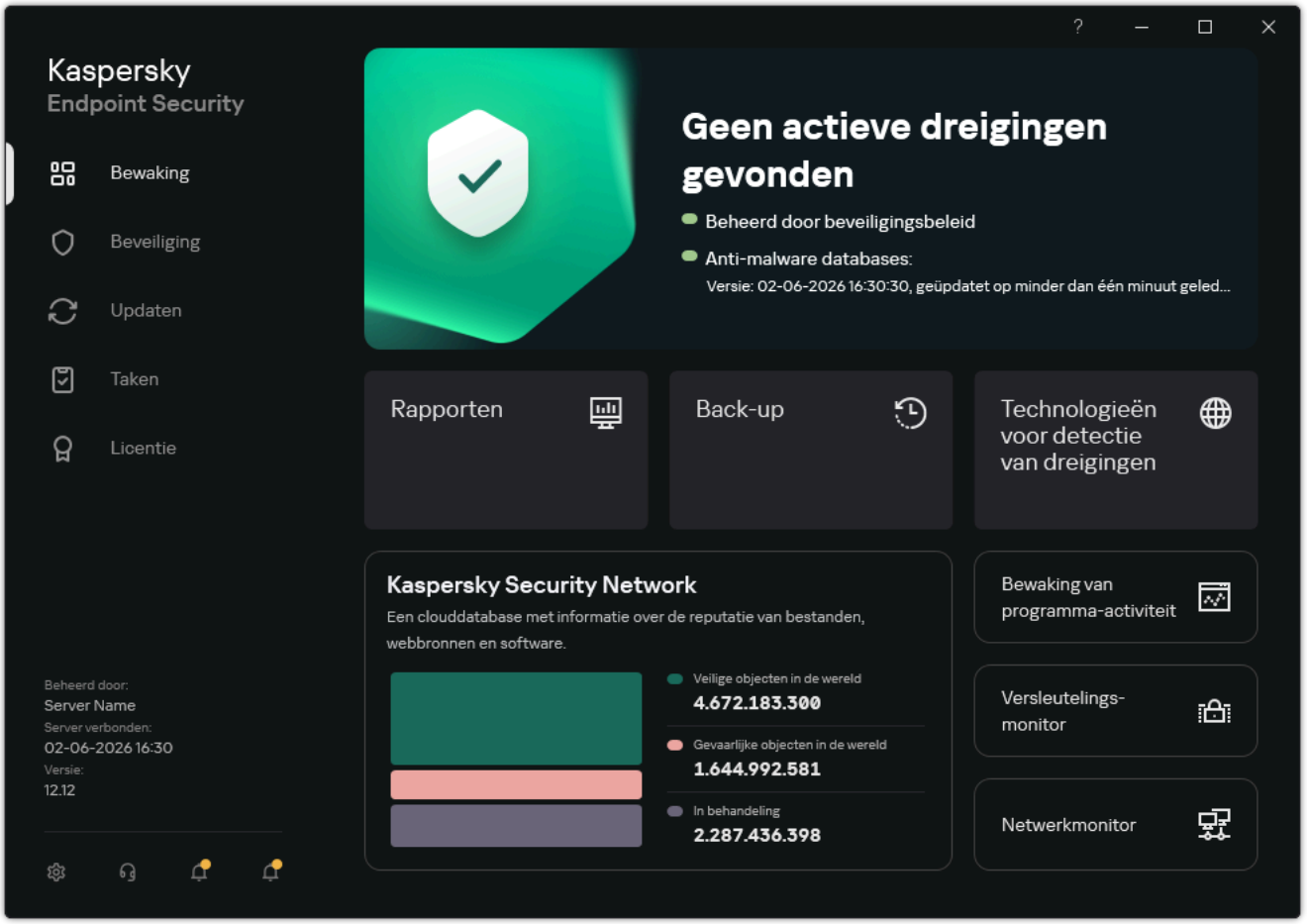
Gebruik van TLS beveiligt het programma door de volgende functies te bieden:

- 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 Self-Signed Certificate. Deze fouten kunnen optreden omdat een HTTPS-inspectietool uit uw omgeving de Kaspersky PKI niet herkent. U kunt dit verhelpen door uitzonderingen 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 het Kaspersky Security Network, voorzien de KSN-services Kaspersky Endpoint Security van informatie over de reputatie van gescande webadressen, evenals informatie over de categorie en reputatie van gescande bestanden. • **Bewaking van programma-activiteit**. Bekijk informatie over de werking van geïnstalleerde applicaties. Programmma-Activiteitenweergave houdt de bestands-, register- en besturingssysteemgebeurtenissen bij die geassocieerd zijn met een programma. • **Netwerkmonitor**. Bekijk informatie over de netwerkactiviteit van de computer in realtime. • **Versleutelings- monitor**. Bewaakt het encryptie- of decryptieproces van de schijf in realtime. Versleutelingsmonitor is beschikbaar als het onderdeel Kaspersky Disk Encryption of BitLocker-stationsversleuteling is geïnstalleerd.
Beveiliging	Bedrijfsstatus van geïnstalleerde componenten. U kunt ook onderdelen configureren of rapporten bekijken.
Updaten	Updatetaken van Kaspersky Endpoint Security beheren. U kunt antivirusdatabases en programmamodules bijwerken en de laatste update terugdraaien. Een beheerder kan het gedeelte verbergen voor de gebruiker of het taakbeheer beperken.
Taken	Scantaken van Kaspersky Endpoint Security beheren. U kunt een Malwarescan en een applicatie-integriteitscontrole uitvoeren. Een beheerder kan taken verbergen voor een gebruiker of het beheer van taken beperken.
Licentie	Licentiebeheer van het programma. U kunt een licentie kopen, het programma activeren of een abonnement verlengen. U kunt ook informatie over de huidige licentie bekijken.

	Programma-instellingen configureren Een beheerder kan wijzigingen in instellingen in Kaspersky Security Center verbieden.
	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.

Als het programmapictogram in het systeemvak van de taakbalk verborgen is, heeft de beheerder de weergave van de programma-interface in het beleid uitgeschakeld.

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 malware-scantaken. Het programma blijft ook Kaspersky Security Network gebruiken.

- **Beleid uitschakelen** / **Beleid inschakelen**. Het Kaspersky Security Center-beleid op de computer uitschakelen. 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**. Het Kaspersky Security Center-beleid op de computer uitschakelen. 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:

  - **Programma Integriteitscontrole**.

  - **Vorige versie van databases terugdraaien**.

  - **Volledige Scan**.

  - **Aangepaste Scan**.

  - **Kritieke Gebiedenscan**.

  - **Update**.

- **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:

- **Vereenvoudigde interface weergeven**. 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 alleen meldingen die een actie van de gebruiker vereisen boven het programmapictogram.

- **Gebruikersinterface weergeven**. 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.

- **Gebruikersinterface niet weergeven**. 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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.

2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

3. Selecteer **Algemene instellingen** → **Interface** in het beleidsvenster.

4. Configureer in het blok **Interactie met gebruiker** hoe de programma-interface wordt weergegeven:

   - **Gebruikersinterface weergeven**. 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. Indien nodig kunt u de functie **Bewaking van programma-activiteit verbergen** inschakelen om gegevens over de activiteiten van programma's op de computer te verbergen, waardoor de toegang van gebruikers tot de tool Bewaking van programma-activiteit wordt beperkt.

   - **Vereenvoudigde interface weergeven**. 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 alleen meldingen die een actie van de gebruiker vereisen boven het programmapictogram.

   - **Gebruikersinterface niet weergeven**. Op een clientcomputer wordt de werking van Kaspersky Endpoint Security niet aangegeven. Het pictogram in het Windows-systeemvak en de meldingen zijn niet beschikbaar.

5. Sla uw wijzigingen op.

De weergavemodus van de applicatie-interface configureren in de webconsole en cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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** → **User Interaction**.

5. Configureer in het blok **Visibility for users** hoe de programma-interface wordt weergegeven:

   - **Display user interface**. Als deze functionaliteit is uitgeschakeld, worden op een clientcomputer geen tekenen van een werking van Kaspersky Endpoint Security weergegeven. Het pictogram in het Windows-systeemvak en de meldingen zijn niet beschikbaar.

   - **Simplified**. 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 alleen meldingen die een actie van de gebruiker vereisen boven het programmapictogram.

   - **Full**. 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.

   - **Hide Application Activity Monitor section**. Als u de informatie over de programma-activiteit wilt verbergen op de computer van een gebruiker, kunt u de toegang van de gebruiker tot Bewaking van programma-activiteit beperken.

6. Sla uw wijzigingen op.

Het programma klaarmaken voor gebruik

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 *Update van databases en programmamodules* en *Malware-scan*.

  De taak *Update van databases en programmamodules* 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 *Update van databases en programmamodules* wordt automatisch gemaakt door de snelstart-wizard van de Administration Server. Voor het maken van de taak *Update van databases en programmamodules* installeert u de beheerplug-in van Kaspersky Endpoint Security voor Windows wanneer u de stappen van de wizard volgt.

  De taak *Malware-scan* is vereist voor de tijdige detectie van virussen en andere malware. U moet de taak *Malware-scan* handmatig aanmaken.

  Een taak Malware-scan maken in de Beheerconsole (MMC)

  1. Selecteer **Tasks** in de structuur van de Beheerconsole van Kaspersky Security Center.

     De lijst met taken wordt geopend.

  2. Klik op **New task**.

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

Stap 1. Een taaktype selecteren

Selecteer **Kaspersky Endpoint Security voor Windows 14.1.** → **Malware-scan**.

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 het programma automatisch om ieder gevonden geïnfecteerd bestand te desinfecteren. Mocht de desinfectie mislukken, dan wordt het bestand door het programma verwijderd.

- **Desinfecteren of melden als desinfectie mislukt**. Als deze optie is geselecteerd, probeert Kaspersky Endpoint Security automatisch om alle gevonden geïnfecteerde bestanden te desinfecteren. Indien desinfectie mislukt, 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.

- **Run only when the computer is idle**. Uitgestelde start van de taak 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. Met deze planningsoptie kunt u computervermogen besparen wanneer de computer wordt gebruikt.

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 *Malware-scan* 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 **Run the task after the wizard finishes** in. U kunt de voortgang van de taak volgen in de taakeigenschappen. De taak Malwarescan wordt volgens het opgegeven schema uitgevoerd op de computers van de gebruikers.

Een taak Malware-scan maken in de webconsole

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

   De lijst met taken wordt geopend.

2. Klik op **Add**.

   De wizard Taak wordt gestart.

3. Configureer de taakinstellingen:

   a. Selecteer in de vervolgkeuzelijst **Application** de optie **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. Selecteer in de vervolgkeuzelijst **Task type** de optie **Malware Scan**.

   c. Typ in het veld **Task name** een korte omschrijving, zoals *Wekelijkse scan*.

   d. Selecteer in het gedeelte **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. Ga naar de volgende stap.

5. Selecteer een account om de taak uit te voeren. Kaspersky Endpoint Security start de taak standaard met de rechten van een lokaal gebruikersaccount.

6. Verlaat de wizard verlaten.

   U ziet een nieuwe taak in de lijst met taken.

7. 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.

8. Schakel het selectievakje naast de taak in.

9. Klik op **Start**.

   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 Malwarescan wordt volgens het opgegeven schema uitgevoerd op de computers van de gebruikers.

- Prestaties van Kaspersky Endpoint Security optimaliseren.

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.

Elke beleidsinstelling heeft het volgende: ("hangslot") kenmerk. De status van dit kenmerk bepaalt of de instelling wordt doorgegeven aan de beheerde apparaten in de beheergroep:

- Als het "hangslot" is geopend ( ), wordt de waarde van deze instelling niet doorgegeven aan de beheerde apparaten. De instelling kan worden gewijzigd in de lokale interface van het programma. Dergelijke instellingen worden *ontgrendeld*.

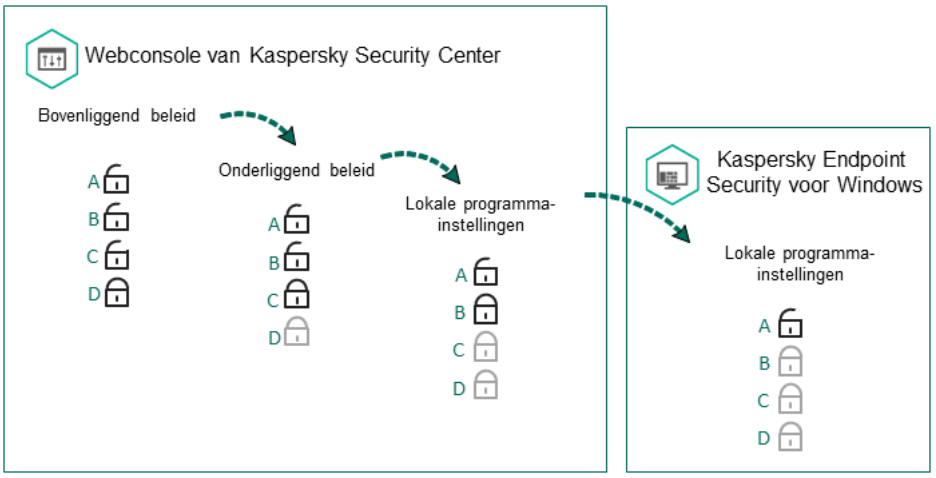
- Als het "hangslot" is gesloten ( ), wordt de waarde van deze instelling doorgegeven en toegepast op de beheerde apparaten. Dergelijke instellingen worden *vergrendeld*. Geblokkeerde instellingen kunnen niet worden gewijzigd in de lokale interface van het programma.

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.

Overname van instellingen

Beleid is, net als beheergroepen, in een hiërarchie gerangschikt. Een *onderliggend beleid* is een beleid voor geneste hiërarchieniveaus, dat een beleid is voor geneste beheergroepen en secundaire Administration Servers.

Standaard neemt een onderliggend beleid instellingen over van het bovenliggende beleid. Als de instelling in het bovenliggende beleid het kenmerk (gesloten "hangslot") heeft, dan wordt in onderliggende beleidsregels en lokale programma-instellingen de waarde van die instelling overschreven volgens het bovenliggende beleid en wordt de instelling vergrendeld. Indien nodig kunt u het overnemen van instellingen van het bovenliggende beleid uitschakelen. 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. Ga om toegangsrechten tot beleidsinstellingen te configureren naar het gedeelte **Security** in het taakscherm van Kaspersky Security Center Administration Server (dit onderdeel wordt standaard verborgen in de console interface).

Beleidswijzigingen

Kaspersky Security Center houdt wijzigingen in het beleid bij en maakt revisies aan. Een *revisie* is een set gewijzigde parameters die door de gebruiker is opgeslagen. Met revisies kunt u wijzigingen in beleidsparameters vergelijken en terugdraaien. Naast de set gewijzigde parameters bevat de revisie informatie over de gebruiker die de wijzigingen heeft aangebracht, evenals de tijd, het IP-adres, de opmerking van de gebruiker en andere relevante gegevens.

Als u het revisielogboek wilt bekijken, open de eigenschappen van het beleid en ga naar de sectie **Revision history**. Voor meer informatie over het werken met revisies raadpleeg de Help van Kaspersky Security Center.

Een beleid aanmaken

Bij het maken van een beleid stelt de wizard instellingen voor die relevant zijn voor de geselecteerde modus. Voor de Light Agent-modus moet u bijvoorbeeld een Protection Server (SVM) toevoegen. Wanneer u het programma gebruikt om een SQL-server te beschermen, moet u vooraf gedefinieerde scanuitzonderingen toevoegen om ervoor te zorgen dat de werking van de server niet wordt verstoord. De wizard stelt relevante beleidsinstellingen voor na het selecteren van een modus. U kunt deze instellingen vervolgens bewerken in de beleidseigenschappen.

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 **Policies**.

4. Klik op **New policy**.

   De wizard Beleid wordt gestart.

5. Volg de instructies van de wizard Beleid.

Stap 1: Het programma selecteren om groepsbeleid te maken

Selecteer een programma **Kaspersky Endpoint Security for Windows (14.1)**.

Stap 2. Het groepsbeleid een naam geven

Voer een naam in voor het groepsbeleid, bijvoorbeeld *Beleid voor kantoor*.

U kunt ook nieuwe beleidsregels maken op basis van bestaande beleidsregels met behulp van de beleidswizard. Schakel hiervoor het selectievakje **Use policy settings for an earlier version of the application** in wanneer u de naam van het groepsbeleid opgeeft. Met de wizard kunt u ook een Kaspersky Endpoint Security (KES)-beleid maken op basis van een beleid van een andere oplossing, bijvoorbeeld Kaspersky Security for Windows Server (KSWS) of Kaspersky Security for Virtualization Light Agent voor Windows

Stap 3. Deelnemen aan Kaspersky Security Network

Lees en accepteer de voorwaarden van de Kaspersky Security Network-verklaring (KSN).

Stap 4. De programmagebruiksmodus op computers selecteren

Afhankelijk van het beoogde gebruik van Kaspersky Endpoint Security kunt u een beleid voor de volgende programmamodi configureren:

- Standaardmodus om hosts te beschermen

  In deze modus kunt u selecteren hoe u het beleid wilt configureren:

  - **Beleid met standaardinstellingen maken**. Standaardinstellingen worden als optimaal beschouwd. Deze instellingen worden aanbevolen door Kaspersky-experts. Standaardinstellingen bieden aanbevolen beschermingsniveau en optimaal gebruik van bronnen.

  - **Wijzig beleidsinstellingen in de Wizard**. Met deze methode kunt u de beleidsinstellingen stapsgewijs beheren met behulp van een wizard. U kunt de beleidsinstellingen ook beheren met een configuratiebestand van het programma (zie de volgende stap).

- Endpoint Detection and Response Agent ter bescherming tegen geavanceerde bedreigingen en gerichte aanvallen.

  Endpoint Detection and Response Agent is een programma die op individuele werkstations en servers in de IT-infrastructuur van de organisatie wordt geïnstalleerd ter ondersteuning van de Detection and Response-oplossingen van Kaspersky. Bij de volgende stap moet u een oplossing voor de integratie van EDR-agenten selecteren.

- Light Agent om virtuele omgevingen te beschermen.

  Als u het programma in de Light Agent-modus wilt gebruiken, moet u een verbinding met een virtuele SVM-machine configureren. Deze instellingen zijn vereist om het programma in de Light Agent-modus te laten werken.

Kaspersky Endpoint Security biedt een gemeenschappelijk beleid voor alle applicatiemodi en besturingssysteemtypen. Dit betekent dat het beleid de hele set instellingen dekt. Het is echter mogelijk dat het programma enkele beleidsinstellingen negeert omdat Kaspersky Endpoint Security is geïmplementeerd in een modus waarin bepaalde functionaliteit niet beschikbaar is. Wanneer u het programma bijvoorbeeld in de modus Endpoint Detection and Response Agent gebruikt, zijn alleen instellingen beschikbaar die relevant zijn voor de integratie met Kaspersky Detection and Response-oplossingen en voor de integratie met KUMA.

We raden aan om verschillende beleidsregels te gebruiken voor verschillende modi en typen besturingssystemen.

Stap 5. Instellingen importeren

Deze stap is beschikbaar als u handmatige beleidsconfiguratie selecteert bij stap 4.

U kunt een beleid maken op basis van de instellingen van Kaspersky Endpoint Security vanuit een CFG-configuratiebestand. Wanneer u een programma-configuratiebestand importeert, zijn niet alle beleidsinstellingen beschikbaar voor de wizard. Beleidsprofielen ontbreken bijvoorbeeld in programma-instellingen. Als u alle instellingen en profielen wilt overzetten naar het beleid, kunt u: ander beleid importeren vanuit een KLP-bestand.

Bij het importeren van een configuratiebestand verstuurt Kaspersky Endpoint Security geen wachtwoorden voor crypto-containers. Als u tweerichtingsverificatie gebruikt wanneer u verbinding maakt met servers, moet u een geheel nieuw wachtwoord voor crypto-containers opgeven.

Stap 6 - 10. Beleidsinstellingen configureren

Deze stap is beschikbaar als u handmatige beleidsconfiguratie selecteert bij stap 4.

Volg de stappen om de beleidsinstellingen te beheren.

Stap 11. De vertrouwde zone configureren

Configureer de vertrouwde zone. U kunt vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's toevoegen. Vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's helpen bij het snel configureren van Kaspersky Endpoint Security op SQL-servers, Microsoft Exchange-servers en System Center Configuration Manager. Dit betekent dat u niet handmatig een vertrouwde zone voor het programma op servers hoeft in te stellen. Vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's kunnen u ook helpen Kaspersky Endpoint Security snel te configureren in de Light Agent-modus in virtuele Citrix- en VMware-omgevingen.

Stap 12. Selecteer de status van het beleid

- **Active**. Na de volgende synchronisatie wordt het beleid gebruikt als het actieve beleid op de computer.

  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.

- **Inactive**. Back-upbeleid. Een inactief beleid kan indien nodig worden geactiveerd.

  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.

- **Out-of-office**. Het beleid wordt geactiveerd wanneer de computer niet meer verbonden is met het bedrijfsnetwerk.

Voltooi de wizard.

Een beleid maken in de Webconsole en de Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
2. Klik op **Add**.

   De wizard Beleid wordt gestart.
3. Selecteer Kaspersky Endpoint Security en klik op **Next**.
4. Lees en accepteer de voorwaarden van de Kaspersky Security Network-verklaring (KSN) en klik op **Next**.
5. Selecteer de modus van het programma:

   - Standard mode to protect workstations and servers
   - Endpoint Detection and Response Agent to protect against advanced threats and targeted attacks.

     Als u deze modus selecteert, kunt u een beleid maken om de computer te integreren met Kaspersky Detection and Response-oplossingen. De wizard vraagt u om de integratie voor Kaspersky Managed Detection and Response en vervolgens Kaspersky Anti Targeted Attack Platform (EDR) te configureren.
   - Light Agent to protect virtual environments.

     Als u deze modus selecteert, moet u in de volgende stap de verbinding met de Protection Server (SVM) configureren. Deze instellingen zijn vereist om het programma in de Light Agent-modus te laten werken.

Kaspersky Endpoint Security biedt een gemeenschappelijk beleid voor alle applicatiemodi en besturingssysteemtypen. Dit betekent dat het beleid de hele set instellingen dekt. Het is echter mogelijk dat het programma enkele beleidsinstellingen negeert omdat Kaspersky Endpoint Security is geïmplementeerd in een modus waarin bepaalde functionaliteit niet beschikbaar is. Wanneer u het programma bijvoorbeeld in de modus Endpoint Detection and Response Agent gebruikt, zijn alleen instellingen beschikbaar die relevant zijn voor de integratie met Kaspersky Detection and Response-oplossingen en voor de integratie met KUMA.

We raden aan om verschillende beleidsregels te gebruiken voor verschillende modi en typen besturingssystemen.

6. Configureer de vertrouwde zone. U kunt vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's toevoegen. Vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's helpen bij het snel configureren van Kaspersky Endpoint Security op SQL-servers, Microsoft Exchange-servers en System Center Configuration Manager. Dit betekent dat u niet handmatig een vertrouwde zone voor het programma op servers hoeft in te stellen. Vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's kunnen u ook helpen Kaspersky Endpoint Security snel te configureren in de Light Agent-modus in virtuele Citrix- en VMware-omgevingen.

7. Op het tabblad **General** kunt u de volgende acties uitvoeren:

   - Wijzig de naam van het beleid.
   - Selecteer de status van het beleid:
     - **Active**. Na de volgende synchronisatie wordt het beleid gebruikt als het actieve beleid op de computer.

       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.
     - **Inactive**. Back-upbeleid. Een inactief beleid kan indien nodig worden geactiveerd.

       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.
     - **Out-of-office**. Het beleid wordt geactiveerd wanneer de computer niet meer verbonden is met het bedrijfsnetwerk.
   - Configureer de overname van instellingen:
     - **Inherit settings from parent policy**. 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.
     - **Force inheritance of settings in child policies**. 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 **Inherit settings from parent policy** 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.

8. U kunt op het tabblad **Application settings** de beleidsinstellingen voor Kaspersky Endpoint Security configureren.

9. Voltooi de wizard.

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.

Een beleid exporteren en importeren

Met Kaspersky Endpoint Security kunt u een beleid met de bijbehorende instellingen en profielen exporteren naar een KLP-bestand. U kunt vervolgens de functionaliteit voor het exporteren/importeren van beleid gebruiken om een back-up te maken van beleid, het migreren van beleid naar een andere server of om bijvoorbeeld beleid te migreren van Kaspersky Security Center Windows naar Kaspersky Security Center Linux. Voor meer informatie over het beheren van beleidsregels raadpleeg de Kaspersky Security Center Help.

Een Beleid 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. Exporteer een beleid:

   a. Klik op het beleid dat u wilt exporteren.

   b. Klik op de link in het rechterdeel van het venster op het **Export policy to file**.

   c. In het venster dat verschijnt, geef de naam op van het KLP-bestand waarnaar u het beleid wilt exporteren en selecteer de map waarin u het bestand wilt opslaan.

   d. Sla het bestand op.

5. Importeer een beleid:

   a. Klik op **Import policy from file**.

   b. In het venster dat verschijnt, selecteer het KLP-beleidsbestand dat u wilt importeren.

   c. Open het bestand.

   Hiermee wordt een nieuw beleid toegevoegd met de *Inactive policy* status.

Exporteer en importeer een beleid in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
2. Exporteer een beleid:
   a. Selecteer het selectievakje aan naast het beleid dat u wilt exporteren.
   b. Klik op de knop **Export**.
   c. In het venster dat verschijnt, geef de naam op van het KLP-bestand waarnaar u het beleid wilt exporteren en selecteer de map waarin u het bestand wilt opslaan.
   d. Sla het bestand op.
3. Importeer een beleid:
   a. Klik op **Import**.
   b. Selecteer het KLP-beleidsbestand dat u wilt importeren.
   c. Nadat het beleid is verwerkt, selecteer de beheergroep waarop u het beleid wilt toepassen.
   d. Klik op de **Complete** om het importeren van het beleid te voltooien.

Hiermee wordt een nieuw beleid toegevoegd met de *Inactive* status.

Indicator voor beschermingsniveau

De indicator voor het beschermingsniveau wordt boven in het venster beleidseigenschappen 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.
    - Bescherming van programmaservices tegen extern beheer.
  - **Belangrijk**. Deze categorie bevat de volgende onderdelen:
    - Kaspersky Security Network.
    - Web Threat Protection.

- Mail Threat Protection.
- Host Intrusion Prevention.
- Wachtwoordbeveiliging.

- **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.

Na het upgraden van het programma kan de beschermingsniveau-indicator een lager beschermingsniveau aangeven dan vóór de upgrade. Dit gebeurt omdat de nieuwere versie van het programma nieuwe onderdelen of functies introduceert die belangrijk zijn voor de veiligheid van de computer. Na het upgraden van het programma moet u mogelijk de nieuwe instellingen beheren om ervoor te zorgen dat het beschermingsniveau hoog blijft.



Indicator voor beschermingsniveau van het beleid

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:

- **Malware-scan**. Kaspersky Endpoint Security scant de in de taakinstellingen opgegeven computergebieden op virussen en andere dreigingen. De taak *Malware-scan* 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.

- **Update van databases en programmamodules**. Kaspersky Endpoint Security updatet databases en programmamodules. De taak *Update van databases en programmamodules* 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.

- **Programma 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.

Als het programma werkt als onderdeel van de Endpoint Detection and Response-oplossingen door Kaspersky, kunt u extra taken uitvoeren als detectieractie (responses). Bijvoorbeeld, met de taak *Proces beëindigen* kunt u op afstand processen beëindigen.

Taken worden pas op een computer uitgevoerd als Kaspersky Endpoint Security actief is.

Een taak aanmaken

Een taak maken in de Beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer de map **Tasks** in de structuur van de Beheerconsole.
3. Klik op **New task**.
   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 **Tasks**.
   De lijst met taken wordt geopend.
2. Klik op **Add**.
   De wizard Taak wordt gestart.
3. Configureer de taakinstellingen:
   a. Selecteer in de vervolgkeuzelijst **Application** de optie **Kaspersky Endpoint Security for Windows 14.1.0**.
   b. Selecteer in de vervolgkeuzelijst **Task type** 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 **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. Ga naar de volgende stap.
5. Selecteer een account om de taak uit te voeren. Kaspersky Endpoint Security start de taak standaard met de rechten van een lokaal gebruikersaccount.
6. Voltooi de wizard.

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 **Start** 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 → Event selections**). 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.

Toegang tot taken beheren

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 **Security** 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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Lokale Taken** → **Taakbeheer** in het beleidsvenster.
4. Configureer de taakbeheermodus (zie onderstaande tabel).
5. Sla uw wijzigingen op.

De taakbeheermodus configureren in de Kaspersky Endpoint Security-interface via de webconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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** → **User Interaction**.
5. Configureer onder **Permitted actions** de taakbeheermodus (zie onderstaande tabel).
6. Sla uw wijzigingen op.

Instellingen van Taakbeheer

Parameter	Beschrijving
Access to local tasks	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. 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. Een gebruiker kan wel een scan van een bestand of een map starten door de optie **Scannen op virussen** 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.

Parameter	Beschrijving
View group tasks	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. Als het selectievakje is uitgeschakeld, geeft Kaspersky Endpoint Security een lege takenlijst weer.
Manage group tasks	Als het selectievakje is ingeschakeld, kunnen gebruikers groepstaken starten en stoppen die zijn opgegeven in de Kaspersky Security Center-console. Gebruikers kunnen taken starten en stoppen in de programma-interface of in de vereenvoudigde programma-interface. Als het selectievakje is uitgeschakeld, start Kaspersky Endpoint Security automatisch geplande taken of start de beheerder taken handmatig in de Kaspersky Security Center-console.

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 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 **Applications** in het venster met computereigenschappen.
6. Selecteer **Kaspersky Endpoint Security voor Windows (14.1)** in de lijst met Kaspersky-programma's die op de computer zijn geïnstalleerd en dubbelklik om de eigenschappen van het programma te openen.
7. Configureer in het gedeelte **Algemene instellingen** Kaspersky Endpoint Security en Rapporten en Opslag.

   De rest van de secties in het venster met programma-eigenschappen zijn standaard voor Kaspersky Security Center. Een beschrijving van deze gedeelten 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.

8. Sla uw wijzigingen op.

De lokale programma-instellingen configureren in de Webconsole en de Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Assets (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. 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.

Opstarten van Kaspersky Endpoint Security configureren in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.

2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

3. Selecteer **Algemene instellingen** → **Programma-instellingen** in het beleidsvenster.

4. Gebruik het selectievakje **Programma starten wanneer computer wordt opgestart (aanbevolen)** om de opstart van het programma te configureren.

5. Sla uw wijzigingen op.

Opstarten van Kaspersky Endpoint Security configureren in de webconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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** → **User Interaction**.

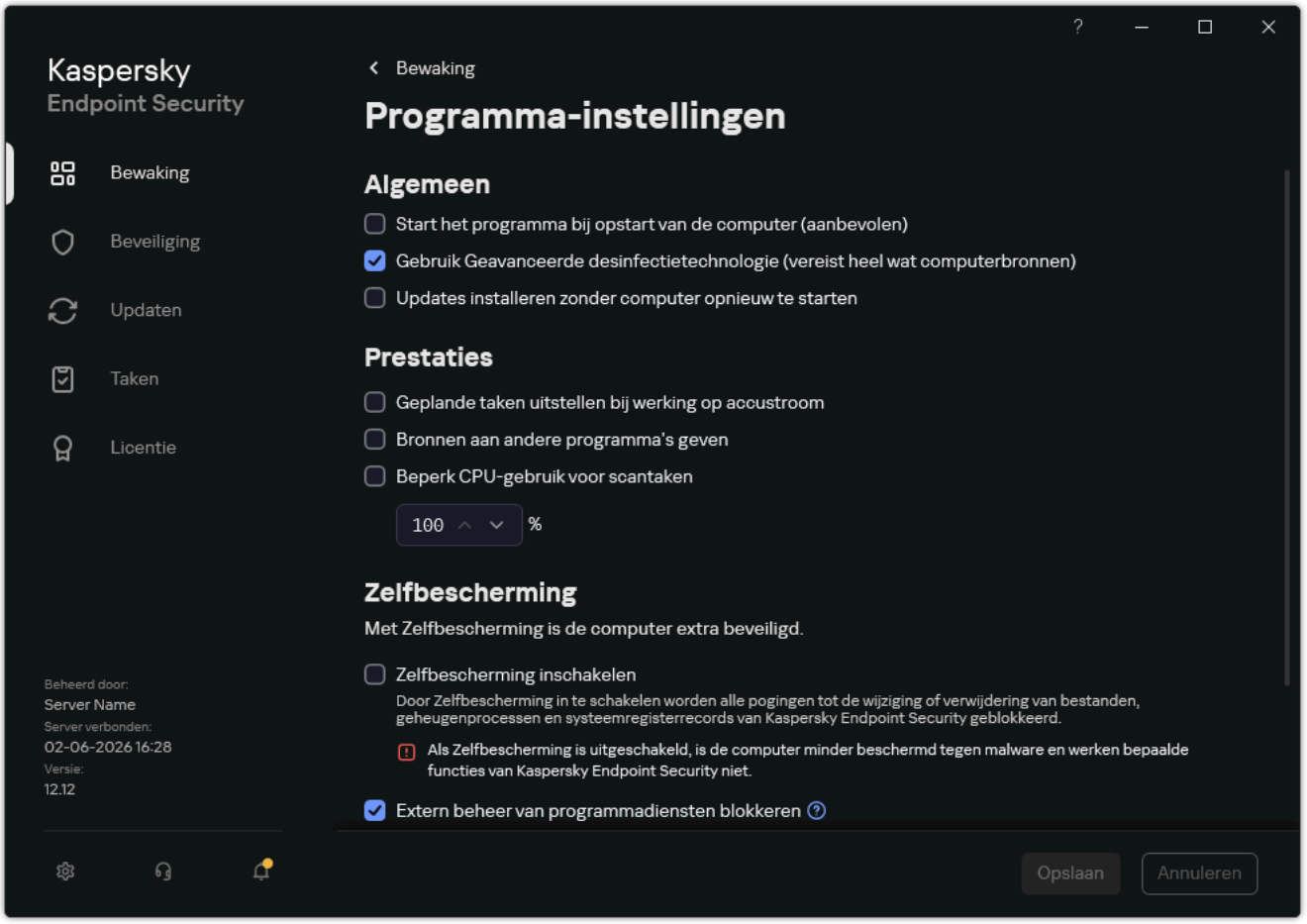
5. Gebruik het selectievakje **Start Kaspersky Endpoint Security on computer startup (recommended)** om de opstart van het programma te configureren.

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.



Instellingen Kaspersky Endpoint Security voor Windows

3. Gebruik het selectievakje **Programma starten wanneer computer wordt opgestart (aanbevolen)** 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 **Protection status**.

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 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 **Applications** in het venster met computereigenschappen.
6. Selecteer **Kaspersky Endpoint Security voor Windows (14.1)** in de lijst met Kaspersky-programma's die op de computer zijn geïnstalleerd en dubbelklik om de eigenschappen van het programma te openen.
7. Doe een van de volgende acties:
   - 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 **Asset management** → **Assets (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 **Applications**.
4. Schakel het selectievakje hiernaast in **Kaspersky Endpoint Security for Windows**.
5. Klik op de **Start** of **Stop** knop.

Kaspersky Endpoint Security starten of stoppen vanaf de opdrachtregel

1. Voer de interpreter van de opdrachtregel (cmd.exe) uit als een beheerder.
2. Ga naar de map waarin het uitvoerbare bestand klpsm.exe zich bevindt.
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`.

Om het programma via de opdrachtregel te stoppen, moet u extern beheer van systeemservices inschakelen.



Het programma vanaf de opdrachtregel starten en stoppen

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.

- Gebruik Kaspersky Security Center om Kaspersky Endpoint Security op afstand te installeren met vooraf gedefinieerde instellingen.

- Programma-instellingen overzetten naar een beleid.

- Migreer de instellingen van Kaspersky Endpoint Security van de ene computer naar de andere (zie de onderstaande instructies).

Een configuratiebestand exporteren

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. Voer indien nodig een wachtwoord in voor het exporteren van de programmaconfiguratie naar een bestand.

   Om het configuratiebestand op te slaan, moet Wachtwoordbeveiliging zijn ingeschakeld. De gebruiker moet de machtiging **Instellingen exporteren** hebben.

6. Sla het bestand op.

Als gevolg hiervan maakt het programma een configuratiebestand aan. Het configuratiebestand kan gegevens van een gebruikersaccount bevatten. Daarom encrypt Kaspersky Endpoint Security het bestand. U kunt een configuratiebestand niet bewerken. Elke poging tot het wijzigen van een configuratiebestand maakt het corrupt.

Een configuratiebestand importeren

Een configuratiebestand kan de details van gebruikersaccounts bevatten die aan het programma zijn toegevoegd. Als u het bestand importeert op dezelfde computer als waarop het bestand is gemaakt, importeert Kaspersky Endpoint Security de wachtwoorden van gebruikersaccounts. Als u het bestand op een andere computer importeert, moet u de wachtwoorden handmatig invoeren.

Bij het importeren van een configuratiebestand verstuurt Kaspersky Endpoint Security geen wachtwoorden voor crypto-containers. Als u tweerichtingsverificatie gebruikt wanneer u verbinding maakt met servers, moet u een geheel nieuw wachtwoord voor crypto-containers opgeven.

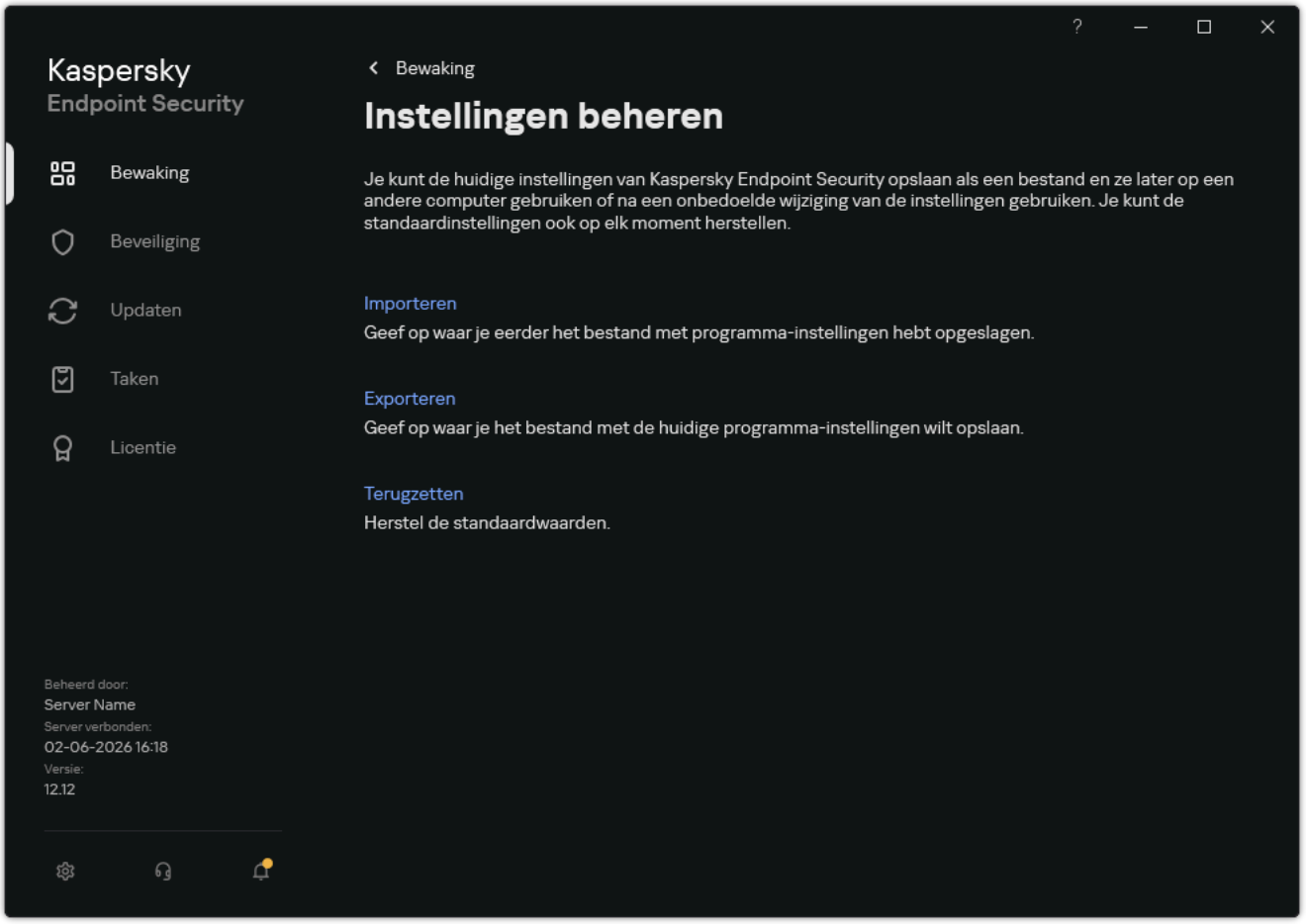
Zo importeert u de instellingen van Kaspersky Endpoint Security vanuit een configuratiebestand:

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.



De programma-instellingen beheren

Standaardinstellingen van het programma herstellen

U kunt de door Kaspersky aanbevolen programma-instellingen op elk moment herstellen. Wanneer de instellingen zijn hersteld, wordt het **Aanbevolen** beveiligingsniveau ingesteld voor alle beschermingsonderdelen.

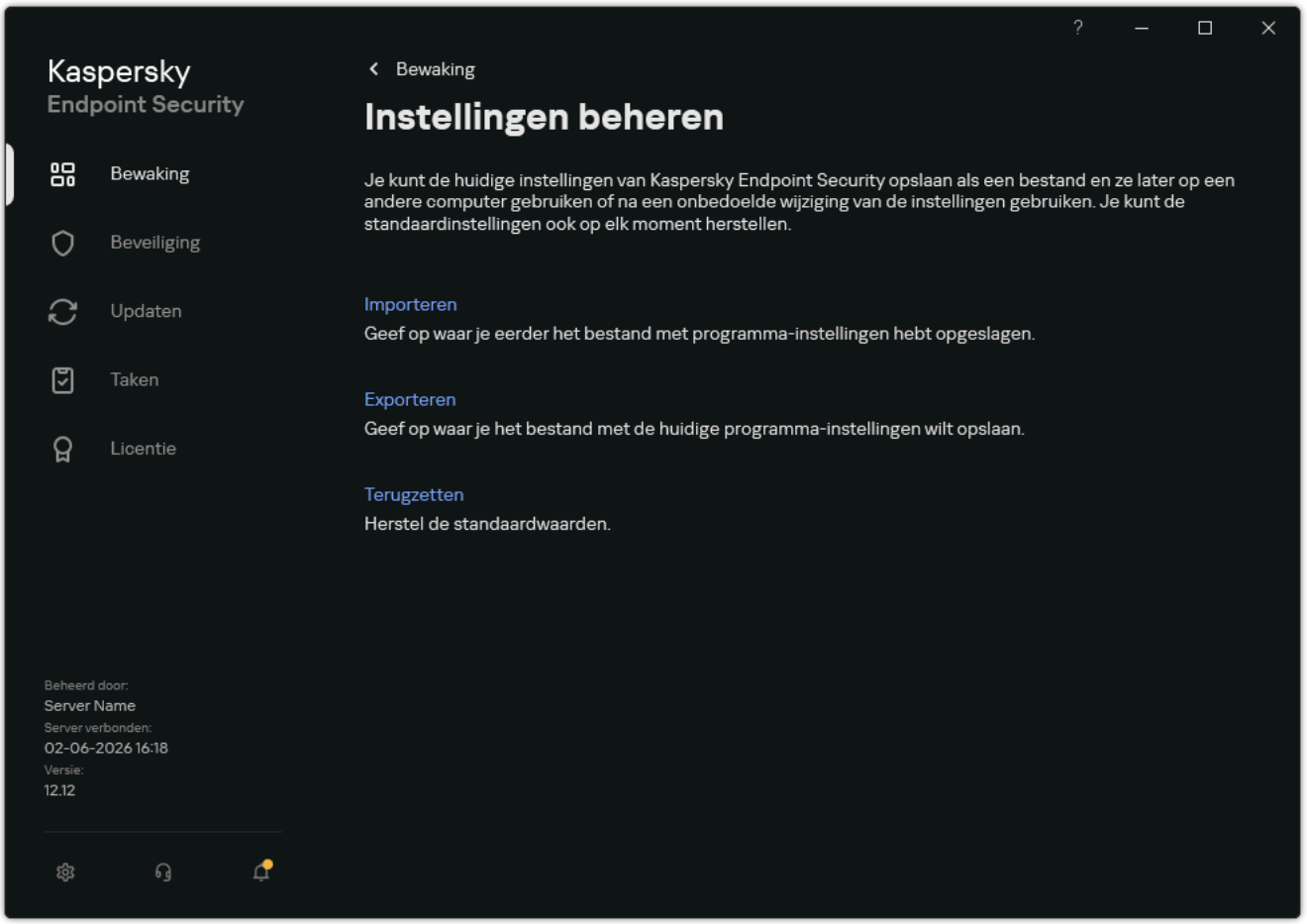
De standaardinstellingen van het programma herstellen:

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.



De programma-instellingen beheren

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:

- 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 bij het scannen van een computer kan de belasting van de CPU en de subsystemen van de harde schijf verhogen. 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 actieve infectie op een server te desinfecteren, schakelt u de actieve desinfectietechnologie voor servers in en start u een *Malware-scan* als groepstaak op een tijdstip dat de gebruikers van de bestandsserver goed uitkomt.

Energiebesparingsmodus inschakelen of uitschakelen

Energiebesparingsmodus is een functionaliteit die de belasting van de bronnen van de laptop vermindert en de levensduur van de batterij verlengt zonder het beveiligingsniveau aanzienlijk in gevaar te brengen. In de energiebesparingsmodus beperkt het programma de start van geplande taken. Op deze manier zorgt de energiebesparingsmodus voor een evenwicht tussen het beveiligingsniveau en de levensduur van de batterij van de laptop.

Wanneer de energiebesparingsmodus is ingeschakeld en een computer op batterijspanning werkt, worden de volgende taken niet gestart zelfs als ze zijn gepland:

- *Volledige Scan*.
- *Kritieke Gebiedenscan*.
- *Aangepaste Scan*.
- *Programma Integriteitscontrole*.
- *IOC-scan*.
- *Update van databases en programmamodules* (alleen patches)

Het programma slaat geplande database-updates alleen over wanneer de laptop werkt op de batterij en het batterijniveau lager is dan 30%. In alle andere gevallen werkt Kaspersky Endpoint Security de databases bij volgens schema, ongeacht of de laptop is aangesloten op een stopcontact of werkt op de batterij, of dat het programma zich in de energiebesparingsmodus bevindt.

Energiebesparingsmodus in- of uitschakelen in de Beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de beheerconsole **Policies**.
3. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
4. Selecteer **Algemene instellingen** → **Programma-instellingen** in het beleidsvenster.

5. Gebruik in het blok **Prestaties** het selectievakje **Geplande taken uitstellen bij werking op accustroom** om de energiebesparingsmodus in of uit te schakelen.

6. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Energiebesparingsmodus in- of uitschakelen in de webconsole

1. Selecteer in het hoofdvenster van de Webconsole het tabblad **Asset management** → **Policies**.

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** → **Performance**.

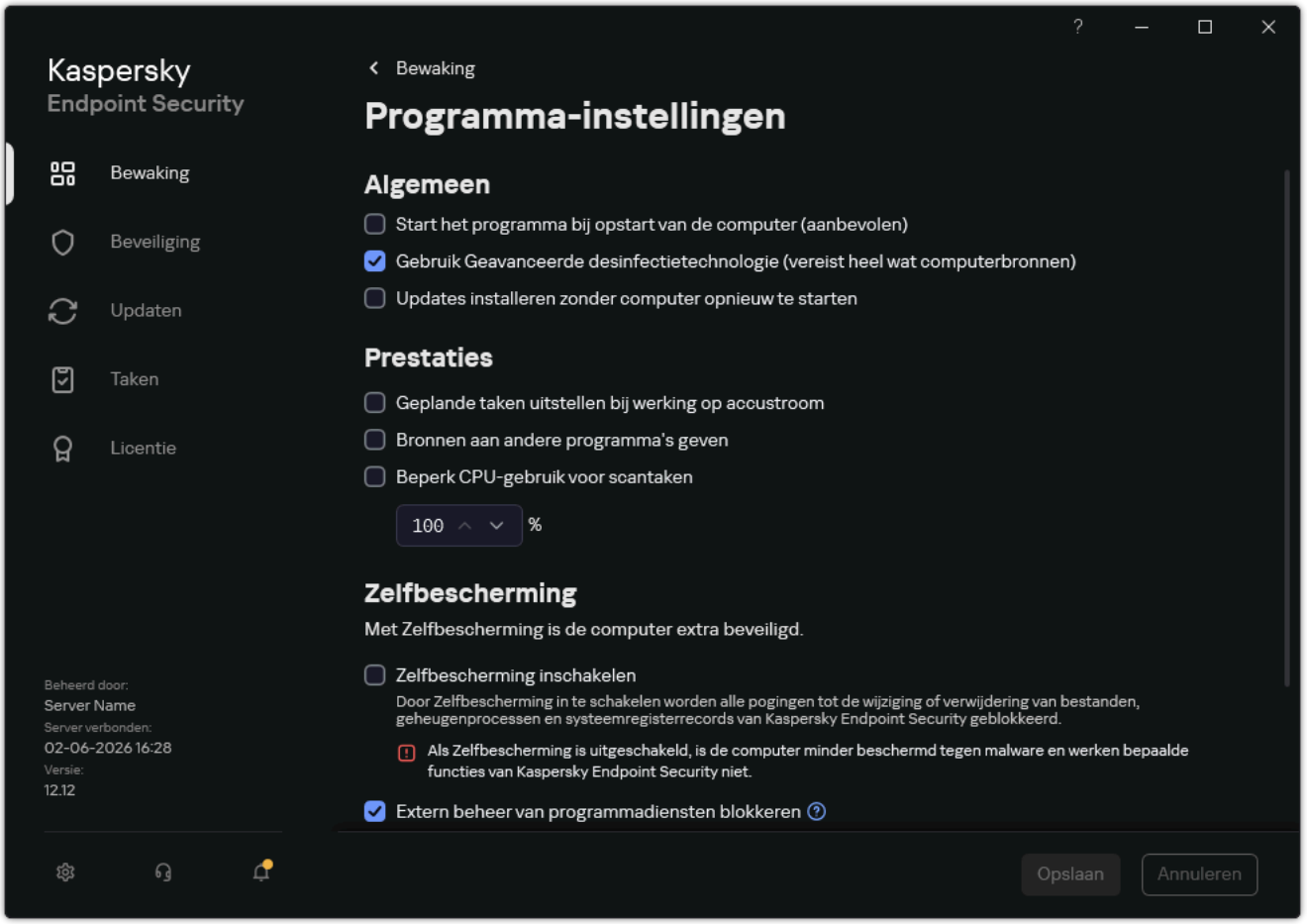
5. Gebruik in het blok **Postpone or skip scheduled tasks while running on battery power** het selectievakje **Postpone or skip scheduled tasks while running on battery power (depends on OS)** om de energiebesparingsmodus in of uit te schakelen.

6. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Energiebesparingsmodus in- of uitschakelen 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.



Instellingen Kaspersky Endpoint Security voor Windows

3. Gebruik in het blok **Prestaties** het selectievakje **Geplande taken uitstellen bij werking op accustroom** om de energiebesparingsmodus in of uit te schakelen.

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.

Hoe het onderdeel bronnen aan andere programma's geven in- of uitschakelen in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.

2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

3. Selecteer **Algemene instellingen → Programma-instellingen** in het beleidsvenster.

4. 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.

5. Sla uw wijzigingen op.

Hoe het onderdeel bronnen aan andere programma's geven in- of uitschakelen in de webconsole en cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management → Policies**.

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**.

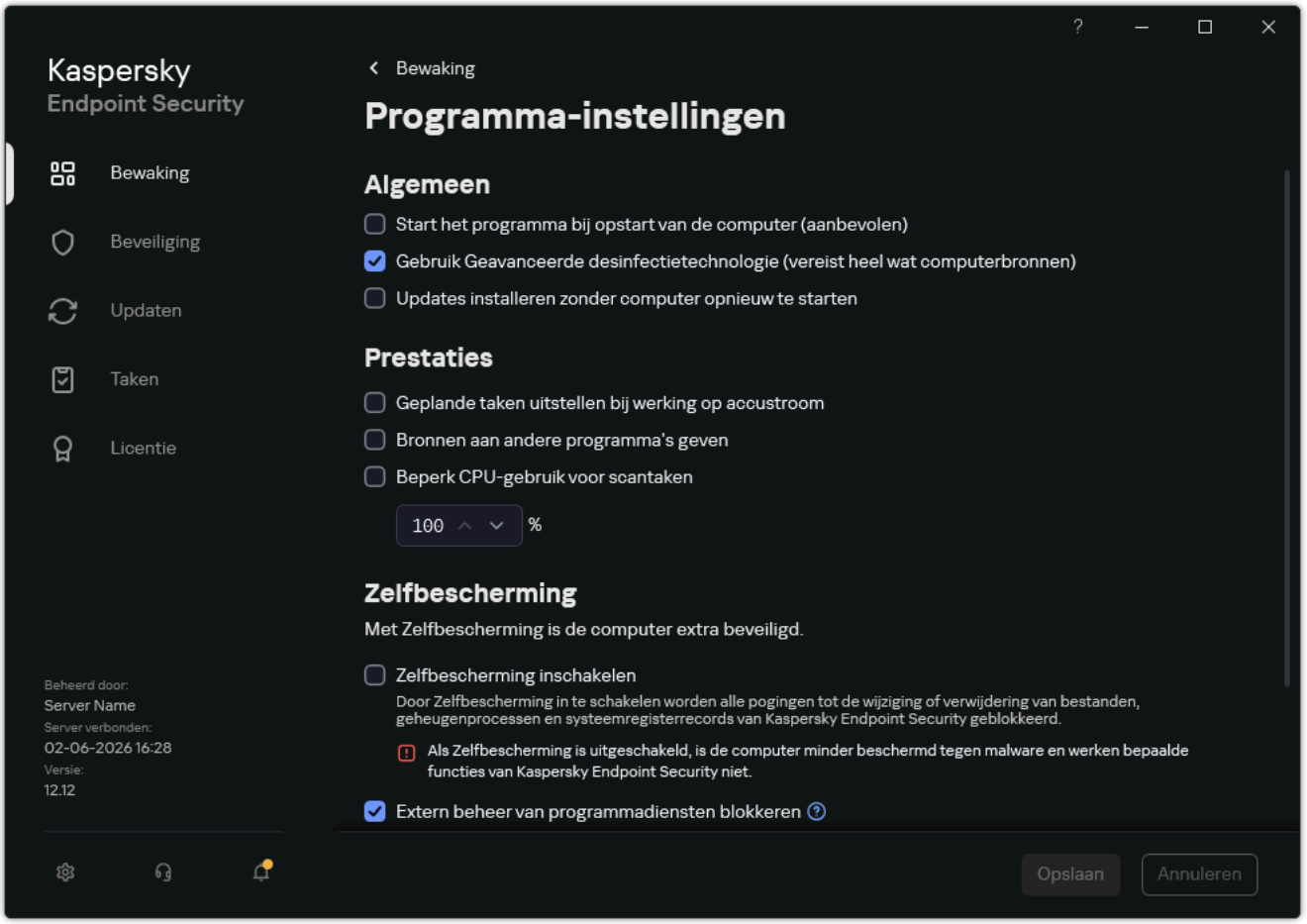
4. Ga naar **General Settings → Performance**.

5. Gebruik in het blok **Yield resources to other applications** de schakelaar **Yield resources to other applications** om het toewijzen van bronnen aan andere programma's in of uit te schakelen.

6. Sla uw wijzigingen op.

Hoe het onderdeel bronnen aan andere programma's geven in- of uitschakelen 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.



Instellingen Kaspersky Endpoint Security voor Windows

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. Raadpleeg voor meer informatie over het omgaan met problemen met computerprestaties de [Knowledge Base van de Technische Support].

General

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.

Malware-scan op werkstations

Het inschakelen van Achtergrondscan wordt aanbevolen voor malwarescan 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 malware-scan 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 *Malware-scan* taak in overeenstemming met de volgende aanbevelingen:

1. Stel een limiet in voor het CPU-bronverbruik tijdens het scannen van de computer.

   U kunt het CPU-gebruik beperken wanneer u de taak *Malware-scan* uitvoert. Om dit te doen, in de programma-instellingen, specificeer het maximale CPU-belastingspercentage voor alle kernen die kunnen worden gebruikt tijdens het scannen van de computer. Hierdoor kan het langer duren om uw computer te scannen.

2. 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 buiten bedrijfsuren de computer uitschakelen, kun je de Wake on LAN-functie 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.

   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.

3. Een scanbereik definiëren.

Selecteer de volgende objecten om te scannen (minimale set scanbereiken):

- Kernelgeheugen
- Actieve processen en opstartobjecten
- Opstartsectoren
- %systemroot% (exclusief submappen)
- %systemroot%\System (exclusief submappen)
- %systemroot%\System32 (exclusief submappen)
- %systemroot%\System32\drivers (exclusief submappen)
- %systemroot%\SysWOW64 (exclusief submappen)
- %systemroot%\SysWOW64\drivers (exclusief submappen)

4. 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.

5. 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.

6. Gelijktijdig starten van meerdere scantaken uitschakelen.

   Kaspersky Endpoint Security zal nieuwe scantaken in de wachtrij plaatsen als de huidige scan doorgaat. Dit helpt de belasting op de computer te optimaliseren.

Malware-scan op de servers

Configureer de *Malware-scan* taak in overeenstemming met de volgende aanbevelingen:

1. Stel een limiet in voor het CPU-bronverbruik tijdens het scannen van de computer.

   U kunt het CPU-gebruik beperken wanneer u de taak *Malware-scan* uitvoert. Om dit te doen, in de programma-instellingen, specificeer het maximale CPU-belastingspercentage voor alle kernen die kunnen worden gebruikt tijdens het scannen van de computer. Hierdoor kan het langer duren om uw computer te scannen.

2. 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.

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.

5. Gelijktijdig starten van meerdere scantaken uitschakelen.

   Kaspersky Endpoint Security zal nieuwe scantaken in de wachtrij plaatsen als de huidige scan doorgaat. Dit helpt de belasting op de computer te optimaliseren.

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 het Kaspersky Security Network, voorzien de KSN-services Kaspersky Endpoint Security van informatie over de reputatie van gescande webadressen, evenals informatie over de categorie en reputatie van gescande bestanden.

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. Kaspersky Private Security Network configureren.

   Kaspersky Private Security Network (KPSN) is een oplossing waarmee gebruikers van computers waarop Kaspersky Endpoint Security of andere Kaspersky-programma's worden gehost toegang krijgen tot reputatiedatabases van Kaspersky en tot andere statistische gegevens zonder gegevens naar Kaspersky 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.

Malware-scan

Een malwarescan is noodzakelijk om de computer veilig te houden. Start daarom regelmatig een malware-scan 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 het scanbereik van de taken *Volledige Scan* niet te veranderen.

Om het gebruik van computerbronnen te beperken, is het raadzaam om in plaats van een volledige scan een achtergrondscan 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 taken *Kritieke Gebiedenscan* niet te veranderen.

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
- 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.

Programma Integriteitscontrole

Kaspersky Endpoint Security controleert de programmamodules op beschadiging of wijzigingen.

Computer scannen

Een scan is noodzakelijk om de computer veilig te houden. Start daarom regelmatig een malware-scan 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 volgende standaardtaken vooraf gedefinieerd: *Volledige Scan*, *Kritieke Gebiedenscan*, *Aangepaste Scan*. Als het Kaspersky Security Center-beheersysteem is geïmplementeerd in uw bedrijf, kunt u een *Malware-scan*-taak maken en de scan configureren.

Een scantaak starten via Beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de beheerconsole **Tasks**.

3. Selecteer de scantaak en dubbelklik om de taakeigenschappen te openen.

   Maak indien nodig de *Malware-scan*-taak aan.

4. Selecteer het gedeelte **Instellingen** in het venster met taakeigenschappen.

5. Configureer de scantaak (zie onderstaande tabel).

   Configureer indien nodig het schema voor de scantaak.

6. Sla uw wijzigingen op.

7. 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 scantaak starten via de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **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 scantaak 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.

Als u de prestaties van Kaspersky Endpoint Security wilt optimaliseren terwijl u de computer scant, kunt u: de geavanceerde instellingen van de taak *Volledige Scan* beheren en het gebruik van CPU-bronnen beperken.

In Kaspersky Security Center kunt u ook de taak *Achtergrondscan* gebruiken in plaats van de taak *Volledige Scan* om de prestaties van het programma te optimaliseren. Dit is niet van invloed op het beveiligingsniveau van de computer. De achtergrondscan kan niet worden geconfigureerd.

Als gevolg hiervan scant Kaspersky Endpoint Security de computer en als er een dreiging wordt gedetecteerd, voert het de actie uit die is geconfigureerd in de programma-instellingen. Meestal probeert het programma geïnfecteerde bestanden te desinfecteren. Als gevolg hiervan kunnen de geïnfecteerde bestanden de volgende statussen ontvangen:

- **Uitgesteld**. Het geïnfecteerde bestand kan niet worden gedesinfecteerd. Het programma verwijdert het geïnfecteerde bestand nadat de computer opnieuw is opgestart.
- **Geregistreerd**. Het geïnfecteerde bestand kan niet worden gedesinfecteerd. Het programma voegt informatie over gedetecteerde geïnfecteerde bestanden toe aan de lijst met actieve dreigingen.
- **Schrijven niet ondersteund** of **Schrijffout**. Het geïnfecteerde bestand kan niet worden gedesinfecteerd. Het programma heeft geen schrijftoegang.
- **Al verwerkt**. Het programma detecteerde eerder een geïnfecteerd bestand. Het programma desinfecteert of verwijdert het geïnfecteerde bestand nadat de computer opnieuw is opgestart.

Scaninstellingen

Parameter	Beschrijving
Beveiligingsniveau	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 *beveiligingsniveaus* genoemd: • **Hoog**. Kaspersky Endpoint Security scant alle soorten bestanden. Bij het scannen van samengestelde bestanden scant het programma wel archieven, distributiepakketten en bestanden in Office-indeling, maar geen archieven die met een wachtwoord zijn beveiligd. Wanneer dit beveiligingsniveau is ingesteld, gebruikt het programma een heuristische analyse met de **Gedetailleerde scan** detailniveau. • **Aanbevolen**. Kaspersky Endpoint Security scant alle soorten bestanden. Bij het scannen van samengestelde bestanden scant het programma wel archieven, distributiepakketten en bestanden in Office-indeling, maar geen archieven die met een wachtwoord zijn beveiligd. Wanneer dit beveiligingsniveau is ingesteld, gebruikt het programma een heuristische analyse met de **Gemiddelde scan** detailniveau. • **Laag**. Kaspersky Endpoint Security scant alleen de opgegeven bestandsindelingen. Bij het scannen van samengestelde bestanden scant het programma wel archieven, distributiepakketten en bestanden in Office-indeling, maar geen archieven die met een wachtwoord zijn beveiligd. Wanneer dit beveiligingsniveau is ingesteld, gebruikt het programma een heuristische analyse met de **Oppervlakkige scan** detailniveau. 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.

Parameter	Beschrijving
Actie bij detectie van een dreiging	**Desinfecteren of verwijderen als desinfectie mislukt**. Als deze optie is geselecteerd, probeert het programma automatisch om ieder gevonden geïnfecteerd bestand te desinfecteren. Mocht de desinfectie mislukken, dan wordt het bestand door het programma verwijderd. **Desinfecteren of melden als desinfectie mislukt**. Als deze optie is geselecteerd, probeert Kaspersky Endpoint Security automatisch om alle gevonden geïnfecteerde bestanden te desinfecteren. Indien desinfectie mislukt, 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. Voordat u probeert een geïnfecteerd bestand te desinfecteren of te verwijderen, maakt het programma een reservekopie van het bestand voor het geval u het bestandmoet herstellen of als het in de toekomst kan worden gedesinfecteerd. Bij het vinden van geïnfecteerde bestanden die onderdeel zijn van het Windows Store-programma probeert Kaspersky Endpoint Security het bestand te wissen.
Geavanceerde desinfectie direct uitvoeren *(alleen beschikbaar in de Kaspersky Security Center-console)*	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. 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. 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.
Scanbereik	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, harde schijf, verwisselbare schijfn, netwerkschijf, map of bestand. In Kaspersky Endpoint Security voor Windows 12.12 valt e-mail niet onder het scanbereik van het programma. Het scannen van inkomende en uitgaande e-mails wordt uitgevoerd door het onderdeel Mail Threat Protection. Als u een oudere versie van de beheerplug-in gebruikt, sluit het programma e-mail uit van het scanbereik, zelfs als het beleid deze wel bevat.
Planning van scan	**Manually**. Uitvoermodus waarin u handmatig kunt beginnen met scannen op een moment dat het u uitkomt. **By schedule**. In deze uitvoermodus voor scantaken wordt de scantaak door het programma gestart volgens het schema dat u aanmaakt. Als deze uitvoermodus voor scantaken is geselecteerd, kunt u de scantaak ook handmatig starten.
Start na programmastart uitstellen met N minuten	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.
Overgeslagen taken starten	Als het selectievakje is ingeschakeld, wordt de overgeslagen taak door Kaspersky Endpoint Security gestart zodra dit mogelijk is. De taak kan bijvoorbeeld worden overgeslagen als de computer uitgeschakeld was op de starttijd van de taak. Als het programma een kans krijgt om gemiste taken uit te voeren, start het de taken willekeurig binnen een bepaalde tijdsinterval om de lading voor de computer te spreiden. Als het selectievakje is uitgeschakeld, worden overgeslagen taken niet gestart door Kaspersky Endpoint Security. In plaats daarvan voert het de volgende taak uit volgens het huidige schema.

Parameter	Beschrijving
Alleen starten als de computer inactief is	Uitgestelde start van de taak 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. Met deze planningsoptie kunt u computervermogen besparen wanneer de computer wordt gebruikt.
Scan starten namens	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 het programma en de scantaak onder dit gebruikersaccount uitvoeren.
Bestandstypen	Kaspersky Endpoint Security beschouwt bestanden zonder extensie als uitvoerbare bestanden. Het programma voert altijd uitvoerbare bestanden ongeacht de bestandstypen die u wilt laten 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, scant het programma alleen infecteerbare bestanden. 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, scant het programma alleen infecteerbare bestanden. De bestandsindeling wordt dan bepaald op basis van de bestandsextensie. 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`).
Scan alleen nieuwe en aangepaste 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.
Sla bestand over waarvan scan langer duurt dan N seconden	De taakuitvoeringstijd 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.
Laat niet meerdere scantaken tegelijk lopen	Uitgestelde start van scantaken als er al een scan loopt. Kaspersky Endpoint Security zal nieuwe scantaken in de wachtrij plaatsen als de huidige scan doorgaat. Dit helpt de belasting op de computer te optimaliseren. Laten we er bijvoorbeeld vanuit gaan dat het programma volgens het schema een volledige scantaak heeft gestart. Als een gebruiker probeert een snelle scan te starten vanuit de programma-interface, zal Kaspersky Endpoint Security deze snelle scan-taak in de wachtrij plaatsen en deze taak automatisch starten nadat de volledige scantaak is voltooid. Kaspersky Endpoint Security start echter onmiddellijk een scantaak, zelfs als een van de volgende scantaken wordt uitgevoerd: • Scan van verwisselbare schijven bij verbinding. • Scannen vanuit contextmenu. • Kritieke Gebiedenscan die werd gestart bij de detectie van een Indicator of Compromise (IoC). Als dit selectievakje is uitgeschakeld, kunt u met Kaspersky Endpoint Security meerdere scantaken tegelijk uitvoeren. Het uitvoeren van meerdere scantaken vereist meer computerbronnen.
Scan archieven	ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE en andere bestanden scannen. Het programma 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 (een archief in een archief).
Scan distributiepakketten	Distributiepakketten van programma's van derden scannen.
Scan Microsoft Office-bestanden	Scant Microsoft Office-bestanden (DOC, DOCX, XLS, PPT en andere Microsoft-extensies). Bestanden in Office-indeling bevatten ook OLE-objecten. Het programma scant office-bestanden die kleiner zijn dan 1 MB, ongeacht of het selectievakje is ingeschakeld of niet.

Parameter	Beschrijving
Bestanden in e-mailindeling scannen	Het scannen van e-mailindelingen en de e-maildatabase. Het programma scant PST- en OST-bestanden gebruikt door MS Outlook en Windows Mail e-mailclients, evenals EML-bestanden. Kaspersky Endpoint Security biedt geen ondersteuning voor de 64-bits versie van de Microsoft Outlook-mailclient. Dit betekent dat Kaspersky Endpoint Security geen Microsoft Outlook-bestanden (PST- en OST-bestanden) scant als een 64-bit versie van Microsoft Outlook op de computer is geïnstalleerd, zelfs als e-mail is opgenomen in het scanbereik. 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. Als dit selectievakje is uitgeschakeld, scant Kaspersky Endpoint Security het bestand met de e-mailindeling als een enkel bestand. Wanneer een kwaadaardig object wordt ontdekt in PST- of OST-bestanden, maakt Kaspersky Endpoint Security het onschadelijk in overeenstemming met de geselecteerde actie (bijvoorbeeld desinfectie of verwijdering van het bestand). Wanneer een kwaadaardig bestand wordt gedetecteerd in bestanden van andere e-mailclients (bijvoorbeeld Mozilla Thunderbird), markeert Kaspersky Endpoint Security alleen het geïnfecteerde bericht. U moet het bericht met een geïnfecteerde bijlage handmatig verwijderen.
Scan wachtwoordbeveiligde archieven	Als het selectievakje is ingeschakeld, worden archieven met wachtwoordbeveiliging gescand door het programma. 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 het programma.
Pak grote samengestelde bestanden niet uit	Als dit selectievakje is ingeschakeld, scant het programma geen samengestelde bestanden als ze groter zijn dan de opgegeven waarde. Als dit selectievakje is uitgeschakeld, worden samengestelde bestanden van alle grootten gescand door het programma. Het programma scant grote bestanden die uit archieven worden gehaald, ongeacht of het selectievakje is ingeschakeld of niet.
Machine learning en analyse op basis van definities	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. Op aanbeveling van Kaspersky-experts is machine learning en analyse op basis van definities altijd ingeschakeld.
Heuristische analyse	De technologie is ontworpen om dreigingen te detecteren die niet met de huidige versie van de databases van het Kaspersky-programma kunnen worden gedetecteerd. De technologie detecteert bestanden die mogelijk geïnfecteerd zijn met een onbekend virus of een nieuwe variëteit van een bekend virus. 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.
iSwift-technologie *(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)*	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 *(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)*	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).

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 eniChecker technologieën voor scanoptimalisatie. De technologieën staan altijd aan en kunnen niet worden uitgeschakeld.

Start van Scan van verwisselbare schijven configureren via de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Lokale Taken** → **Scan van Verwisselbare Schijven** in het beleidsvenster.
4. Selecteer in de vervolgkeuzelijst **Actie op een verwisselbare schijfverbinding** de optie **Gedetailleerde Scan** of **Snelle Scan**.
5. Configureer geavanceerde opties voor Scan van verwisselbare schijven (zie onderstaande tabel).
6. Sla uw wijzigingen op.

Start van Scan van verwisselbare schijven configureren via de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Host Threat Protection** → **Removable Drives Scan**.
5. Gebruik de schakelaar **Removable Drives Scan ENABLED** om de component in of uit te schakelen.
6. Selecteer in het blok **Scan type Detailed Scan** of **Quick 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 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
Scan type	**Detailed Scan**. Als deze optie is geselecteerd, scant Kaspersky Endpoint Security alle bestanden wanneer een verwisselbaar station wordt aangesloten, inclusief bestanden in samengestelde objecten, archieven, distributiepakketten en bestanden in Office-indelingen. Kaspersky Endpoint Security scant geen bestanden met een e-mailindeling of archieven met wachtwoordbeveiliging. **Quick Scan**. Als deze optie is geselecteerd en een verwisselbare schijf wordt aangesloten, scant Kaspersky Endpoint Security alleen bestanden met specifieke indelingen die heel kwetsbaar zijn voor infecties en pakt het geen samengestelde objecten uit.
Maximum drive size (MB)	Als dit selectievakje is ingeschakeld, voert Kaspersky Endpoint Security de gekozen actie uit op verwisselbare schijven die kleiner zijn dan de opgegeven waarde. Als de grootte van de verwisselbare schijf groter is dan de geconfigureerde waarde, slaat Kaspersky Endpoint Security de scan over. Als het selectievakje is uitgeschakeld, voert Kaspersky Endpoint Security de gekozen actie uit op verwisselbare schijven van elke grootte.
Hide scan progress bar	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 **Taken**. Als het selectievakje is uitgeschakeld, voert Kaspersky Endpoint Security de scan van verwisselbare schijven op de achtergrond uit.
Prevent users from stopping the scan	Als dit selectievakje is ingeschakeld, zijn voor de scantaak voor verwisselbare schijven in de lokale interface van Kaspersky Endpoint Security de knop **Stoppen** in het gedeelte **Taken** en de knop **Stoppen** in het venster scan van verwisselbare schijven niet beschikbaar.

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.

Om het gebruik van computerbronnen te beperken, is het raadzaam om in plaats van een volledige scan een achtergrondscan uit te voeren. Dit is niet van invloed op het beveiligingsniveau van de computer. Deze taken hebben hetzelfde scanbereik. Om de belasting op de computer te optimaliseren, voert het programma niet tegelijkertijd een volledige scantaak en een achtergrondscantaak uit. Als u al een volledige scantaak hebt uitgevoerd, start Kaspersky Endpoint Security geen achtergrondscantaak gedurende zeven dagen nadat de volledige scantaak is voltooid.

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 accumodus.

> 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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Lokale Taken** → **Achtergrondscan** in het beleidsvenster.
4. Gebruik het selectievakje **Schakel achtergrondscan in** om achtergrondscans in of uit te schakelen.
5. Sla uw wijzigingen op.

Achtergrondscans inschakelen via de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Host Threat Protection** → **File Threat Protection**.
5. Gebruik onder **Background Scan** de schakelaar **Background Scan ENABLED** om de achtergrondscan 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 ⚙.

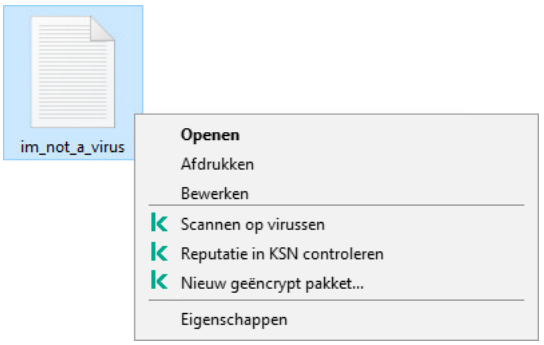
3. Gebruik de schakelaar **Achtergrondscan** om achtergrondscans in of uit te schakelen.
4. Sla uw wijzigingen op.

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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Lokale Taken** → **Scannen vanuit contextmenu** in het beleidsvenster.
4. Configureer Scannen vanuit contextmenu (zie onderstaande tabel).
5. Sla uw wijzigingen op.

Scannen vanuit contextmenu configureren via de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Host Threat Protection** → **File Threat Protection**.
5. Configureer **Scan from Context Menu** de functie '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
Beveiligingsniveau	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 *beveiligingsniveaus* genoemd: • **Hoog**. Kaspersky Endpoint Security scant alle soorten bestanden. Bij het scannen van samengestelde bestanden scant het programma wel archieven, distributiepakketten en bestanden in Office-indeling, maar geen archieven die met een wachtwoord zijn beveiligd. Wanneer dit beveiligingsniveau is ingesteld, gebruikt het programma een heuristische analyse met de **Gedetailleerde scan** detailniveau. • **Aanbevolen**. Kaspersky Endpoint Security scant alle soorten bestanden. Bij het scannen van samengestelde bestanden scant het programma wel archieven, distributiepakketten en bestanden in Office-indeling, maar geen archieven die met een wachtwoord zijn beveiligd. Wanneer dit beveiligingsniveau is ingesteld, gebruikt het programma een heuristische analyse met de **Gemiddelde scan** detailniveau. • **Laag**. Kaspersky Endpoint Security scant alleen de opgegeven bestandsindelingen. Bij het scannen van samengestelde bestanden scant het programma wel archieven, distributiepakketten en bestanden in Office-indeling, maar geen archieven die met een wachtwoord zijn beveiligd. Wanneer dit beveiligingsniveau is ingesteld, gebruikt het programma een heuristische analyse met de **Oppervlakkige scan** detailniveau.
Actie bij detectie van een dreiging	**Desinfecteren of verwijderen als desinfectie mislukt**. Als deze optie is geselecteerd, probeert het programma automatisch om ieder gevonden geïnfecteerd bestand te desinfecteren. Mocht de desinfectie mislukken, dan wordt het bestand door het programma verwijderd. **Desinfecteren of melden als desinfectie mislukt**. Als deze optie is geselecteerd, probeert Kaspersky Endpoint Security automatisch om alle gevonden geïnfecteerde bestanden te desinfecteren. Indien desinfectie mislukt, 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.
Bestandstypen	Kaspersky Endpoint Security beschouwt bestanden zonder extensie als uitvoerbare bestanden. Het programma voert altijd uitvoerbare bestanden ongeacht de bestandstypen die u wilt laten 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, scant het programma alleen infecteerbare bestanden. 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, scant het programma alleen infecteerbare bestanden. De bestandsindeling wordt dan bepaald op basis van de bestandsextensie. 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`).
Scan alleen nieuwe en aangepaste 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.
Sla bestand over waarvan scan langer duurt dan N seconden	De taakuitvoeringstijd 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.

Parameter	Beschrijving
Scan archieven	ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE en andere bestanden scannen. Het programma 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 (een archief in een archief).
Scan distributiepakketten	Het selectievakje schakelt het scannen van distributiepakketten in of uit.
Scan Microsoft Office-bestanden	Scant Microsoft Office-bestanden (DOC, DOCX, XLS, PPT en andere Microsoft-extensies). Bestanden in Office-indeling bevatten ook OLE-objecten. Het programma scant office-bestanden die kleiner zijn dan 1 MB, ongeacht of het selectievakje is ingeschakeld of niet.
Bestanden in e-mailindeling scannen	Het scannen van e-mailindelingen en de e-maildatabase. Het programma scant PST- en OST-bestanden gebruikt door MS Outlook en Windows Mail e-mailclients, evenals EML-bestanden. Kaspersky Endpoint Security biedt geen ondersteuning voor de 64-bits versie van de Microsoft Outlook-mailclient. Dit betekent dat Kaspersky Endpoint Security geen Microsoft Outlook-bestanden (PST- en OST-bestanden) scant als een 64-bit versie van Microsoft Outlook op de computer is geïnstalleerd, zelfs als e-mail is opgenomen in het scanbereik. 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. Als dit selectievakje is uitgeschakeld, scant Kaspersky Endpoint Security het bestand met de e-mailindeling als een enkel bestand. Wanneer een kwaadaardig object wordt ontdekt in PST- of OST-bestanden, maakt Kaspersky Endpoint Security het onschadelijk in overeenstemming met de geselecteerde actie (bijvoorbeeld desinfectie of verwijdering van het bestand). Wanneer een kwaadaardig bestand wordt gedetecteerd in bestanden van andere e-mailclients (bijvoorbeeld Mozilla Thunderbird), markeert Kaspersky Endpoint Security alleen het geïnfecteerde bericht. U moet het bericht met een geïnfecteerde bijlage handmatig verwijderen.
Scan wachtwoordbeveiligde archieven	Als het selectievakje is ingeschakeld, worden archieven met wachtwoordbeveiliging gescand door het programma. 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 het programma.
Pak grote samengestelde bestanden niet uit	Als dit selectievakje is ingeschakeld, scant het programma geen samengestelde bestanden als ze groter zijn dan de opgegeven waarde. Als dit selectievakje is uitgeschakeld, worden samengestelde bestanden van alle grootten gescand door het programma. Het programma scant grote bestanden die uit archieven worden gehaald, ongeacht of het selectievakje is ingeschakeld of niet.
Machine learning en analyse op basis van definities	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. Op aanbeveling van Kaspersky-experts is machine learning en analyse op basis van definities altijd ingeschakeld.
Heuristische analyse	De technologie is ontworpen om dreigingen te detecteren die niet met de huidige versie van de databases van het Kaspersky-programma kunnen worden gedetecteerd. De technologie detecteert bestanden die mogelijk geïnfecteerd zijn met een onbekend virus of een nieuwe variëteit van een bekend virus. 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.
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).

Programma Integriteitscontrole

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 *Programma Integriteitscontrole* is bedoeld voor het controleren van programmabestanden. Start de taak *Programma Integriteitscontrole* als Kaspersky Endpoint Security een schadelijk object heeft gevonden maar het niet heeft geneutraliseerd.

U kunt de taak *Programma 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. Selecteer **Tasks** in de structuur van de Beheerconsole van Kaspersky Security Center.

   De lijst met taken wordt geopend.

2. Klik op **New task**.

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

Stap 1. Een taaktype selecteren

Selecteer **Kaspersky Endpoint Security voor Windows 14.1.** → **Programma 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 **Run the task after the wizard finishes** 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 **Tasks**.

   De lijst met taken wordt geopend.

2. Klik op **Add**.

   De wizard Taak wordt gestart.

3. Configureer de taakinstellingen:

   a. Selecteer in de vervolgkeuzelijst **Application** de optie **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. Selecteer in de vervolgkeuzelijst **Task type** de optie **Application Integrity Check**.

c. Typ in het veld **Task name** een korte omschrijving, zoals *Integriteit van het programma controleren na een infectie*.

d. Selecteer in het gedeelte **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. Ga naar de volgende stap.

5. Selecteer een account om de taak uit te voeren. Kaspersky Endpoint Security start de taak standaard met de rechten van een lokaal gebruikersaccount.

6. Verlaat de wizard verlaten.

   U ziet een nieuwe taak in de lijst met taken.

7. 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 *Programma Integriteitscontrole* en klik op **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 de taak *Programma Integriteitscontrole* niet ziet, heeft de beheerder het gebruik van lokale taken verboden in het beleid.

Instellingen voor de taak Integriteitscontrole

Parameter	Beschrijving
Planning van scan	**Handmatig**. Uitvoermodus waarin u handmatig kunt beginnen met scannen op een moment dat het u uitkomt. **Volgens schema**. In deze uitvoermodus voor scantaken wordt de scantaak door het programma gestart volgens het schema dat u aanmaakt. Als deze uitvoermodus voor scantaken is geselecteerd, kunt u de scantaak ook handmatig starten.
Overgeslagen taken starten	Als het selectievakje is ingeschakeld, wordt de overgeslagen taak door Kaspersky Endpoint Security gestart zodra dit mogelijk is. De taak kan bijvoorbeeld worden overgeslagen als de computer uitgeschakeld was op de starttijd van de taak. Als het programma een kans krijgt om gemiste taken uit te voeren, start het de taken willekeurig binnen een bepaalde tijdsinterval om de lading voor de computer te spreiden. Als het selectievakje is uitgeschakeld, worden overgeslagen taken niet gestart door Kaspersky Endpoint Security. In plaats daarvan voert het de volgende taak uit volgens het huidige schema.
Alleen starten als de computer inactief is	Uitgestelde start van de taak 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. Met deze planningsoptie kunt u computervermogen besparen wanneer de computer wordt gebruikt.

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 taken *Volledige Scan* en *Kritieke Gebiedenscan* niet te veranderen.

Kaspersky Endpoint Security heeft de volgende vooraf gedefinieerde objecten als onderdeel van het scanbereik:

- **Systeemgeheugen**.
- **Lopende processen en 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**.
- **Alle harde schijven**.
- **Alle netwerkschijven**.

> In Kaspersky Endpoint Security voor Windows 12.12 valt e-mail niet onder het scanbereik van het programma. Het scannen van inkomende en uitgaande e-mails wordt uitgevoerd door het onderdeel Mail Threat Protection. Als u een oudere versie van de beheerplug-in gebruikt, sluit het programma e-mail uit van het scanbereik, zelfs als het beleid deze wel bevat.

> We raden u aan een aparte scantaak te maken voor het scannen van netwerkstations of gedeelde mappen. In de instellingen van de *Malware-scan* taak, geef een gebruiker op die schrijftoegang heeft tot deze schijf; dit is nodig om gedetecteerde bedreigingen te beperken. Als de server waar de netwerkschijf zich bevindt zijn eigen beveiligingshulpmiddelen heeft, voer dan de scantaak niet uit voor die schijf. Op deze manier kunt u voorkomen dat objecten twee keer worden gecontroleerd en de prestaties van de server verbeteren.

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. Selecteer in de beheerconsole **Tasks**.
3. Selecteer de scantaak en dubbelklik om de taakeigenschappen te openen.

   Maak indien nodig de *Malware-scan*-taak aan.
4. Selecteer het gedeelte **Instellingen** in het venster met taakeigenschappen.
5. Klik in het gedeelte **Scanbereik** op **Instellingen**.
6. Selecteer in het venster dat opent de objecten die u aan het scanbereik wilt toevoegen of daarvan wilt uitsluiten.

7. 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:\Folder\**\*.txt` omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen bevinden genest in de `Folder`, uitgezonderd de `Folder` 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:\Folder\???.txt` omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam `Folder` bevinden, die een TXT-extensie hebben en die een naam met drie tekens hebben.

      U kunt maskers overal in een bestands- of mappad gebruiken. Als u bijvoorbeeld wilt dat het scanbereik de map Downloads bevat voor alle gebruikersaccounts op de computer, voert u het masker `C:\Users\*\Downloads\` uit.

      Het object **Deze pc** in de lijst van bestandsbronnen van de computer omvat de volgende objecten: **Alle harde schijven**, **Alle netwerkschijven** en **Alle verwisselbare schijven**.

   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. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Een scanuitzondering bewerken via de Webconsole en Cloudconsole

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

   De lijst met taken wordt geopend.

2. Klik op de scantaak.

   U ziet nu het venster met de taakeigenschappen. Maak indien nodig de *Malware Scan*-taak aan.

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 **Add**.

   b. Voer 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:\Folder\**\*.txt` omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen bevinden genest in de `Folder`, uitgezonderd de `Folder` 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:\Folder\???.txt` omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam `Folder` bevinden, die een TXT-extensie hebben en die een naam met drie tekens hebben.

U kunt maskers overal in een bestands- of mappad gebruiken. Als u bijvoorbeeld wilt dat het scanbereik de map Downloads bevat voor alle gebruikersaccounts op de computer, voert u het masker `C:\Users\*\Downloads\` uit.

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. U ziet nu de lijst met taken: selecteer de taak *Aangepaste Scan* en klik op **Selecteren**.

   U kunt ook het scanbereik voor andere taken bewerken. Kaspersky-experts raden u aan het scanbereik van de taken *Volledige Scan* en *Kritieke Gebiedenscan* niet te veranderen.

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

Scannen op malware met de *Malware-scan* taak kan tijdrovend zijn en kan het gebruik van computerbronnen door Kaspersky Endpoint Security verhogen. Daarom wordt aanbevolen een optimaal tijdstip te selecteren om de taak uit te voeren, zodat de impact op de prestaties van andere programma's tot een minimum wordt beperkt.

Als werknemers in uw organisatie bijvoorbeeld volgens een vast schema werken, kunt u een computerscan zo configureren dat deze 's nachts of in het weekend wordt uitgevoerd. Als de taak 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. Deze functie moet met de nodige voorzichtigheid worden gebruikt, aangezien deze programma's op de computer van de gebruiker kan vertragen wanneer de computer 's ochtends wordt aangezet.

Als u geen optimaal schema voor scans voor uw behoeften kunt bepalen, kunt u de scan configureren om te worden uitgevoerd wanneer aan een van 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 na een bepaalde tijd na het opstarten 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.

- Wake-on-LAN-functie.

  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 *Malware-scan* 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. In dit geval kan de Volledige Scan enkele dagen duren.

- Wanneer de taak is overgeslagen.

  Kaspersky Endpoint Security voert de overgeslagen taak uit zodra dit mogelijk is. De taak kan bijvoorbeeld worden overgeslagen als de computer uitgeschakeld was op de starttijd van de taak. Als het programma een kans krijgt om gemiste taken uit te voeren, start het de taken willekeurig binnen een bepaalde tijdsinterval om de lading voor de computer te spreiden.

Het schema voor scans configureren via de Webconsole en Cloudconsole

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

   De lijst met taken wordt geopend.

2. Klik op de scantaak.

   U ziet nu het venster met de taakeigenschappen.

3. Selecteer het tabblad **Schedule** in het venster met taakeigenschappen.

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 *Malware-scan* 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
Planning van scan	**Handmatig**. Uitvoermodus waarin u handmatig kunt beginnen met scannen op een moment dat het u uitkomt. **Volgens schema**. In deze uitvoermodus voor scantaken wordt de scantaak door het programma gestart volgens het schema dat u aanmaakt. Als deze uitvoermodus voor scantaken is geselecteerd, kunt u de scantaak ook handmatig starten.
Start na programmastart uitstellen met N minuten	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.
Overgeslagen taken starten	Als het selectievakje is ingeschakeld, wordt de overgeslagen taak door Kaspersky Endpoint Security gestart zodra dit mogelijk is. De taak kan bijvoorbeeld worden overgeslagen als de computer uitgeschakeld was op de starttijd van de taak. Als het programma een kans krijgt om gemiste taken uit te voeren, start het de taken willekeurig binnen een bepaalde tijdsinterval om de lading voor de computer te spreiden. Als het selectievakje is uitgeschakeld, worden overgeslagen taken niet gestart door Kaspersky Endpoint Security. In plaats daarvan voert het de volgende taak uit volgens het huidige schema.
Alleen starten als de computer inactief is	Uitgestelde start van de taak 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. Met deze planningsoptie kunt u computervermogen besparen wanneer de computer wordt gebruikt.
Use automatically randomized delay for task starts *(alleen beschikbaar in de Kaspersky Security Center-console)*	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. 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. Als het selectievakje is uitgeschakeld, wordt de taak precies op het geplande tijdstip uitgevoerd.
Use randomized delay for task starts within an interval of (min)	Als dit selectievakje is ingeschakeld, wordt de taak uitgevoerd op computers op een willekeurig tijdstip binnen een bepaald tijdsbestek. 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. Als het selectievakje is uitgeschakeld, wordt de taak precies op het geplande tijdstip uitgevoerd.

Parameter	Beschrijving
Stop the task if it runs longer than (min) *(alleen beschikbaar in de Kaspersky Security Center-console)*	De taakuitvoeringstijd 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. Om de uitvoeringstijd van de taak te verkorten, kunt u bijvoorbeeld het scanbereik configureren of de scan optimaliseren.
Turn on devices by using the Wake-on-LAN function before starting the task (min) *(alleen beschikbaar in de Kaspersky Security Center-console)*	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. Schakel het selectievakje in als u de taak wilt uitvoeren op alle computers, inclusief computers die uit staan.
Shut down the devices after completing the task *(alleen beschikbaar in de Kaspersky Security Center-console)*	U kunt deze functie bijvoorbeeld inschakelen om de computer op vrijdag na werktijd te scannen. Wanneer de taak is voltooid, schakelt het programma de computer uit voor het weekend.
Taak pauzeren	U kunt een tijdsinterval opgeven waarin de uitvoering van een eerder geplande taak wordt gepauzeerd. Zodra de opgegeven periode is verstreken, wordt de taak hervat. Dit kan bijvoorbeeld nodig zijn om de impact van Kaspersky Endpoint Security op de prestaties van de computer tijdens perioden van piekgebruik te minimaliseren.
Schema uitschakelen vanaf	Als het selectievakje is ingeschakeld, stopt Kaspersky Endpoint Security met het uitvoeren van de geplande taak vanaf de opgegeven datum. De taak wordt ingesteld op **Handmatig**-modus.

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 het programma 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 **Tasks**.
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 **Asset management** → **Tasks**.
   De lijst met taken wordt geopend.
2. Klik op de scantaak.
   U ziet nu het venster met de taakeigenschappen.
3. Selecteer het tabblad **Settings**.
4. In het blok **Account**, klikt u op de knop **Settings**.
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

CPU-gebruik beperken tijdens het scannen van de computer

U kunt het CPU-gebruik beperken wanneer u de taak *Malware-scan* uitvoert. Hierdoor kan het langer duren om uw computer te scannen.

Het CPU-gebruik beperken bij het scannen van de computer in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

3. Selecteer **Algemene instellingen** → **Programma-instellingen** in het beleidsvenster.

4. Onder **Prestaties**, selecteer de **Beperk CPU-gebruik voor scantaken** selectievakje en voer de gemiddelde waarde van het CPU-bronverbruik in procenten in.

5. Sla uw wijzigingen op.

Het CPU-gebruik beperken bij het scannen van de computer in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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** → **Performance**.

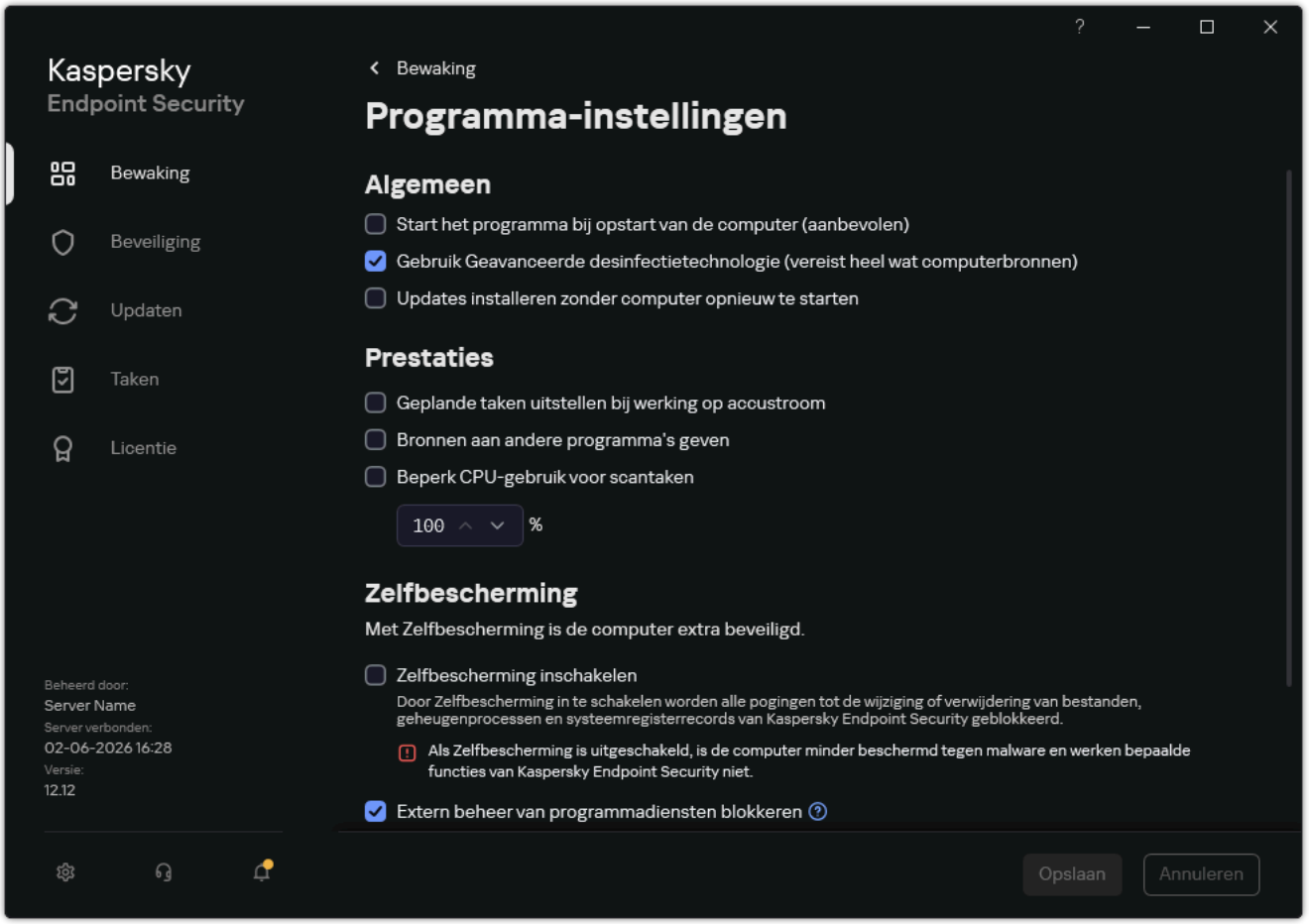
5. Zet Onder **Limit CPU usage for scan tasks**, de schakelaarop **Limit CPU usage for scan tasks** en voer de gemiddelde waarde van het CPU-bronverbruik in procenten in.

6. Sla uw wijzigingen op.

Hoe het CPU-gebruik te beperken bij het scannen van de computer in het 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.



Instellingen Kaspersky Endpoint Security voor Windows

3. Onder **Prestaties**, selecteer de **Beperk CPU-gebruik voor scantaken** selectievakje en voer de gemiddelde waarde van het CPU-bronverbruik in procenten in.

4. Sla uw wijzigingen op.

Geavanceerde taakinstellingen configureren voor: Malware-scan.

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. Selecteer in de beheerconsole **Tasks**.

3. Selecteer de scantaak en dubbelklik om de taakeigenschappen te openen.

   Maak indien nodig de *Malware-scan*-taak aan.

4. Selecteer het gedeelte **Instellingen** in het venster met taakeigenschappen.

5. In het blok **Beveiligingsniveau**, klikt u op de knop **Instellingen**.

   U ziet nu het venster met de instellingen van de scantaak.

6. Configureer in het blok **Optimalisatie** 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 bestanden over waarvan scan langer duurt dan N s**. De taakuitvoeringstijd 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.

- **Laat niet meerdere scantaken tegelijk lopen**. Uitgestelde start van scantaken als er al een scan loopt. Kaspersky Endpoint Security zal nieuwe scantaken in de wachtrij plaatsen als de huidige scan doorgaat. Dit helpt de belasting op de computer te optimaliseren. Laten we er bijvoorbeeld vanuit gaan dat het programma volgens het schema een volledige scantaak heeft gestart. Als een gebruiker probeert een snelle scan te starten vanuit de programma-interface, zal Kaspersky Endpoint Security deze snelle scan-taak in de wachtrij plaatsen en deze taak automatisch starten nadat de volledige scantaak is voltooid.

7. Klik op **Extra**.

   U ziet nu het venster met instellingen voor het scannen van samengestelde bestanden.

8. Schakel in het blok **Maximale grootte** het selectievakje **Grote samengestelde bestanden niet uitpakken** in. De taakuitvoeringstijd 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.

   Kaspersky Endpoint Security scant grote bestanden die uit archieven zijn uitgepakt, ongeacht of het selectievakje **Grote samengestelde bestanden niet uitpakken** is ingeschakeld.

9. Klik op **OK**.

10. Ga naar het tabblad **Extra**.

11. 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).

12. Sla uw wijzigingen op.

Scans optimaliseren via de Webconsole en Cloudconsole

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

   De lijst met taken wordt geopend.

2. Klik op de scantaak.

   U ziet nu het venster met de taakeigenschappen. Maak indien nodig de *Malware Scan*-taak aan.

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

4. Schakel in het blok **Action on threat detection** het selectievakje **Scan only new and modified 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 in het blok **Scan optimization** het selectievakje **Do not unpack large compound files** in. De taakuitvoeringstijd 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.

   > Kaspersky Endpoint Security scant grote bestanden die uit archieven zijn uitgepakt, ongeacht of het selectievakje **Do not unpack large compound files** is ingeschakeld.

6. Selecteer het selectievakje **Do not run multiple scan tasks at the same time**. Uitgestelde start van scantaken als er al een scan loopt. Kaspersky Endpoint Security zal nieuwe scantaken in de wachtrij plaatsen als de huidige scan doorgaat. Dit helpt de belasting op de computer te optimaliseren. Laten we er bijvoorbeeld vanuit gaan dat het programma volgens het schema een volledige scantaak heeft gestart. Als een gebruiker probeert een snelle scan te starten vanuit de programma-interface, zal Kaspersky Endpoint Security deze snelle scan-taak in de wachtrij plaatsen en deze taak automatisch starten nadat de volledige scantaak is voltooid.

7. Schakel in het blok **Advanced settings** het selectievakje **Skip file that is scanned for longer than (sec)** in. De taakuitvoeringstijd 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.

8. 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 **Optimalisatie** de scaninstellingen:

   - **Scan alleen nieuwe en aangepaste 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 bestand over waarvan scan langer duurt dan N seconden**. De taakuitvoeringstijd 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.

- **Start geen meerdere scantaken tegelijk**. Uitgestelde start van scantaken als er al een scan loopt. Kaspersky Endpoint Security zal nieuwe scantaken in de wachtrij plaatsen als de huidige scan doorgaat. Dit helpt de belasting op de computer te optimaliseren. Laten we er bijvoorbeeld vanuit gaan dat het programma volgens het schema een volledige scantaak heeft gestart. Als een gebruiker probeert een snelle scan te starten vanuit de programma-interface, zal Kaspersky Endpoint Security deze snelle scan-taak in de wachtrij plaatsen en deze taak automatisch starten nadat de volledige scantaak is voltooid.

5. Schakel in het blok **Beperking van grootte** het selectievakje **Pak grote samengestelde bestanden niet uit** in. De taakuitvoeringstijd 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.

   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.

Update-functionaliteit (inclusief het leveren van updates van antivirussignaturen en codebase-updates) is mogelijk niet beschikbaar in het programma in de Verenigde Staten.

Voor periodieke updates hebt u een actieve licentie nodig. Zonder actieve licentie kunt u maar één keer een update uitvoeren.

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.

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.

Als het programma in de Light Agent-modus werkt, zijn er speciale overwegingen bij het bijwerken van programmadatabases en modules.

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 wordt op computers van gebruikers geüpdatet:

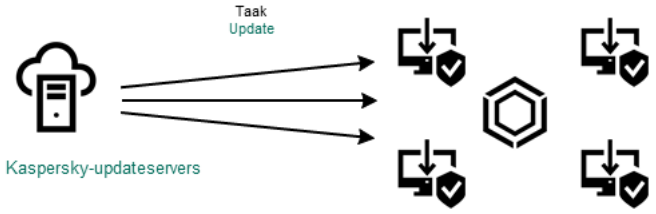
- Antivirusdatabases. De antivirusdatabases bevatten databases met definities van malware, beschrijvingen van netwerkaanvallen, databases met schadelijke webadressen en phishingadressen, databases met banners, databases met spam en andere gegevens.

- 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.



Updaten vanaf Kaspersky-servers

- 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 *Download updates to the Administration Server repository*.

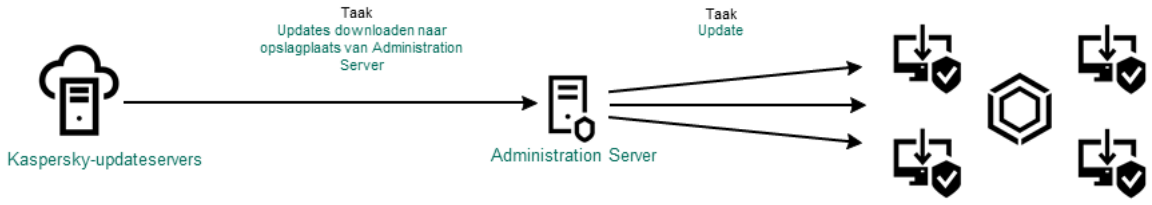
  2. Download het updatepakket naar een gedeelde map (optioneel).

Op de volgende manieren kunt u het updatepakket naar een gedeelde map downloaden:

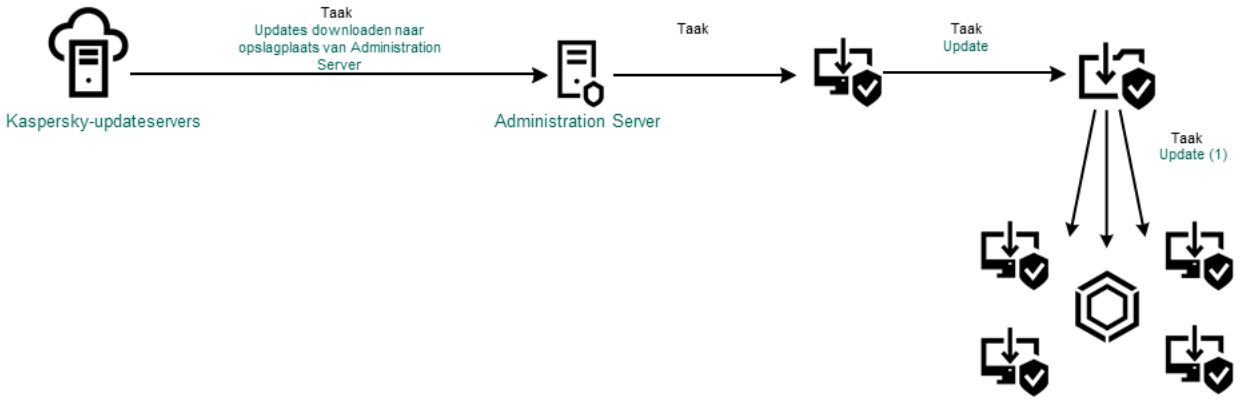
- Met de taak *Update van databases en programmamodules* van Kaspersky Endpoint Security. De taak is bedoeld voor een van de computers in het lokale bedrijfsnetwerk.
- Met Kaspersky Update Utility. Voor gedetailleerde informatie over het gebruik van Kaspersky Update Utility raadpleegt u de Knowledge Base van Kaspersky.

3. Verstuur het updatepakket naar clientcomputers.

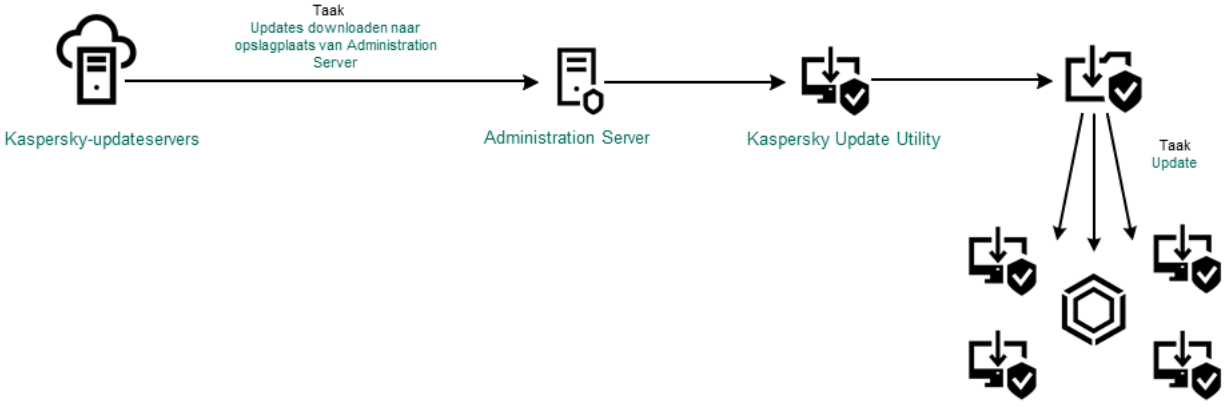
   Het updatepakket wordt naar clientcomputers verspreid met de taak *Update van databases en programmamodules* van Kaspersky Endpoint Security. U kunt een onbeperkt aantal updatetaken voor elke beheergroep maken.



Updaten vanaf een opslagplaats op een server



Updaten vanaf een gedeelde map



Updaten met Kaspersky Update Utility

Voor Kaspersky Security Center 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. Een updatepakket downloaden naar de opslagplaats van de Administratioon Server (*Download updates to the Administration Server repository* task).

   De taak *Download updates to the Administration Server repository* wordt automatisch gemaakt door de snelstart-wizard van de Administration Server en deze taak heeft mogelijk slechts één exemplaar. Standaard kopieert Kaspersky Security Center het updatepakket naar de map `\\<server name>\KLSHARE\Updates`. Voor meer informatie over het downloaden van updates in het Administration Server-archief raadpleegt u de Help van Kaspersky Security Center.

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 *Update van databases en programmamodules*).

   Kaspersky Endpoint Security-update configureren vanaf de opgegeven serveropslag in de Administration Console (MMC)

   1. Open de Beheerconsole van Kaspersky Security Center.

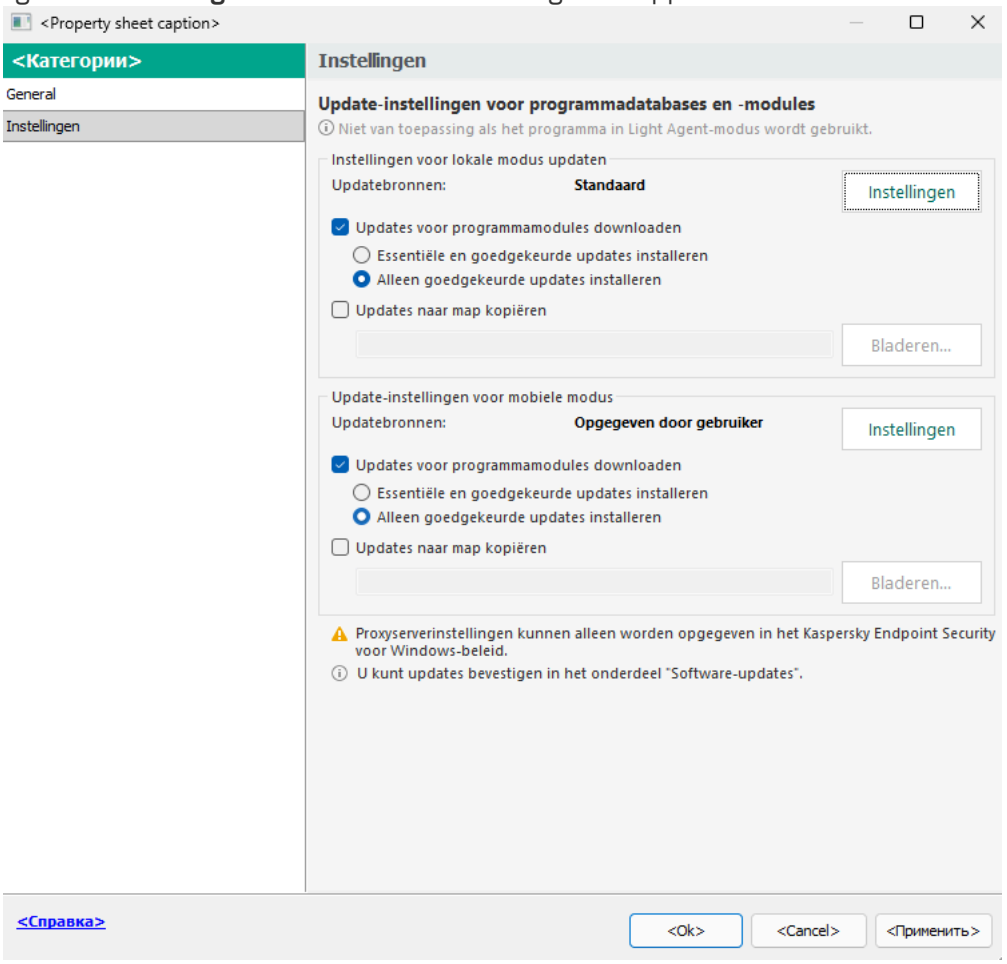
      Selecteer in de beheerconsole **Tasks**.

   2. Klik op de taak **Update van databases en programmamodules** van Kaspersky Endpoint Security.

      U ziet nu het venster met de taakeigenschappen.

      De taak *Update van databases en programmamodules* wordt automatisch gemaakt door de snelstart-wizard van de Administration Server. Voor het maken van de taak *Update van databases en programmamodules* installeert u de beheerplug-in van Kaspersky Endpoint Security voor Windows wanneer u de stappen van de wizard volgt.

3. Selecteer het gedeelte **Settings** in het venster met taakeigenschappen.



Instellingen van Update van databases en programmamodules-taak

4. In het blok **Instellingen voor lokale modus updaten**, klikt u op de knop **Instellingen**.

5. In de lijst met updatebronnen, zorg ervoor dat de update van de bron **Kaspersky Security Center** ingeschakeld is. Bovendien moet de bron **Kaspersky Security Center** de hoogste prioriteit krijgen.

6. Voeg indien nodig de updatebronnen toe:

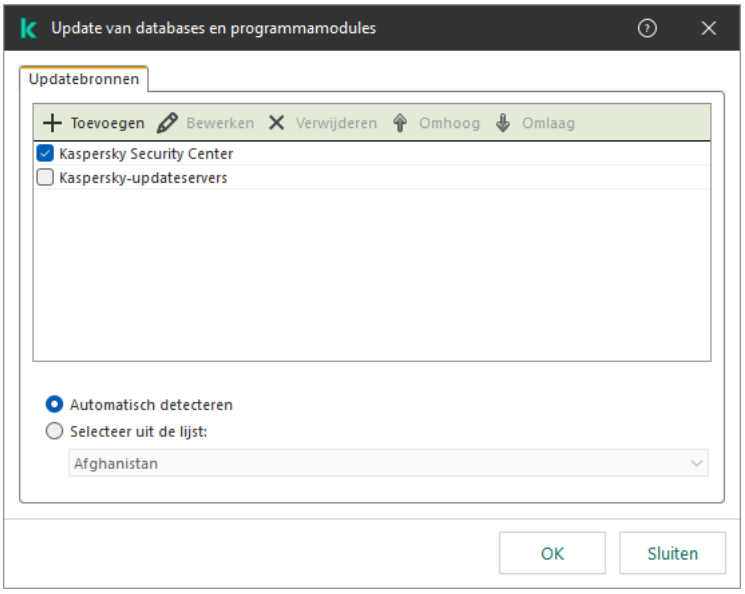
   a. Klik in de lijst met updatebronnen op de knop **Toevoegen**.

   b. Geef in het veld **Updatebronnen** 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 (taak *Download updates to the Administration Server repository*).

   c. Klik op **OK**.

U kunt de updatebron uitsluiten zonder deze uit de lijst met updatebronnen te verwijderen. Schakel hiervoor het selectievakje naast het object uit.



Updatebronnen

7. Configureer de prioriteiten van updatebronnen met de knoppen **Omhoog** en **Omlaag**.

   Als een update niet kan worden uitgevoerd vanaf de eerste updatebron, schakelt Kaspersky Endpoint Security automatisch over naar de volgende bron.

8. Selecteer in het venster met taakeigenschappen het gedeelte **Schedule** en configureer de taakuitvoermodus.

9. Standaard voert Kaspersky Endpoint Security de taak uit in de handmatige modus.

10. Sla uw wijzigingen op.

Zo configureert u het updaten van Kaspersky Endpoint Security vanaf de opgegeven opslagplaats in de webconsole

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

   De lijst met taken wordt geopend.

2. Klik op de taak **Update** van Kaspersky Endpoint Security.

   U ziet nu het venster met de taakeigenschappen.

   De taak *Update* wordt automatisch gemaakt door de snelstart-wizard van de Administration Server. Voor het maken van de taak *Update* installeert u de beheerplug-in van Kaspersky Endpoint Security voor Windows wanneer u de stappen van de wizard volgt.

3. Selecteer het tabblad **Application settings → Local mode**.

4. In de lijst met updatebronnen, zorg ervoor dat de update van de bron **Kaspersky Security Center** ingeschakeld is. Bovendien moet de bron **Kaspersky Security Center** de hoogste prioriteit krijgen.

5. Voeg indien nodig de updatebronnen toe:

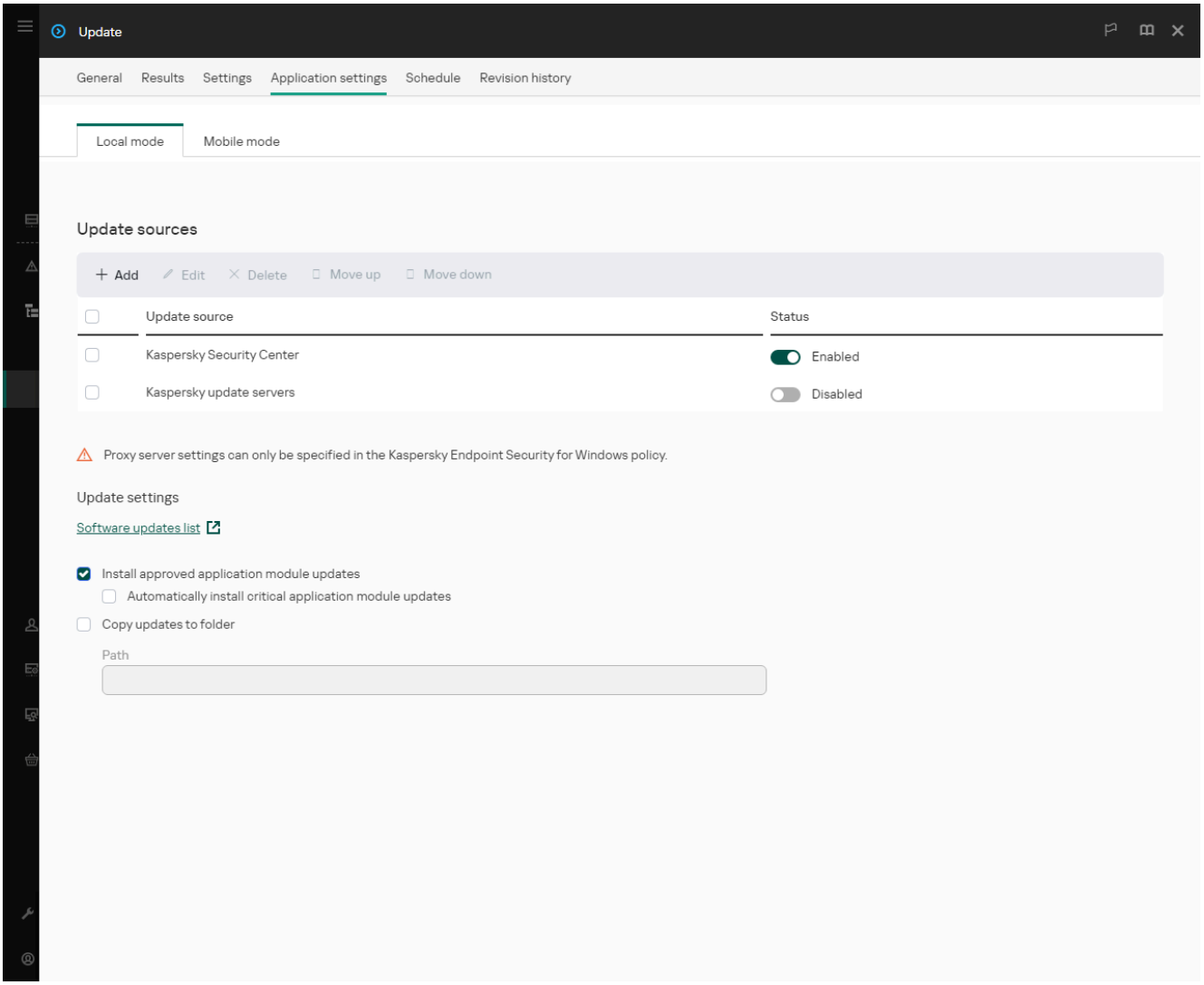
   a. Klik in de lijst met updatebronnen op de knop **Add**.

   b. Geef in het veld **Update sources** 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 (taak *Download updates to the Administration Server repository*).

   c. Klik op **Save**.

   U kunt de updatebron uitsluiten zonder deze uit de lijst met updatebronnen te verwijderen. Dat doet u door de schakelaar ernaast uit te zetten.



Updatebronnen

6. Configureer de prioriteiten van updatebronnen met de knoppen **Up** en **Down**.

   Als een update niet kan worden uitgevoerd vanaf de eerste updatebron, schakelt Kaspersky Endpoint Security automatisch over naar de volgende bron.

7. Selecteer in het venster met taakeigenschappen het gedeelte **Schedule** en configureer de taakuitvoermodus.

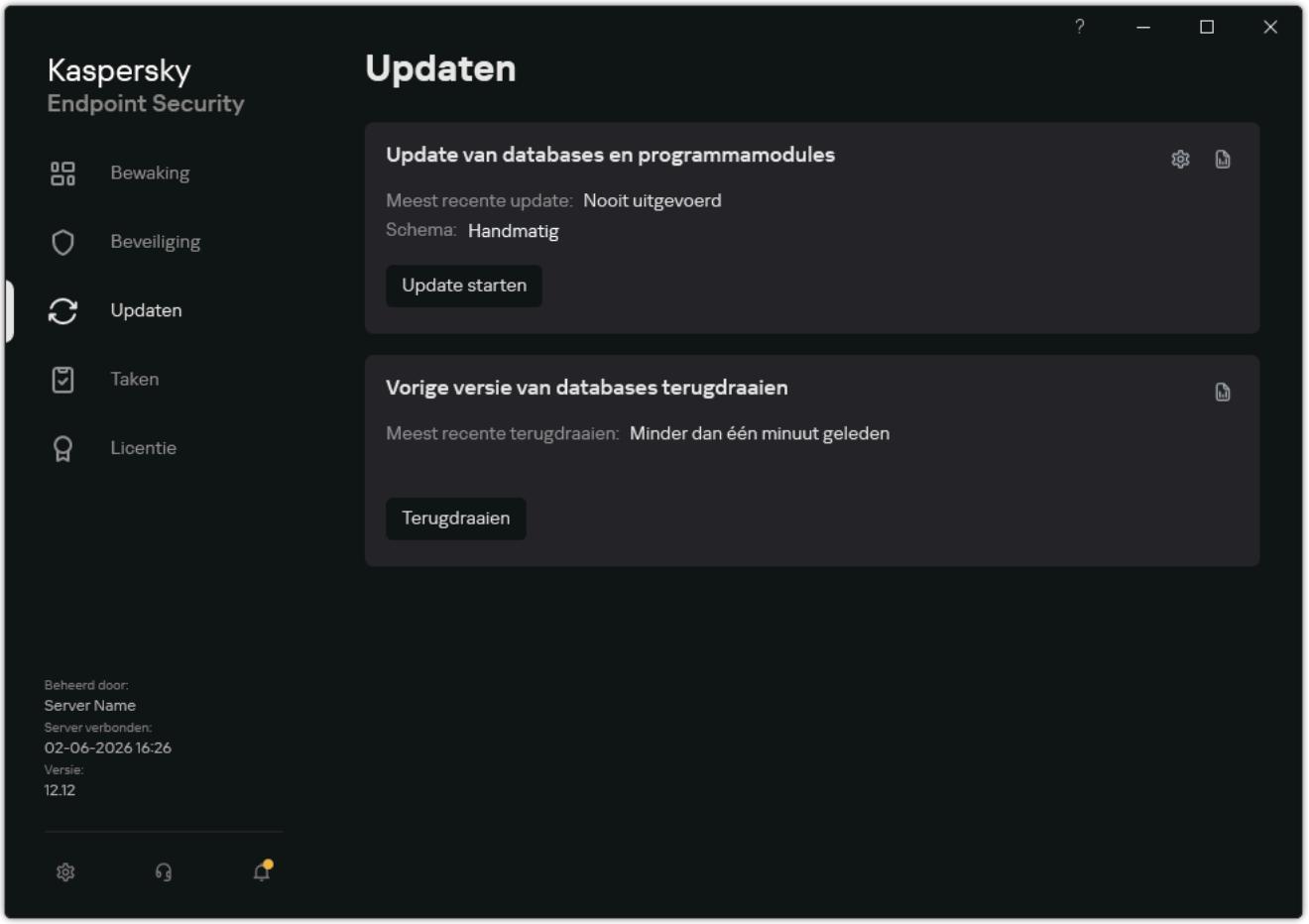
8. Standaard voert Kaspersky Endpoint Security de taak uit in de handmatige modus.

9. Sla uw wijzigingen op.

Zo configureert u het updaten van Kaspersky Endpoint Security vanaf de opgegeven opslagplaats op de server in de interface van het programma:

U kunt de groepstaak *Update van databases en programmamodules* niet configureren in de interface van het programma. Er is alleen een lokale updatetaak *Update van databases en programmamodules* beschikbaar voor de gebruiker. Als u de taak *Update van databases en programmamodules* niet ziet, heeft de beheerder het gebruik van lokale taken verboden in het beleid.

1. Ga in het hoofdvenster van het programma naar het gedeelte **Updaten**.



Lokale updatetaken

2. U ziet nu de lijst met taken: selecteer de taak *Update van databases en programmamodules* en klik op ⚙.

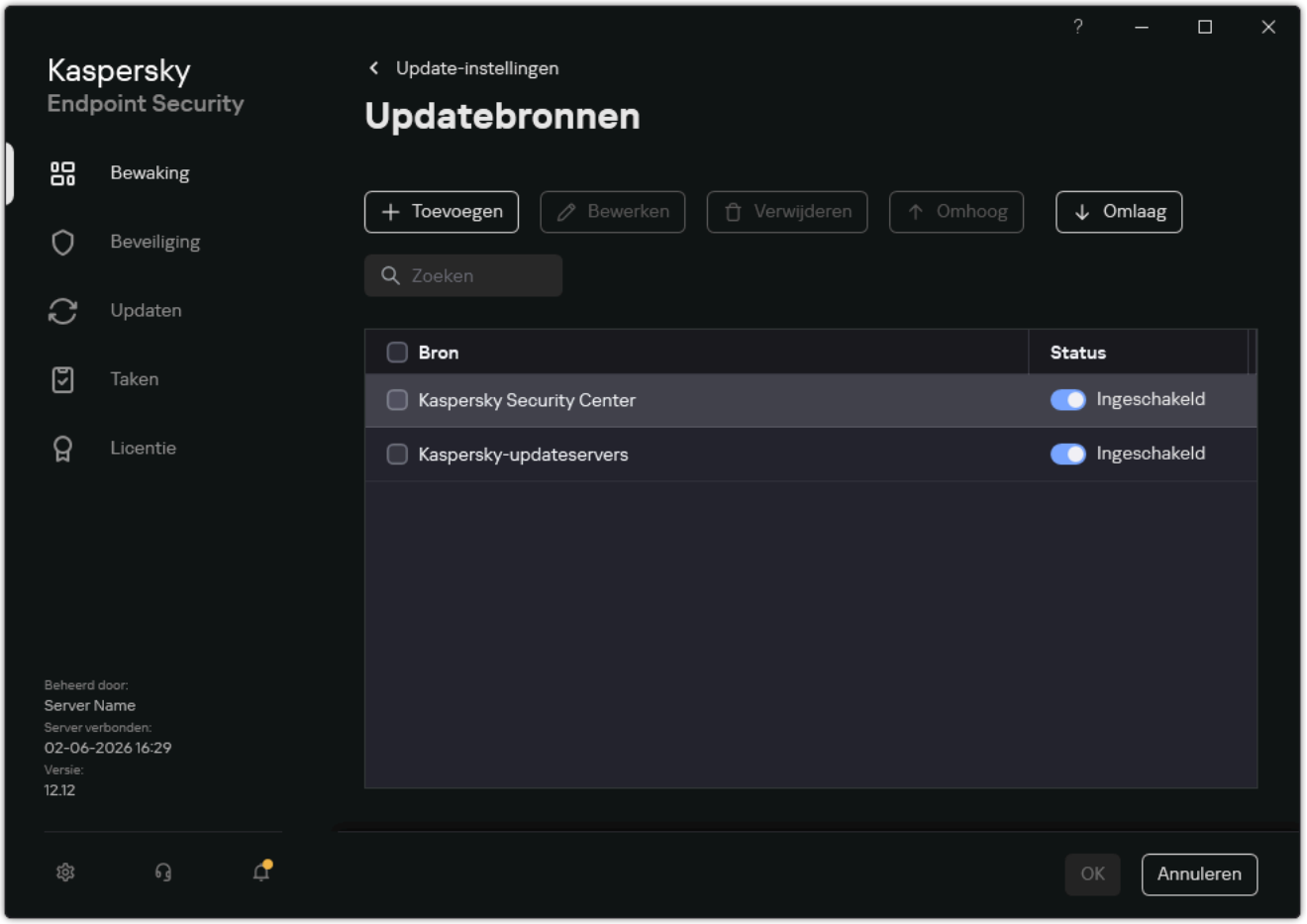
   U ziet nu het venster met de taakeigenschappen.

3. Klik in het venster taakeigenschappen op **Updatebronnen selecteren**.

4. In de lijst met updatebronnen, zorg ervoor dat de update van de bron **Kaspersky Security Center** ingeschakeld is. Bovendien moet de bron **Kaspersky Security Center** de hoogste prioriteit krijgen.

5. Voeg indien nodig de updatebronnen toe:

   a. Klik in de lijst met updatebronnen op de knop **Toevoegen**.



Updatebronnen

   a. Geef 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 (taak *Download updates to the Administration Server repository*).

   b. Klik op **Selecteren**.

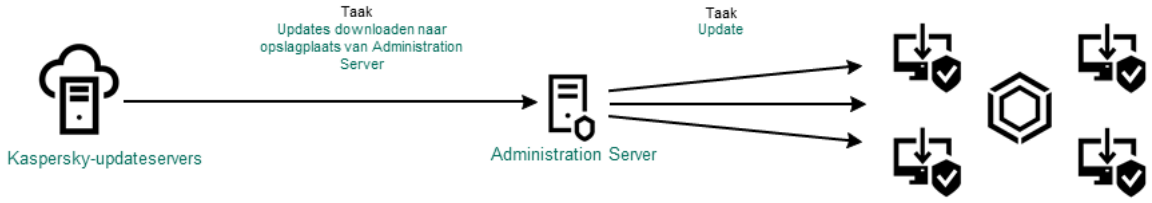
   U kunt de updatebron uitsluiten zonder deze uit de lijst met updatebronnen te verwijderen. Dat doet u door de schakelaar ernaast uit te zetten.

6. Configureer de prioriteiten van updatebronnen met de knoppen **Omhoog** en **Omlaag**.

   Als een update niet kan worden uitgevoerd vanaf de eerste updatebron, schakelt Kaspersky Endpoint Security automatisch over naar de volgende bron.

Als een computer wordt beheerd door Kaspersky Security Center, is het niet mogelijk om de uitvoeringsmodus te configureren voor de taak *Update van databases en programmamodules*. U kunt de taak alleen handmatig uitvoeren.

7. Sla uw wijzigingen op.



Updaten vanaf een opslagplaats op een server

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.

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.

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 lokale netwerk.

   Kopiëren van het updatepakket naar de gedeelde map inschakelen in de Beheerconsole (MMC)

   1. Open de Beheerconsole van Kaspersky Security Center.

   2. Selecteer in de beheerconsole **Tasks**.

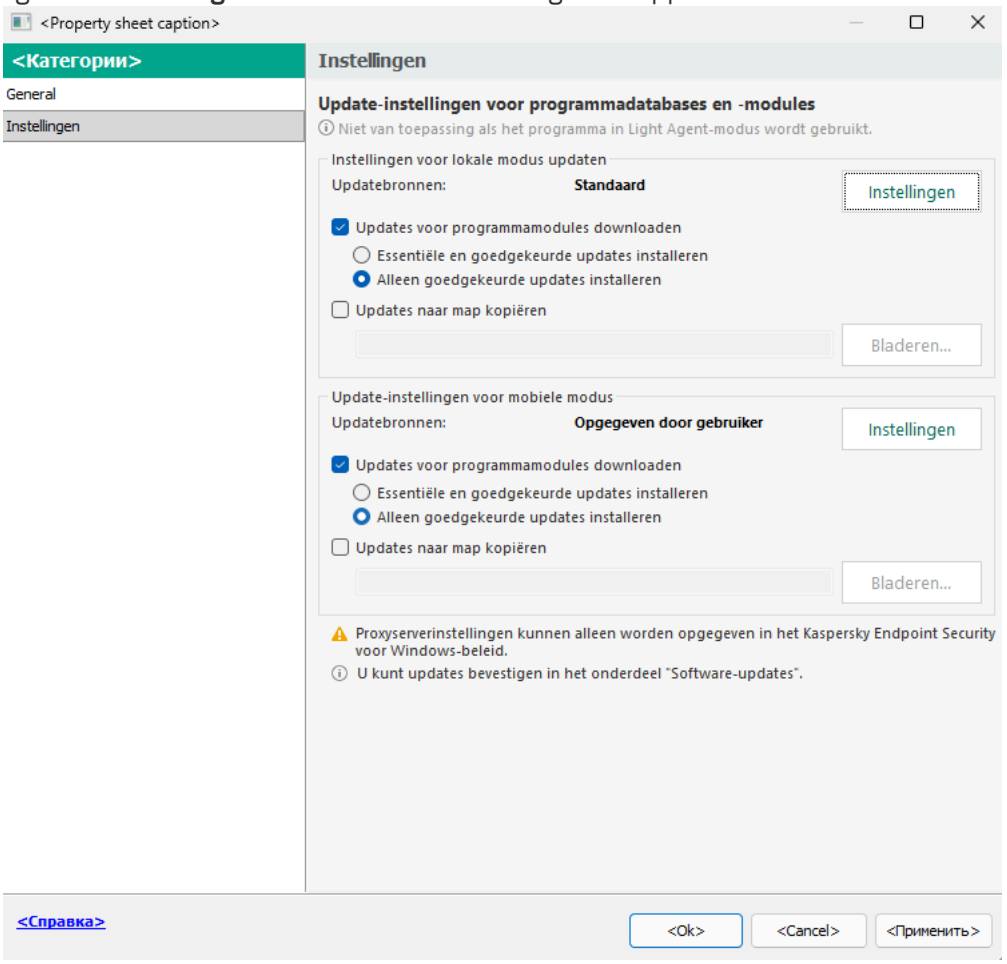
      De taak *Update van databases en programmamodules* moet toegewezen zijn aan een computer die als updatebron zal optreden.

   3. Klik op de taak **Update van databases en programmamodules** van Kaspersky Endpoint Security.

      U ziet nu het venster met de taakeigenschappen.

      De taak *Update van databases en programmamodules* wordt automatisch gemaakt door de snelstart-wizard van de Administration Server. Voor het maken van de taak *Update van databases en programmamodules* installeert u de beheerplug-in van Kaspersky Endpoint Security voor Windows wanneer u de stappen van de wizard volgt.

4. Selecteer het gedeelte **Settings** in het venster met taakeigenschappen.



Instellingen van Update van databases en programmamodules-taak

5. In het blok **Instellingen voor lokale modus updaten**, klikt u op de knop **Instellingen**.

6. Configureer de updatebronnen.

   De updatebronnen kunnen Kaspersky-updateservers, Administration Server van Kaspersky Security Center, andere FTP- of HTTP-servers, lokale mappen of netwerkmappen zijn.

7. Selecteer het selectievakje **Updates naar map kopiëren**.

8. Voer in het veld **Pad naar map** het UNC-pad naar de gedeelde map in (bijvoorbeeld `\\<server name>\KLSHARE\Updates`).

   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\AVP12\Update distribution\`.

9. Sla uw wijzigingen op.

Kopiëren van het updatepakket naar de gedeelde map inschakelen in de Webconsole en Cloudconsole.

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

   De lijst met taken wordt geopend.

   De taak *Update* moet toegewezen zijn aan een computer die als updatebron zal optreden.

2. Klik op de taak **Update** van Kaspersky Endpoint Security.

U ziet nu het venster met de taakeigenschappen.

De taak *Update* wordt automatisch gemaakt door de snelstart-wizard van de Administration Server. Voor het maken van de taak *Update* installeert u de beheerplug-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. Selecteer het selectievakje **Copy updates to folder**.

6. Voer in het veld **Path** het UNC-pad naar de gedeelde map in (bijvoorbeeld `\\<server name>\KLSHARE\Updates`).

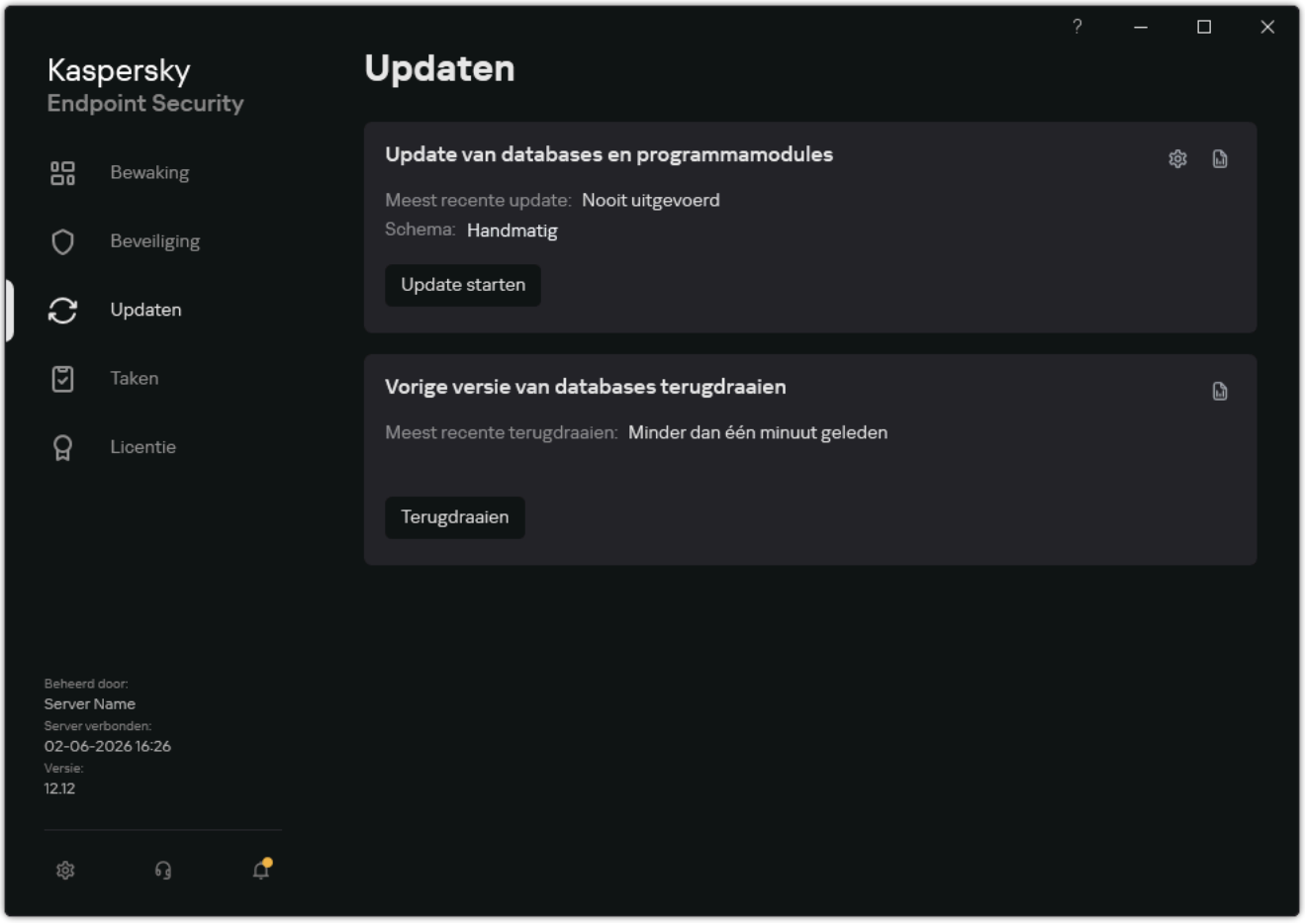
   Als het veld leeg wordt gelaten, kopieert Kaspersky Endpoint Security het updatepakket naar de map `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

7. Sla uw wijzigingen op.

Kopiëren van het updatepakket naar de gedeelde map inschakelen in de programma-interface

U kunt de groepstaak *Update van databases en programmamodules* niet configureren in de interface van het programma. Er is alleen een lokale updatetaak *Update van databases en programmamodules* beschikbaar voor de gebruiker. Als u de taak *Update van databases en programmamodules* niet ziet, heeft de beheerder het gebruik van lokale taken verboden in het beleid.

1. Ga in het hoofdvenster van het programma naar het gedeelte **Updaten**.



Lokale updatetaken

2. U ziet nu de lijst met taken: selecteer de taak *Update van databases en programmamodules* en klik op ⚙.

   U ziet nu het venster met de taakeigenschappen.

3. Schakel in het blok **Updates distribueren** het selectievakje **Updates naar map kopiëren** in.

4. Voer het UNC-pad naar de gedeelde map in (bijvoorbeeld `\\<server name>\KLSHARE\Updates`).

5. Sla uw wijzigingen op.

3. Configureer het ophalen van updates voor databases en programmamodules in de gedeelde map voor de resterende computers in het bedrijfsnetwerk.

Updates configureren vanuit de gedeelde folder via de Beheerconsole (MMC)

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

   De lijst met taken wordt geopend.

2. Klik op **Add**.

   De wizard Taak wordt gestart.

3. Configureer de taakinstellingen:

   a. Selecteer in de vervolgkeuzelijst **Application** de optie **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. Selecteer in de vervolgkeuzelijst **Task type** de optie **Update van databases en programmamodules**.

4. Selecteer **Tasks** in de structuur van de Beheerconsole van Kaspersky Security Center.

   De lijst met taken wordt geopend.

5. Klik op **New task**.

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

Stap 1. Een taaktype selecteren

Selecteer **Kaspersky Endpoint Security voor Windows 14.1.** → **Update van databases en programmamodules**.

Stap 2. Updatebronnen selecteren

Voeg een nieuwe updatebron toe: een gedeelde map. Het bronadres moet overeenkomen met het adres dat u eerder hebt opgegeven in het veld **Pad naar map** wanneer u het kopiëren van het updatepakket naar de gedeelde map hebt geconfigureerd. Configureer de prioriteiten van updatebronnen met de knoppen **Omhoog** en **Omlaag**.

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.

De taak *Update van databases en programmamodules* moet toegewezen zijn aan de computers van het bedrijfsnetwerk, behalve de computer die als updatebron optreedt.

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

Selecteer een account om de *Update van databases en programmamodules* uit te voeren. Kaspersky Endpoint Security start de taak standaard met de rechten van een lokaal gebruikersaccount.

Stap 5. Een taakstartschema configureren

Configureer een schema voor het starten van een taak, bijvoorbeeld handmatig of nadat antivirusdatabases zijn gedownload naar de opslagplaats.

Stap 6. Taaknaam definiëren

Voer de naam van de taak in, bijvoorbeeld *Updaten van een gedeelde map*.

Stap 7. Aanmaak van de taak voltooien

Verlaat de wizard verlaten. Schakel indien nodig het selectievakje **Run the task after the wizard finishes** in. U kunt de voortgang van de taak volgen in de taakeigenschappen. Als resultaat wordt de updatetaak volgens het opgegeven schema uitgevoerd op de computers van de gebruikers.

Updates configureren vanuit de gedeelde map via de Webconsole en Cloudconsole

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

   De lijst met taken wordt geopend.

2. Klik op **Add**.

   De wizard Taak wordt gestart.

3. Configureer de taakinstellingen:

   a. Selecteer in de vervolgkeuzelijst **Application** de optie **Kaspersky Endpoint Security for Windows 14.1.0**.

   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 **Devices to which the task will be assigned** 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. Selecteer het tabblad **Application settings** → **Local mode**.

8. In het blok **Update sources**, klikt u op de knop **Add**.

9. 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 in het veld **Path** wanneer u het kopiëren van het updatepakket naar de gedeelde map hebt geconfigureerd (zie eerder vermelde instructies).

10. Klik op **OK**.

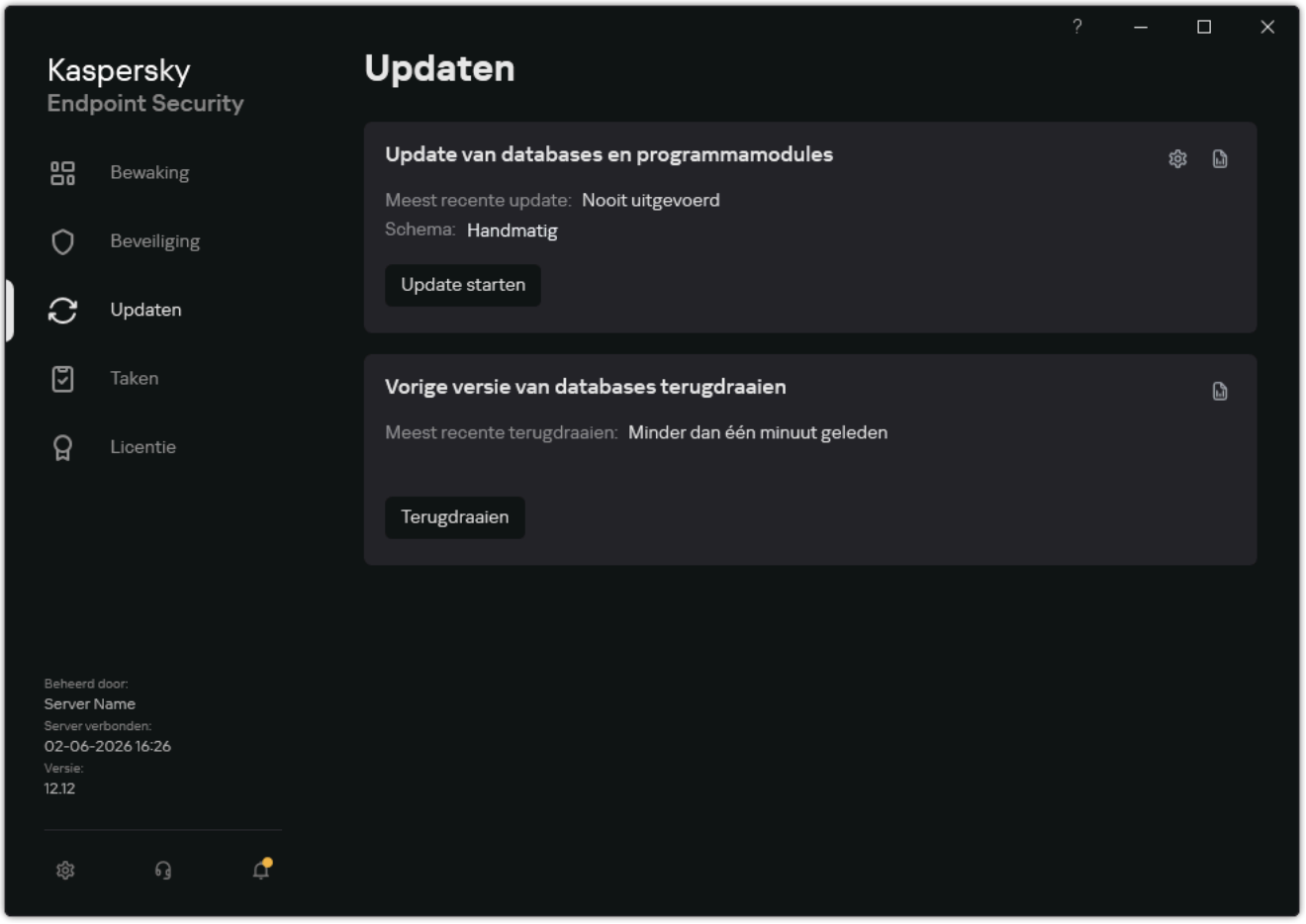
11. Configureer de prioriteiten van updatebronnen met de knoppen **Up** en **Down**.

12. Sla uw wijzigingen op.

Updates configureren vanuit de gedeelde map in de programma-interface

U kunt de groepstaak *Update van databases en programmamodules* niet configureren in de interface van het programma. Er is alleen een lokale updatetaak *Update van databases en programmamodules* beschikbaar voor de gebruiker. Als u de taak *Update van databases en programmamodules* niet ziet, heeft de beheerder het gebruik van lokale taken verboden in het beleid.

1. Ga in het hoofdvenster van het programma naar het gedeelte **Updaten**.



Lokale updatetaken

2. U ziet nu de lijst met taken: selecteer de taak *Update van databases en programmamodules* en klik op ⚙.

   U ziet nu het venster met de taakeigenschappen.

3. Klik op **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.

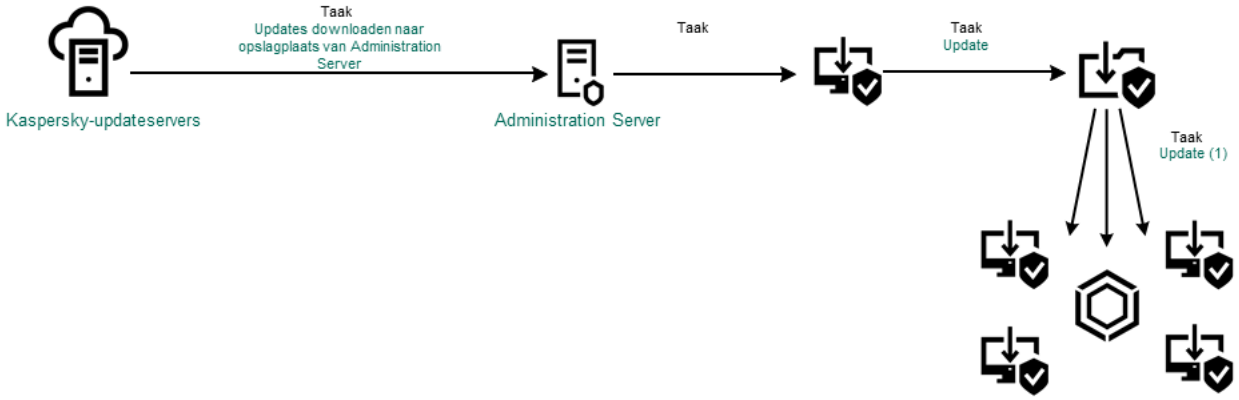
   Het bronadres moet overeenkomen met het adres dat u eerder hebt opgegeven wanneer u het kopiëren van het updatepakket naar de gedeelde map hebt geconfigureerd (zie instructies hierboven).

6. Klik op **Selecteren**.

7. Configureer de prioriteiten van updatebronnen met de knoppen **Omhoog** en **Omlaag**.

   Als een update niet kan worden uitgevoerd vanaf de eerste updatebron, schakelt Kaspersky Endpoint Security automatisch over naar de volgende bron.

8. Sla uw wijzigingen op.



Updaten vanaf een gedeelde map

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.

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.

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.

   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.

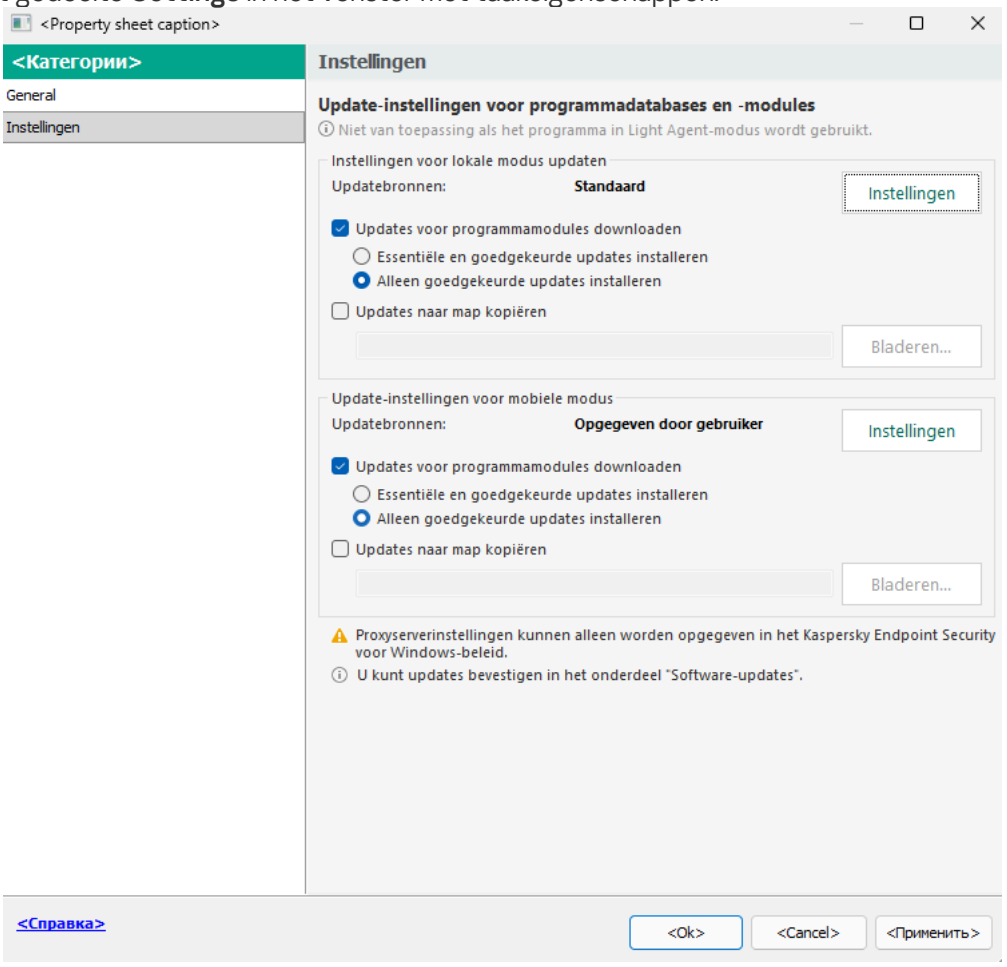
4. Configureer het ophalen van updates voor databases en programmamodules in de gedeelde map voor de resterende computers in het bedrijfsnetwerk.

Updates configureren vanuit de gedeelde folder via de Beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de beheerconsole **Tasks**.
3. Klik op de taak **Update van databases en programmamodules** van Kaspersky Endpoint Security.

   U ziet nu het venster met de taakeigenschappen.

   De taak *Update van databases en programmamodules* wordt automatisch gemaakt door de snelstart-wizard van de Administration Server. Voor het maken van de taak *Update van databases en programmamodules* installeert u de beheerplug-in van Kaspersky Endpoint Security voor Windows wanneer u de stappen van de wizard volgt.
4. Selecteer het gedeelte **Settings** in het venster met taakeigenschappen.



Instellingen van Update van databases en programmamodules-taak

5. In het blok **Instellingen voor lokale modus updaten**, klikt u op de knop **Instellingen**.
6. Klik in de lijst met updatebronnen op de knop **Toevoegen**.
7. Voer in het venster dat verschijnt het UNC-pad naar de gedeelde map in (bijvoorbeeld `\\<server name>\KLSHARE\Updates`).

   Het bronadres moet overeenkomen met het adres in de instellingen van Kaspersky Update Utility.
8. Klik op **OK**.

9. Configureer de prioriteiten van updatebronnen met de knoppen **Omhoog** en **Omlaag**.

   Als een update niet kan worden uitgevoerd vanaf de eerste updatebron, schakelt Kaspersky Endpoint Security automatisch over naar de volgende bron.

10. Sla uw wijzigingen op.

Updates configureren vanuit de gedeelde map via de Webconsole en Cloudconsole

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

   De lijst met taken wordt geopend.

2. Klik op de taak **Update** van Kaspersky Endpoint Security.

   U ziet nu het venster met de taakeigenschappen.

   De taak *Update* wordt automatisch gemaakt door de snelstart-wizard van de Administration Server. Voor het maken van de taak *Update* installeert u de beheerplug-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. Voer in het venster dat verschijnt het UNC-pad naar de gedeelde map in (bijvoorbeeld `\\<server name>\KLSHARE\Updates`).

   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**.

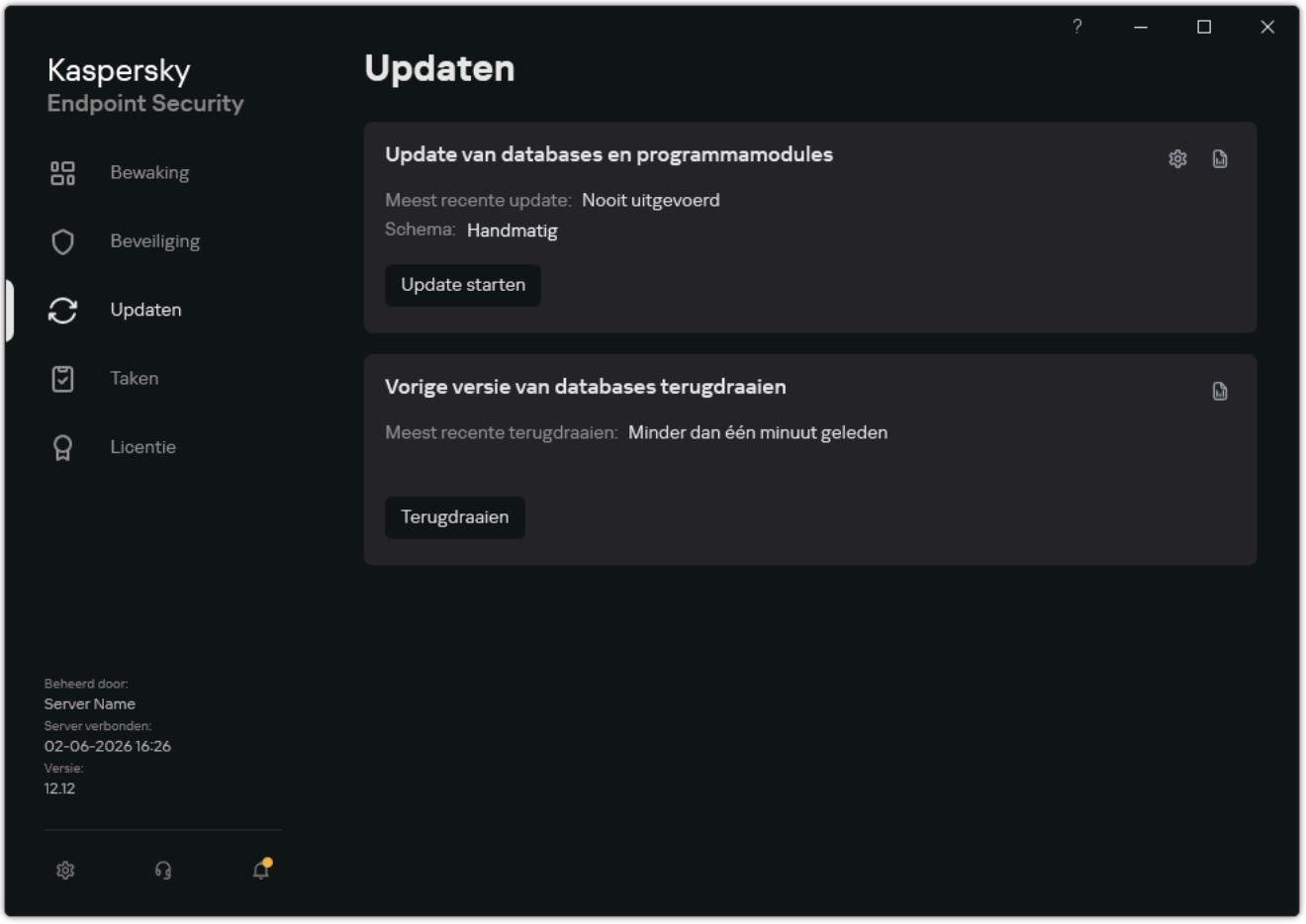
   Als een update niet kan worden uitgevoerd vanaf de eerste updatebron, schakelt Kaspersky Endpoint Security automatisch over naar de volgende bron.

8. Sla uw wijzigingen op.

Updates configureren vanuit de gedeelde map in de programma-interface

U kunt de groepstaak *Update van databases en programmamodules* niet configureren in de interface van het programma. Er is alleen een lokale updatetaak *Update van databases en programmamodules* beschikbaar voor de gebruiker. Als u de taak *Update van databases en programmamodules* niet ziet, heeft de beheerder het gebruik van lokale taken verboden in het beleid.

1. Ga in het hoofdvenster van het programma naar het gedeelte **Updaten**.



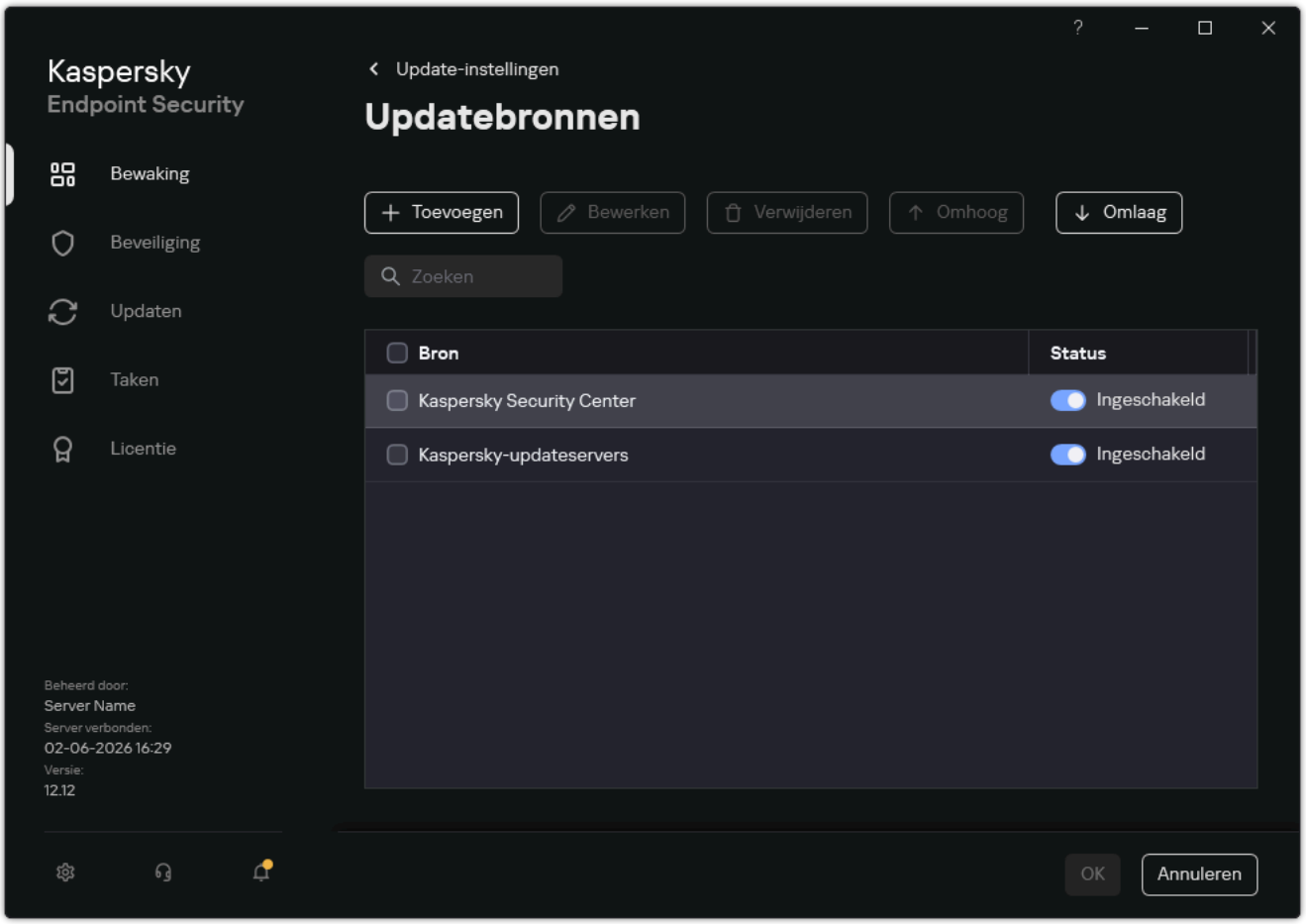
Lokale updatetaken

2. U ziet nu de lijst met taken: selecteer de taak *Update van databases en programmamodules* en klik op ⚙.

   U ziet nu het venster met de taakeigenschappen.

3. Klik in het venster taakeigenschappen op **Updatebronnen selecteren**.

4. Klik in de lijst met updatebronnen op de knop **Toevoegen**.



Updatebronnen

5. Voer het UNC-pad naar de gedeelde map in (bijvoorbeeld `\\<server name>\KLSHARE\Updates`).

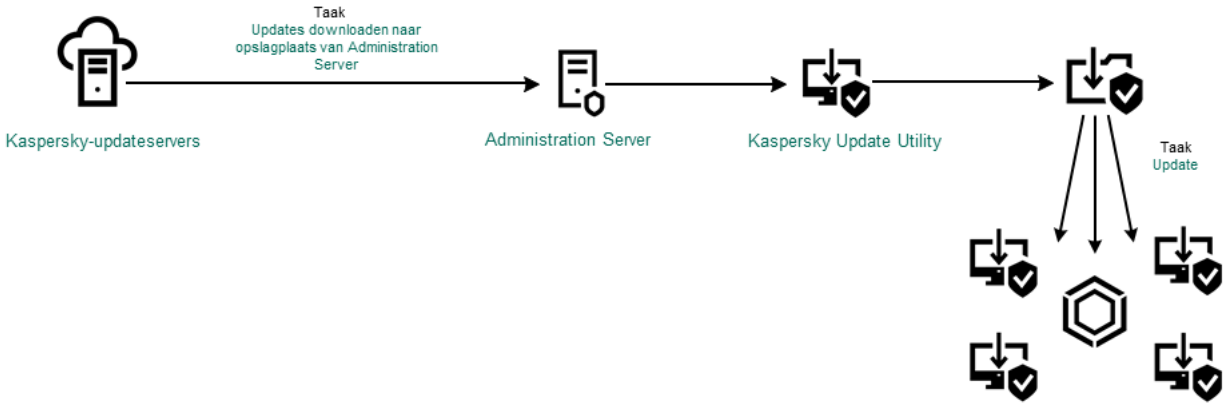
   Het bronadres moet overeenkomen met het adres in de instellingen van Kaspersky Update Utility.

6. Klik op **Selecteren**.

7. Configureer de prioriteiten van updatebronnen met de knoppen **Omhoog** en **Omlaag**.

   Als een update niet kan worden uitgevoerd vanaf de eerste updatebron, schakelt Kaspersky Endpoint Security automatisch over naar de volgende bron.

8. Sla uw wijzigingen op.



Updaten met Kaspersky Update Utility

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.

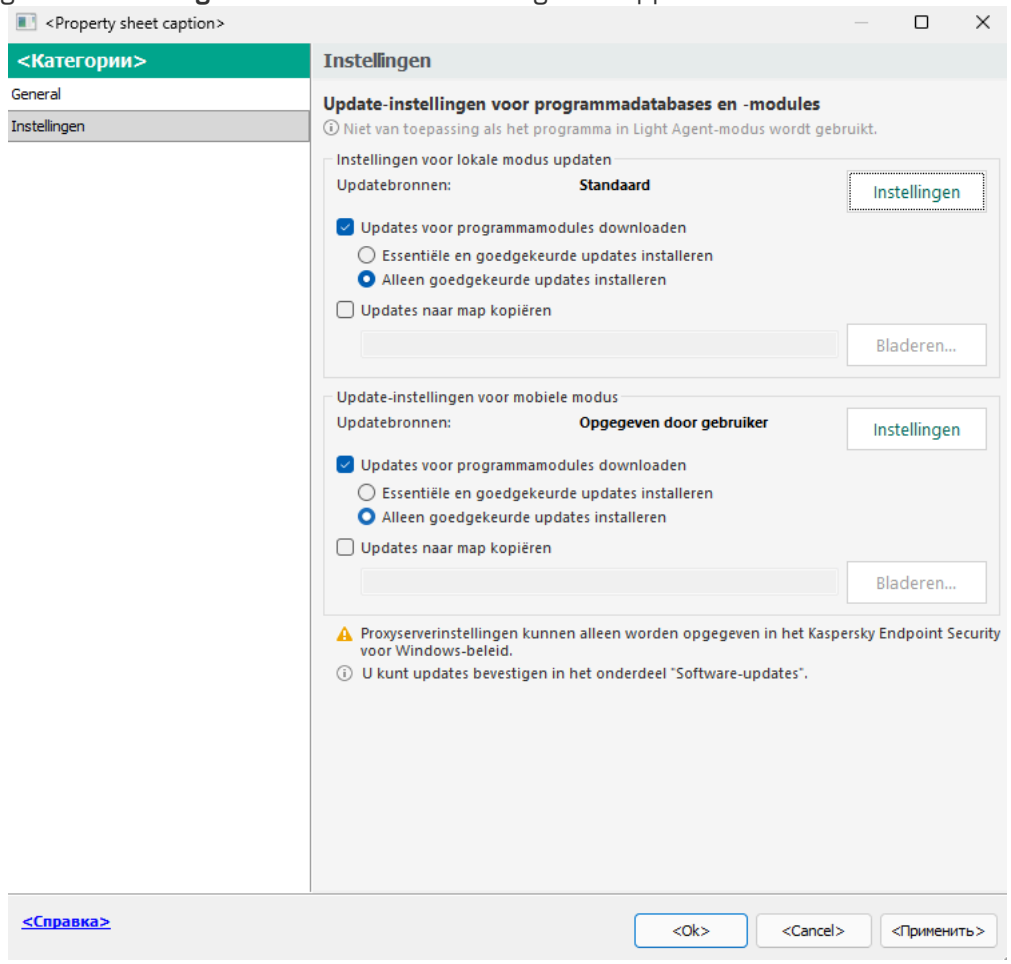
De update-instellingen voor mobiele modus configureren in de Beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de beheerconsole **Tasks**.
3. Klik op de taak **Update van databases en programmamodules** van Kaspersky Endpoint Security.

   U ziet nu het venster met de taakeigenschappen.

   De taak *Update van databases en programmamodules* wordt automatisch gemaakt door de snelstart-wizard van de Administration Server. Voor het maken van de taak *Update van databases en programmamodules* installeert u de beheerplug-in van Kaspersky Endpoint Security voor Windows wanneer u de stappen van de wizard volgt.

4. Selecteer het gedeelte **Settings** in het venster met taakeigenschappen.



Instellingen van Update van databases en programmamodules-taak

5. In het blok **Update-instellingen voor mobiele modus**, klikt u op de knop **Instellingen**.

6. Configureer de updatebronnen. De updatebronnen kunnen Kaspersky-updateservers, andere FTP- en HTTP-servers, lokale mappen of netwerkmappen zijn.

7. Sla uw wijzigingen op.

De update-instellingen voor mobiele modus configureren in Web Console en Cloud Console

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

   De lijst met taken wordt geopend.

2. Klik op de taak **Update** van Kaspersky Endpoint Security.

   U ziet nu het venster met de taakeigenschappen.

   De taak *Update* wordt automatisch gemaakt door de snelstart-wizard van de Administration Server. Voor het maken van de taak *Update* installeert u de beheerplug-in van Kaspersky Endpoint Security voor Windows wanneer u de stappen van de wizard volgt.

3. Selecteer het tabblad **Application settings** → **Mobile mode**.

4. Configureer de updatebronnen. De updatebronnen kunnen Kaspersky-updateservers, andere FTP- en HTTP-servers, lokale mappen of netwerkmappen zijn.

5. 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

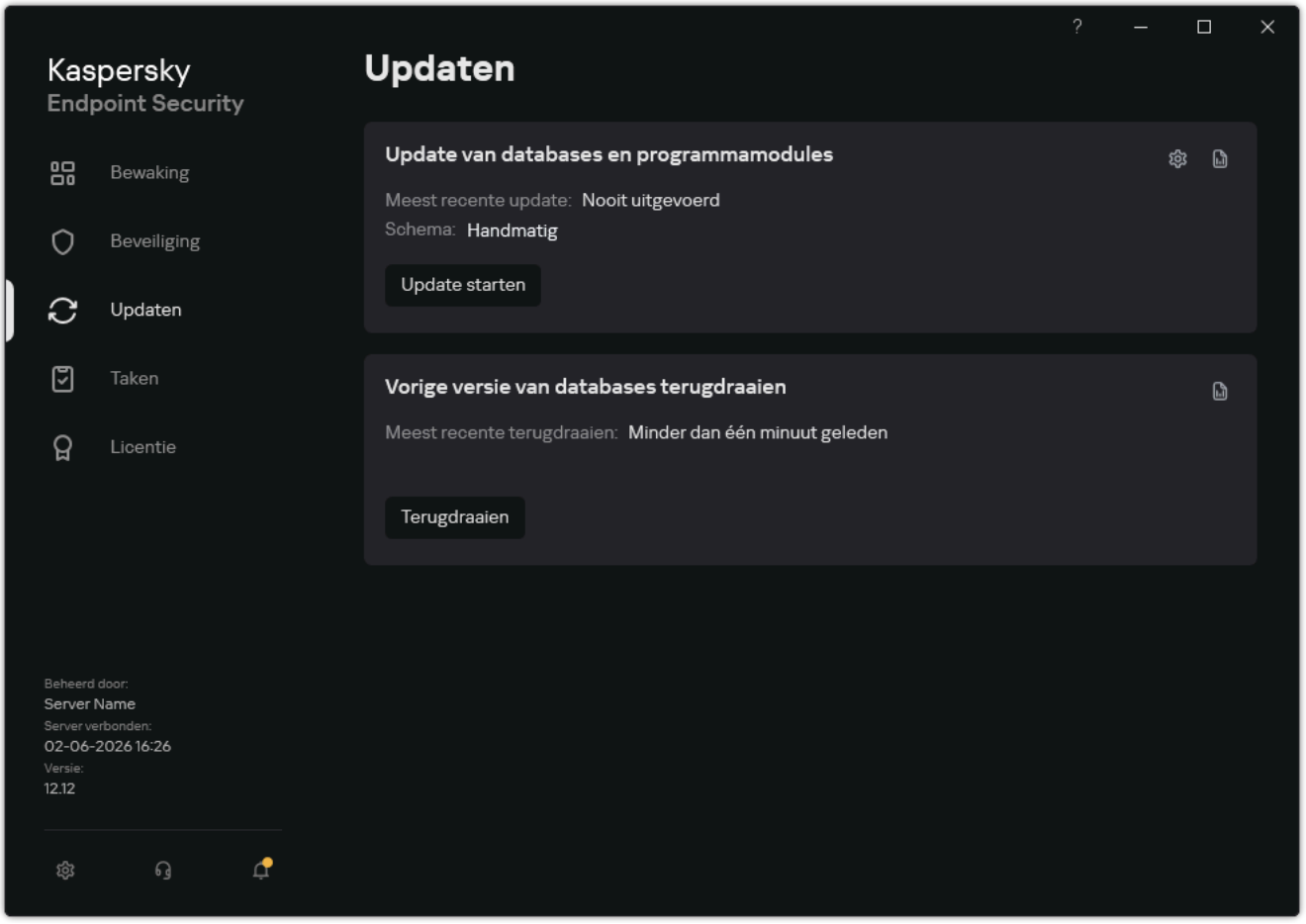
Een updatetaak met de rechten van een ander gebruikersaccount starten

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 programma-instellingen 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:

U kunt de groepstaak *Update van databases en programmamodules* niet configureren in de interface van het programma. Er is alleen een lokale updatetaak *Update van databases en programmamodules* beschikbaar voor de gebruiker. Als u de taak *Update van databases en programmamodules* niet ziet, heeft de beheerder het gebruik van lokale taken verboden in het beleid.

1. Ga in het hoofdvenster van het programma naar het gedeelte **Updaten**.



Lokale updatetaken

2. U ziet nu de lijst met taken: selecteer de taak *Update van databases en programmamodules* en klik op ⚙.

   U ziet nu het venster met de taakeigenschappen.

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

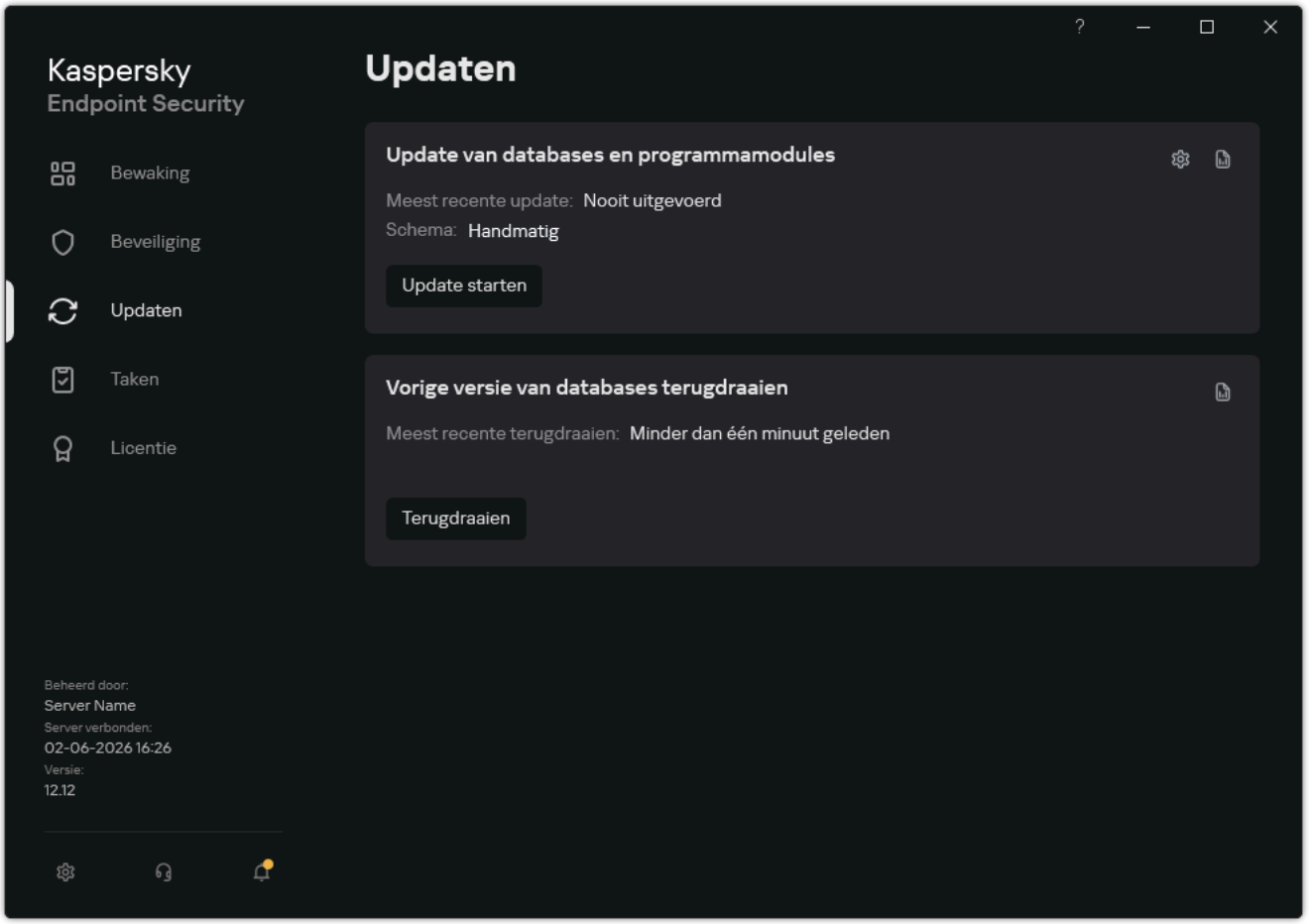
Als de updatetaak om een willekeurige reden niet kan worden uitgevoerd (de computer is bijvoorbeeld uitgeschakeld op dat moment), kunt u instellen dat de overgeslagen taak automatisch moet worden gestart zodra dit mogelijk is.

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:

U kunt de groepstaak *Update van databases en programmamodules* niet configureren in de interface van het programma. Er is alleen een lokale updatetaak *Update van databases en programmamodules* beschikbaar voor de gebruiker. Als u de taak *Update van databases en programmamodules* niet ziet, heeft de beheerder het gebruik van lokale taken verboden in het beleid.

1. Ga in het hoofdvenster van het programma naar het gedeelte **Updaten**.



Lokale updatetaken

2. U ziet nu de lijst met taken: selecteer de taak *Update van databases en programmamodules* en klik op ⚙.

   U ziet nu het venster met de taakeigenschappen.

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 **Start na programmastart uitstellen 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. Als het programma een kans krijgt om gemiste taken uit te voeren, start het de taken willekeurig binnen een bepaalde tijdsinterval om de lading voor de computer te spreiden.

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.

Als de Kaspersky updateservers niet beschikbaar zijn, kan Kaspersky Endpoint Security alternatieve domeinen gebruiken om de databases en softwaremodules van het programma bij te werken. Raadpleeg de Knowledge Base van de Technische Support voor gedetailleerde informatie.

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.

Kaspersky Endpoint Security gebruikt standaard de Kaspersky Security Center-server als eerste updatebron. Dit helpt verkeer te besparen tijdens het updaten. Als een beleid niet op de computer wordt toegepast, worden Kaspersky-servers geselecteerd als de eerste updatebron in de instellingen van de lokale taak *Update van databases en programmamodules* omdat het programma mogelijk geen toegang heeft tot de Kaspersky Security Center-server.

Als het programma in Light Agent-modus draait, wordt een map op de SVM geselecteerd als updatebron.

Een updatebron toevoegen in de Beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.

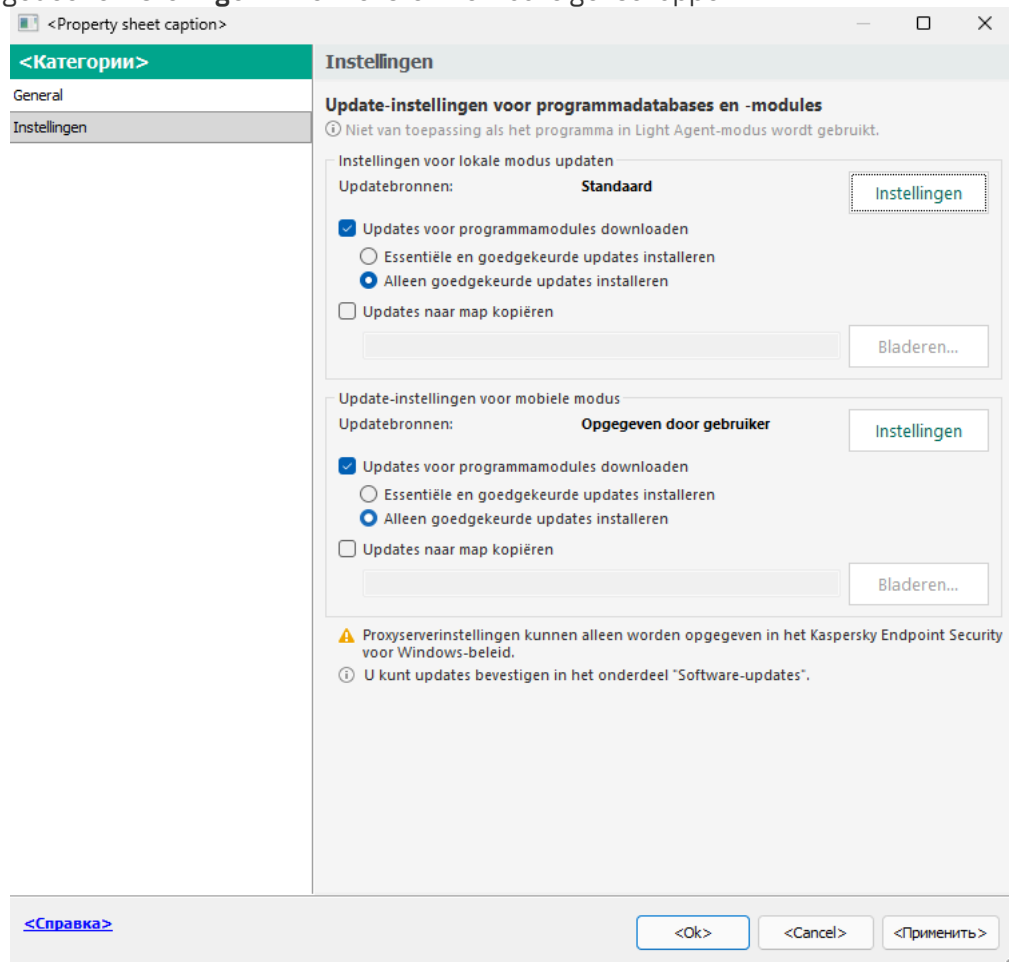
   Selecteer in de beheerconsole **Tasks**.

2. Klik op de taak **Update van databases en programmamodules** van Kaspersky Endpoint Security.

   U ziet nu het venster met de taakeigenschappen.

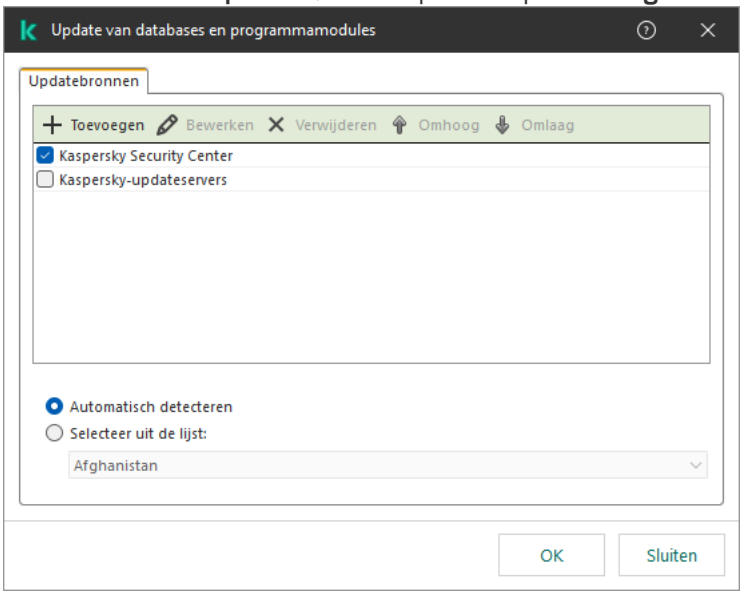
   De taak *Update van databases en programmamodules* wordt automatisch gemaakt door de snelstart-wizard van de Administration Server. Voor het maken van de taak *Update van databases en programmamodules* installeert u de beheerplug-in van Kaspersky Endpoint Security voor Windows wanneer u de stappen van de wizard volgt.

3. Selecteer het gedeelte **Instellingen** in het venster met taakeigenschappen.



Instellingen van Update van databases en programmamodules-taak

4. In het blok **Instellingen voor lokale modus updaten**, klikt u op de knop **Instellingen**.



Updatebronnen

5. Klik in de lijst met updatebronnen op de knop **Toevoegen**.

6. Geef in het veld **Updatebronnen** 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://dnl-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://<user name>:<password>@<node>:<port>`.

   - 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\AVP12\Update distribution\`.

   U kunt de updatebron uitsluiten zonder deze uit de lijst met updatebronnen te verwijderen. Schakel hiervoor het selectievakje naast het object uit.

7. Klik op **OK**.

8. Configureer de prioriteiten van updatebronnen met de knoppen **Omhoog** en **Omlaag**.

   Als een update niet kan worden uitgevoerd vanaf de eerste updatebron, schakelt Kaspersky Endpoint Security automatisch over naar de volgende bron.

9. Voeg indien nodig een updatebron toe voor 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*).

10. Sla uw wijzigingen op.

Een bijgewerkte bron toevoegen in de Webconsole en de Cloudconsole

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

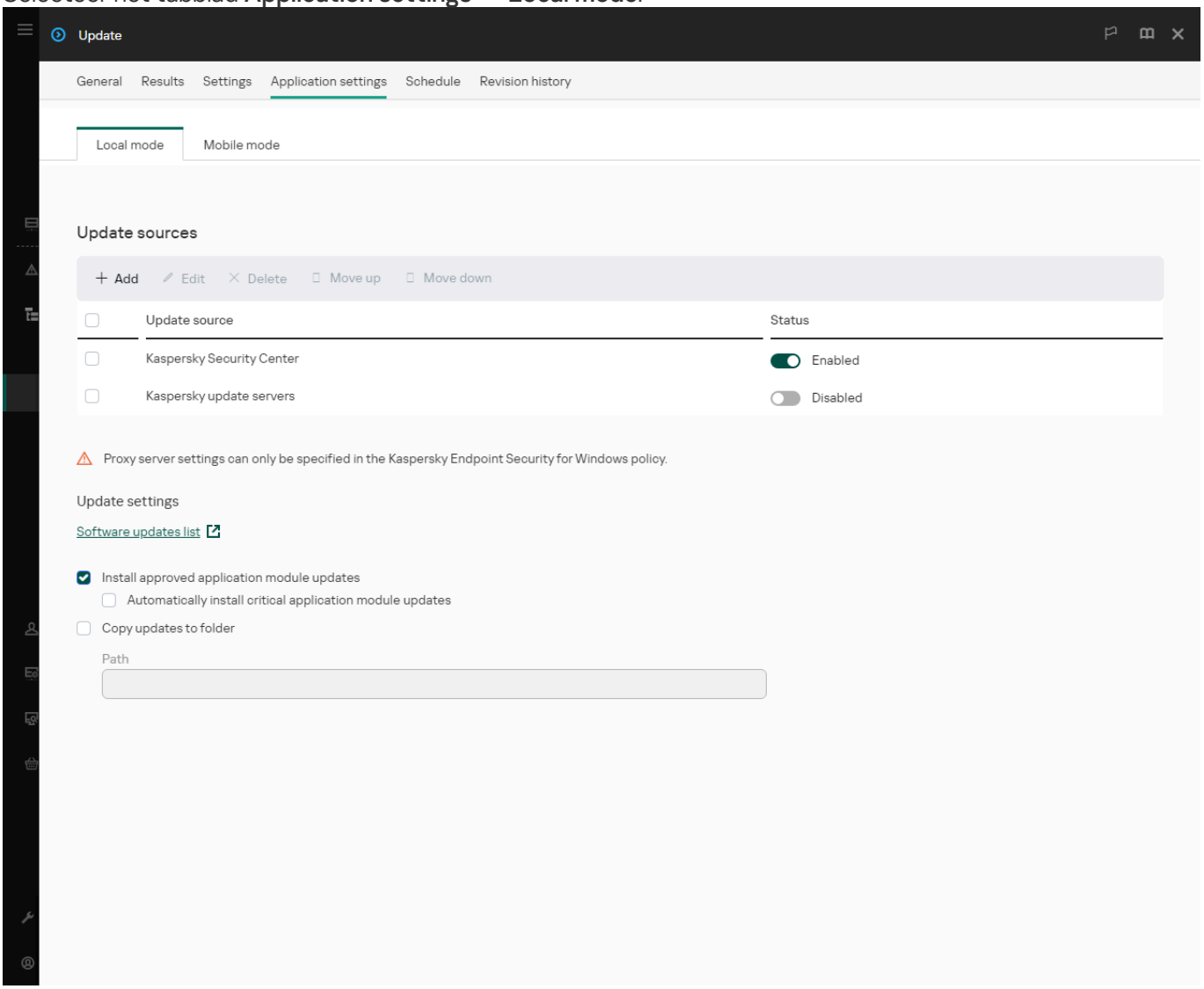
   De lijst met taken wordt geopend.

2. Klik op de taak **Update** van Kaspersky Endpoint Security.

   U ziet nu het venster met de taakeigenschappen.

   De taak *Update* wordt automatisch gemaakt door de snelstart-wizard van de Administration Server. Voor het maken van de taak *Update* installeert u de beheerplug-in van Kaspersky Endpoint Security voor Windows wanneer u de stappen van de wizard volgt.

3. Selecteer het tabblad **Application settings** → **Local mode**.



Updatebronnen

4. Klik in de lijst met updatebronnen op de knop **Add**.

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://dnl-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://<user name>:<password>@<node>:<port>`.

- 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\AVP12\Update distribution\`.

U kunt de updatebron uitsluiten zonder deze uit de lijst met updatebronnen te verwijderen. Dat doet u door de schakelaar ernaast uit te zetten.

6. Klik op **OK**.

7. Configureer de prioriteiten van updatebronnen met de knoppen **Up** en **Down**.

   Als een update niet kan worden uitgevoerd vanaf de eerste updatebron, schakelt Kaspersky Endpoint Security automatisch over naar de volgende bron.

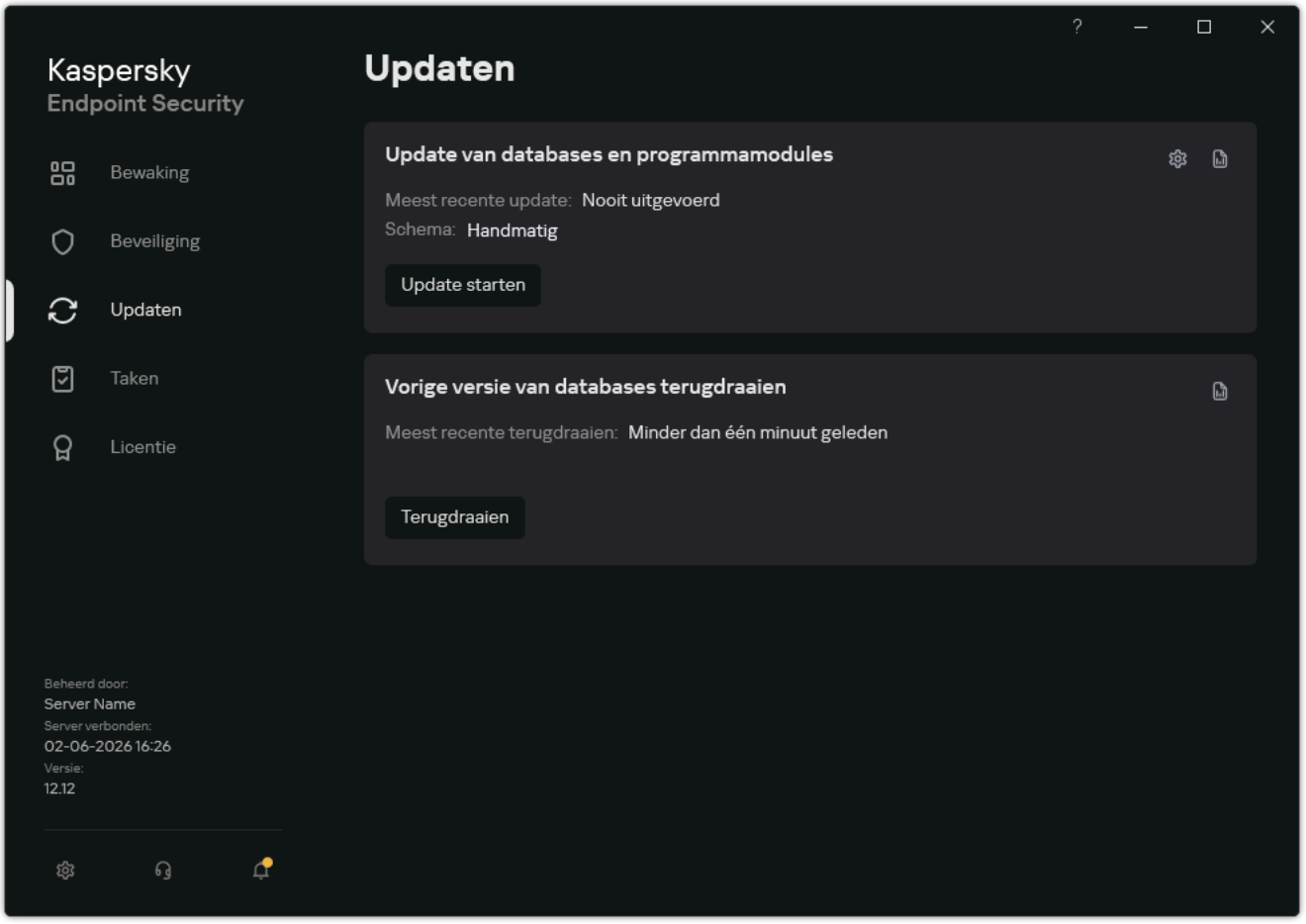
8. Voeg indien nodig een updatebron toe voor mobiele modus. De *mobiele modus* is de modus waarin Kaspersky Endpoint Security werkt wanneer een computer niet langer verbonden is met het bedrijfsnetwerk (*offline computer*).

9. Sla uw wijzigingen op.

Voeg een updatebron toe in het programma-interface

U kunt de groepstaak *Update van databases en programmamodules* niet configureren in de interface van het programma. Er is alleen een lokale updatetaak *Update van databases en programmamodules* beschikbaar voor de gebruiker. Als u de taak *Update van databases en programmamodules* niet ziet, heeft de beheerder het gebruik van lokale taken verboden in het beleid.

1. Ga in het hoofdvenster van het programma naar het gedeelte **Updaten**.



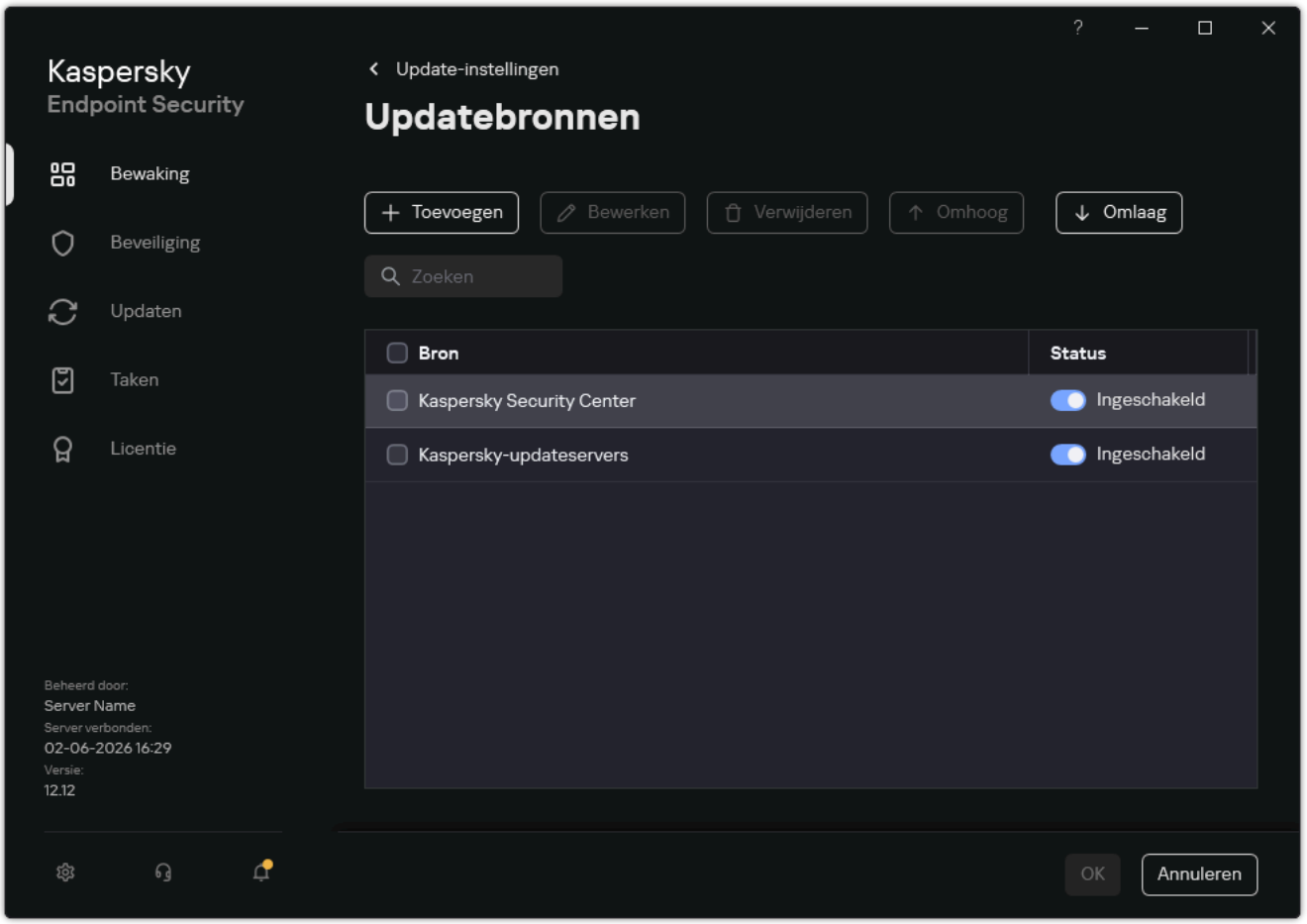
Lokale updatetaken

2. U ziet nu de lijst met taken: selecteer de taak *Update van databases en programmamodules* en klik op ⚙.

   U ziet nu het venster met de taakeigenschappen.

3. Klik op **Updatebronnen selecteren**.

4. Klik in het venster op de knop **Toevoegen**.



Updatebronnen

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://dnl-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://<user name>:<password>@<node>:<port>`.

   - 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\AVP12\Update distribution\`.

6. Klik op **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.

Na het installeren van een programma-update, moet u mogelijk uw computer opnieuw opstarten.

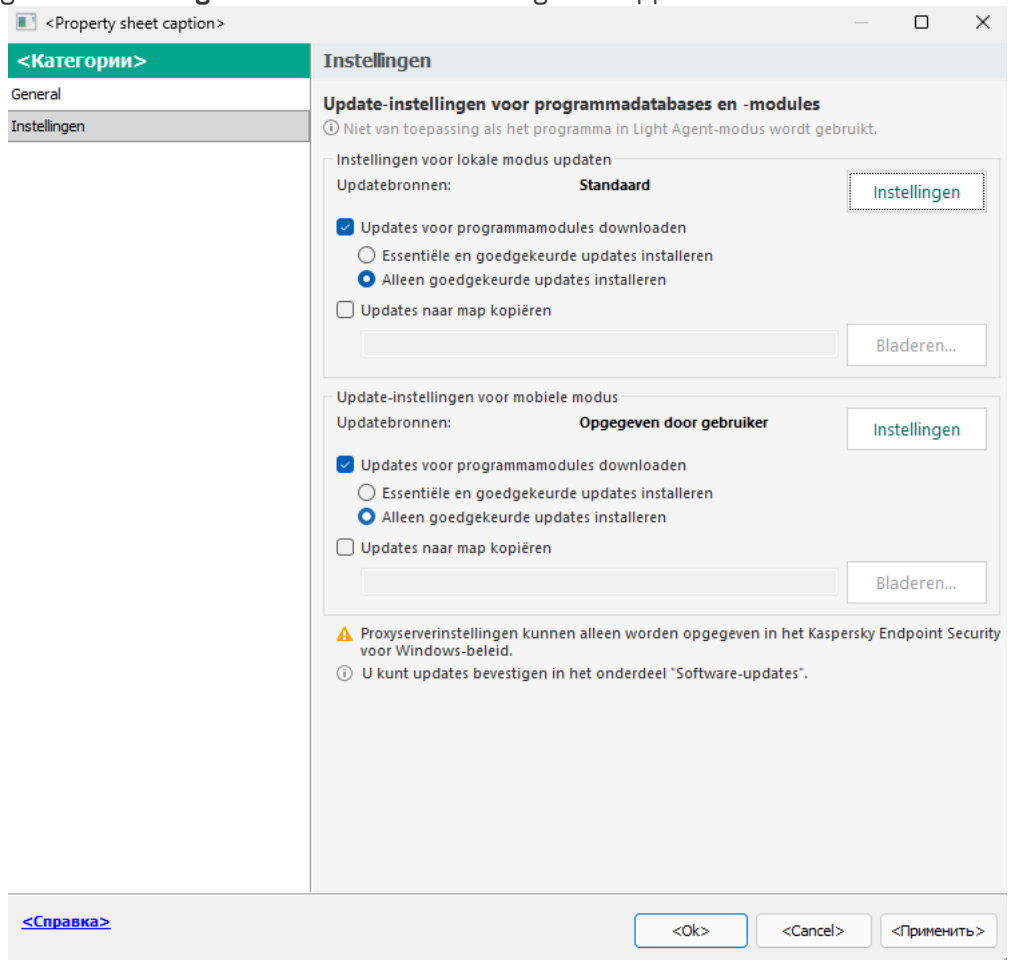
Updates van programmamodules configureren in de Beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de beheerconsole **Tasks**.
3. Klik op de taak **Update van databases en programmamodules** van Kaspersky Endpoint Security.

   U ziet nu het venster met de taakeigenschappen.

   De taak *Update van databases en programmamodules* wordt automatisch gemaakt door de snelstart-wizard van de Administration Server. Voor het maken van de taak *Update van databases en programmamodules* installeert u de beheerplug-in van Kaspersky Endpoint Security voor Windows wanneer u de stappen van de wizard volgt.

4. Selecteer het gedeelte **Settings** in het venster met taakeigenschappen.



Instellingen van Update van databases en programmamodules-taak

5. Schakel in het blok **Instellingen voor lokale modus updaten** het selectievakje **Updates voor programmamodules downloaden** in.

   Als u wilt voorkomen dat updates van programmamodules worden gedownload, schakel het selectievakje **Updates voor programmamodules downloaden** uit en verbiedt het gebruik van lokale taken door de gebruiker.

6. 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.

7. Indien nodig, configureer updates van programmamodule voor 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*).

8. Sla uw wijzigingen op.

Updates van programmamodules configureren in de Webconsole en Cloudconsole

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

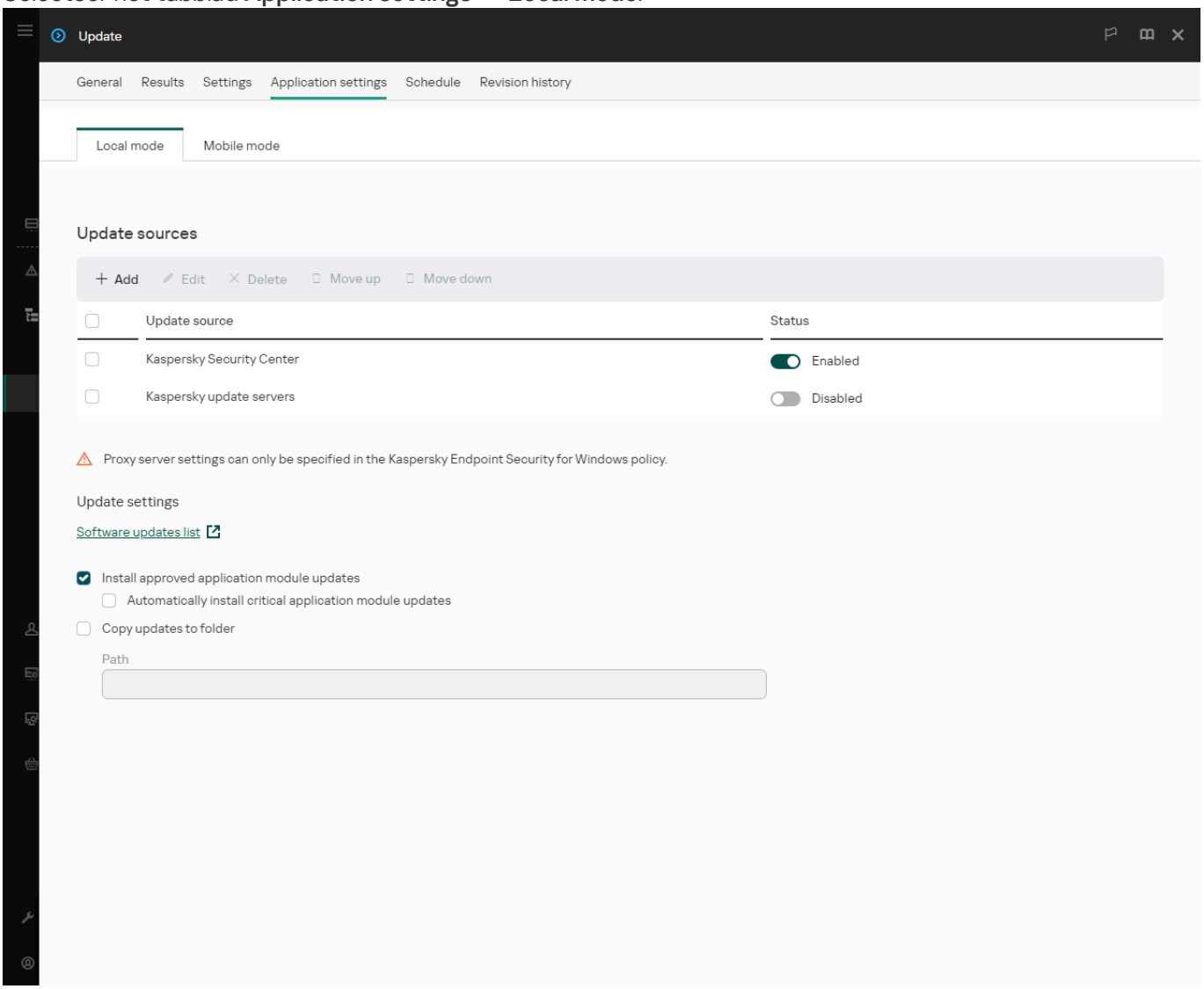
   De lijst met taken wordt geopend.

2. Klik op de taak **Update van databases en programmamodules** van Kaspersky Endpoint Security.

   U ziet nu het venster met de taakeigenschappen.

   De taak *Update van databases en programmamodules* wordt automatisch gemaakt door de snelstart-wizard van de Administration Server. Voor het maken van de taak *Update van databases en programmamodules* installeert u de beheerplug-in van Kaspersky Endpoint Security voor Windows wanneer u de stappen van de wizard volgt.

3. Selecteer het tabblad **Application settings** → **Local mode**.



Instellingen van Update-taak

4. Selecteer onder **Update settings**, de updates van de programmamodule die u wilt installeren:

   - **Install approved application module updates**. 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.

   - **Automatically install critical application module updates**. 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.

   Als u wilt voorkomen dat updates van programmamodules worden gedownload, schakel de selectievakjes **Install approved application module updates** en **Automatically install critical application module updates** uit en verbiedt het gebruik van lokale taken door de gebruiker.

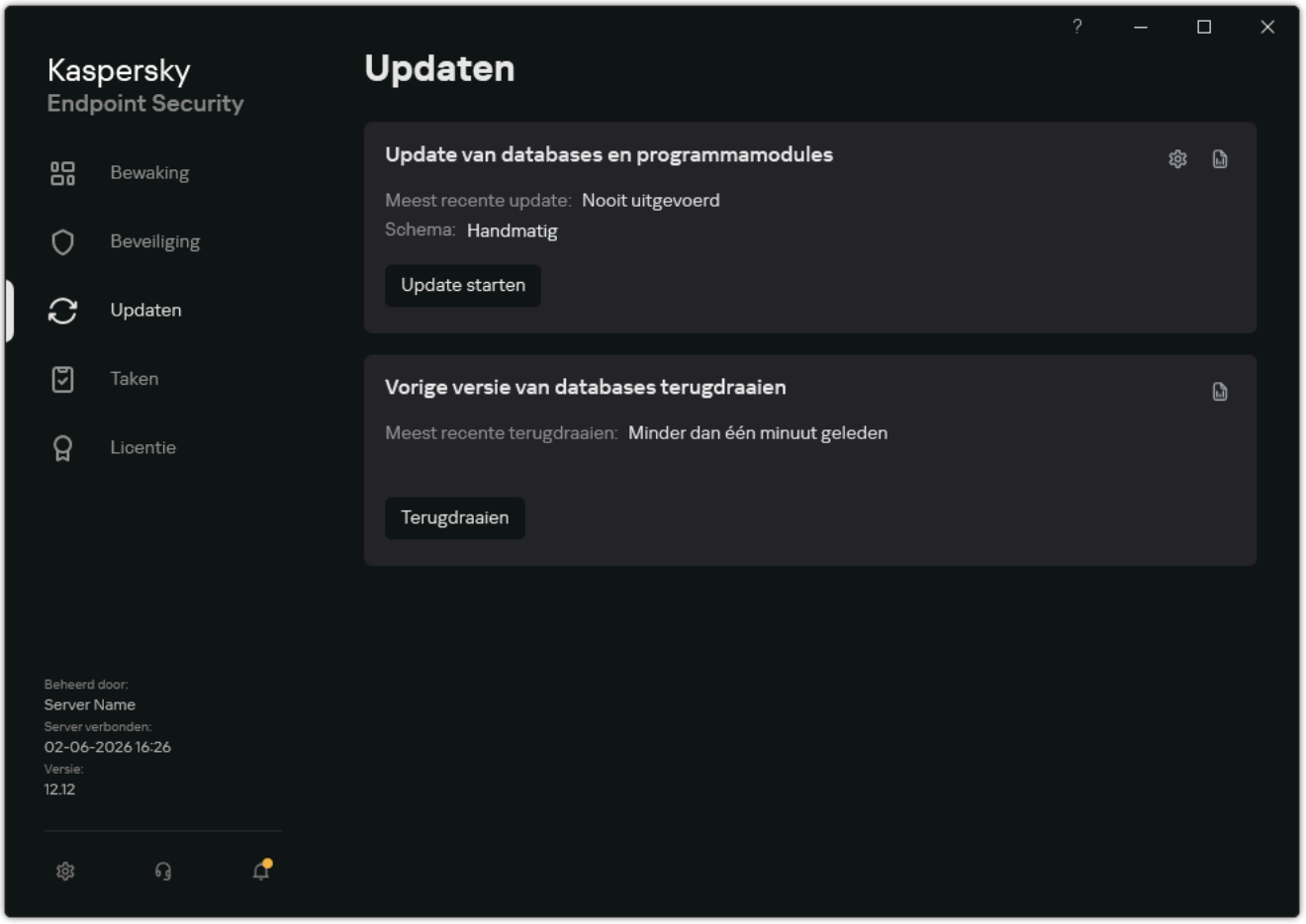
5. Indien nodig, configureer updates van programmamodule voor mobiele modus. De *mobiele modus* is de modus waarin Kaspersky Endpoint Security werkt wanneer een computer niet langer verbonden is met het bedrijfsnetwerk (*offline computer*).

6. Sla uw wijzigingen op.

Updates van programmamodules configureren in het programma-interface

U kunt de groepstaak *Update van databases en programmamodules* niet configureren in de interface van het programma. Er is alleen een lokale updatetaak *Update van databases en programmamodules* beschikbaar voor de gebruiker. Als u de taak *Update van databases en programmamodules* niet ziet, heeft de beheerder het gebruik van lokale taken verboden in het beleid.

1. Ga in het hoofdvenster van het programma naar het gedeelte **Updaten**.



Lokale updatetaken

2. U ziet nu de lijst met taken: selecteer de taak *Update van databases en programmamodules* en klik op ⚙.

   U ziet nu het venster met de taakeigenschappen.

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. Selecteer het selectievakje **Use proxy server**.

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 in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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** → **Network Settings**.

5. In het blok **Proxy server**, klikt u op de knop **Settings**.

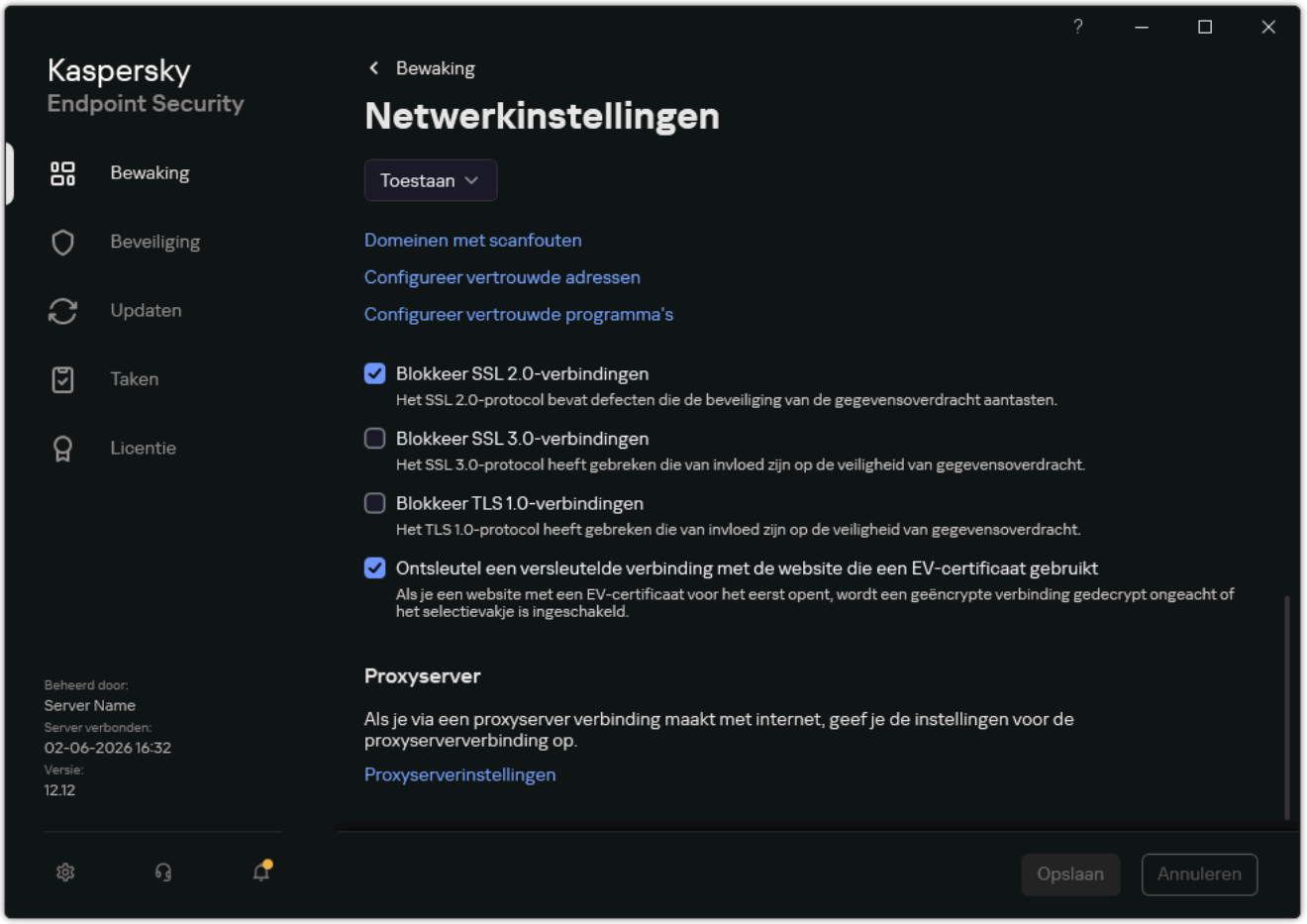
6. Selecteer in het venster dat opent het selectievakje **Bypass a proxy server for local addresses**.

7. Sla uw wijzigingen op.

De instellingen van de proxyserver configureren in de programma-interface:

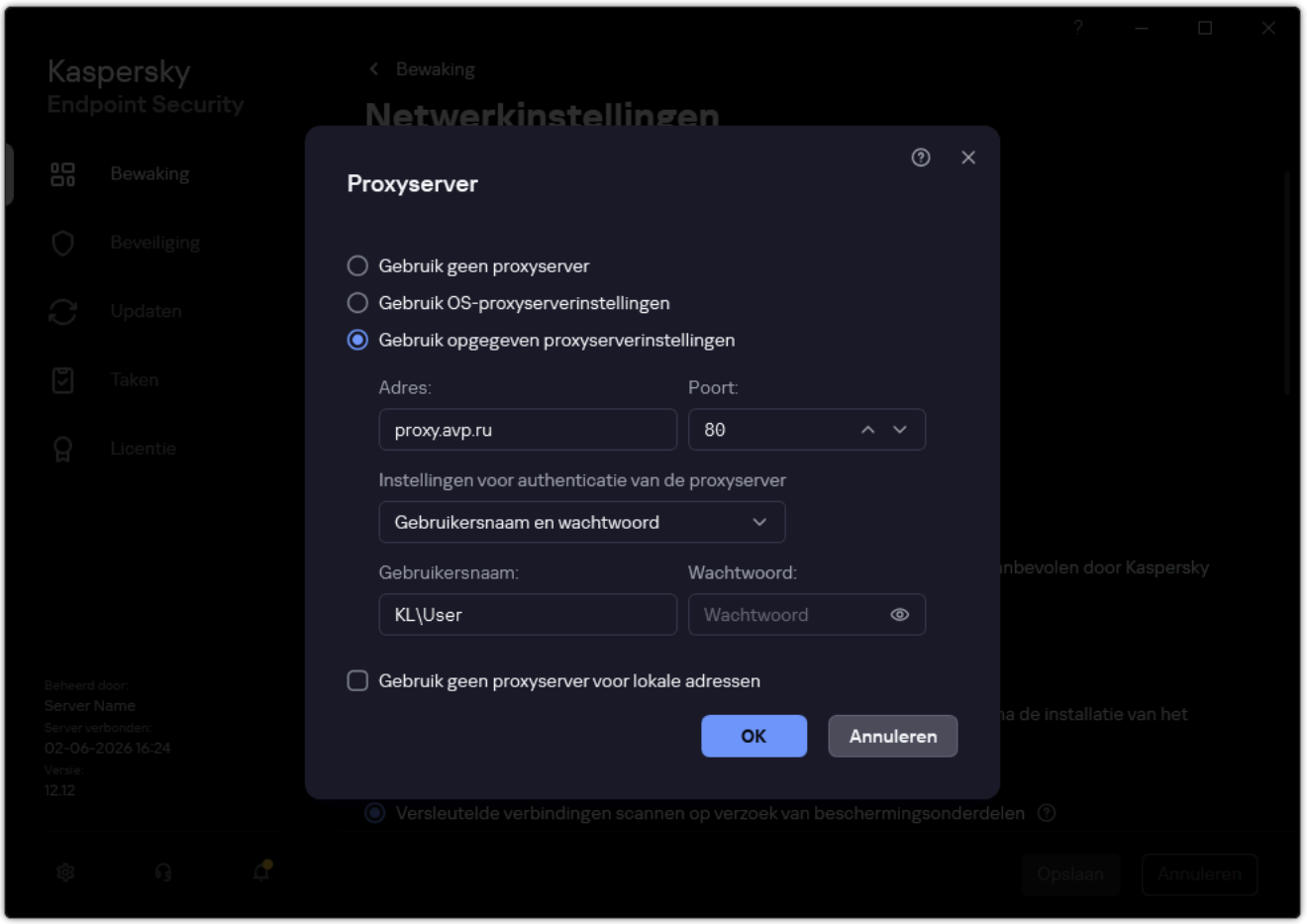
1. Klik in het hoofdvenster van het programma op de knop ⚙.

2. Selecteer **Algemene instellingen** → **Netwerkinstellingen** in het venster met de programma-instellingen.



Netwerkinstellingen programma

3. Klik in het blok **Proxyserver** op de koppeling **Proxyserverinstellingen**.



Instellingen proxyserververbinding

4. Selecteer in het venster dat opent één van de volgende opties voor het bepalen van het proxyserveradres:

   - **Gebruik OS-proxyserverinstellingen**.

     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. Selecteer hoe het programma zich moet verifiëren op de proxyserver. Standaard gebruikt het programma domein NTLM-authenticatie van de huidige gebruiker.

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 laatste update is bijvoorbeeld handig als een nieuwe databaseversie een vals positief resultaat oplevert waardoor Kaspersky Endpoint Security een veilig programma blokkeert.

Kaspersky Endpoint Security in de Light Agent-modus ondersteunt de taak *Update terugdraaien* niet.

De laatste update in de Beheerconsole (MMC) terugdraaien

1. Selecteer **Tasks** in de structuur van de Beheerconsole van Kaspersky Security Center.

   De lijst met taken wordt geopend.

2. Klik op **New task**.

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

Stap 1. Een taaktype selecteren

1. Selecteer **Kaspersky Endpoint Security voor Windows 14.1.** → **Update terugdraaien**.

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 het taakschema bijvoorbeeld handmatig.

Stap 4. Taaknaam definiëren

Voer een naam voor de taak in.

Stap 7. Aanmaak van de taak voltooien

Verlaat de wizard verlaten. Schakel indien nodig het selectievakje **Run the task after the wizard finishes** in. U kunt de voortgang van de taak volgen in de taakeigenschappen.

De laatste update terugdraaien in de Webconsole

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

   De lijst met taken wordt geopend.

2. Klik op **Add**.

   De wizard Taak wordt gestart.

3. Configureer de taakinstellingen:

   a. Selecteer in de vervolgkeuzelijst **Application** de optie **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. Selecteer in de vervolgkeuzelijst **Task type** de optie **Update rollback**.

   c. Typ in het veld **Task name** een korte omschrijving, zoals *Update terugdraaien*.

   d. Selecteer in het gedeelte **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. Ga naar de volgende stap.

5. Selecteer een account om de taak uit te voeren. Kaspersky Endpoint Security start de taak standaard met de rechten van een lokaal gebruikersaccount.

6. Verlaat de wizard verlaten.

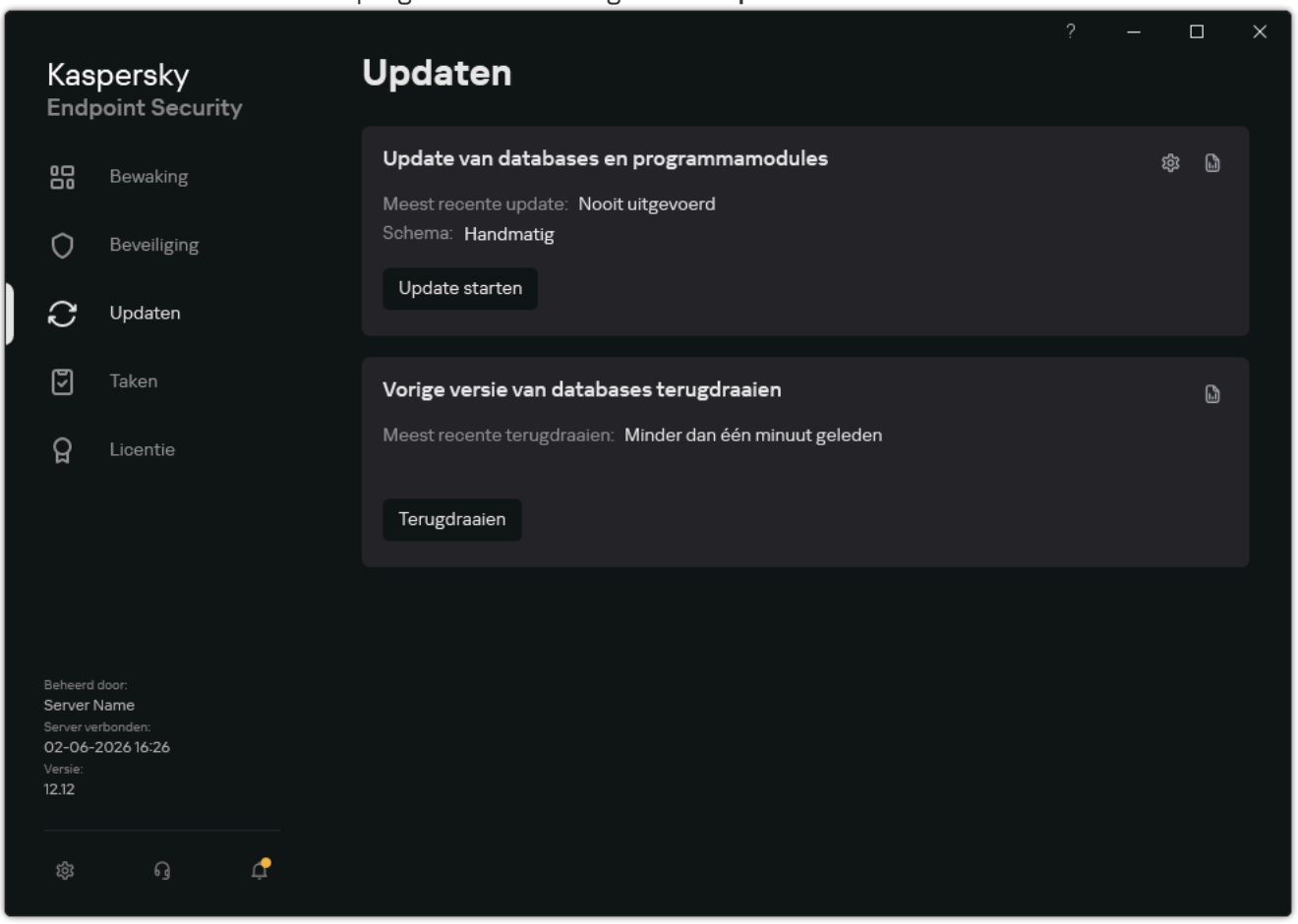
7. U ziet een nieuwe taak in de lijst met taken.

8. Schakel het selectievakje naast de taak in.

9. Klik op **Start**.

De laatste update in het programma-interface terugdraaien.

1. Ga in het hoofdvenster van het programma naar het gedeelte **Updaten**.



Lokale updatetaken

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 gedownloade bestanden en de updatebron. U kunt de taak op elk moment stoppen door op de knop **Update stoppen** te klikken.

Geavanceerde desinfectietechnologie

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 *Malware-scan*-taakinstellingen en in programma-instellingen.

Als Kaspersky Endpoint Security de malware niet kan tegenhouden, dan kunt u de geavanceerde desinfectietechnologie gebruiken. Voor computers onder het beleid is geavanceerde desinfectie standaard uitgeschakeld, omdat deze technologie een aanzienlijke hoeveelheid verwerkingsvermogen van de computer gebruikt. Voor computers die niet onder beleid staan, is Geavanceerde desinfectie standaard ingeschakeld.

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 *Malware-scan*. Deze voorwaarde is niet nodig om de technologie op werkstations te gebruiken.

Het onderdeel Geavanceerde desinfectietechnologie in- of uitschakelen in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Algemene instellingen** → **Programma-instellingen** in het beleidsvenster.
4. Selecteer of deselecteer in het blok **Algemeen** het selectievakje **Geavanceerde desinfectietechnologie inschakelen** in om de Geavanceerde desinfectietechnologie in of uit te schakelen.
5. Sla uw wijzigingen op.

Het onderdeel Geavanceerde desinfectietechnologie in- of uitschakelen in de Webconsole en Cloudconsole

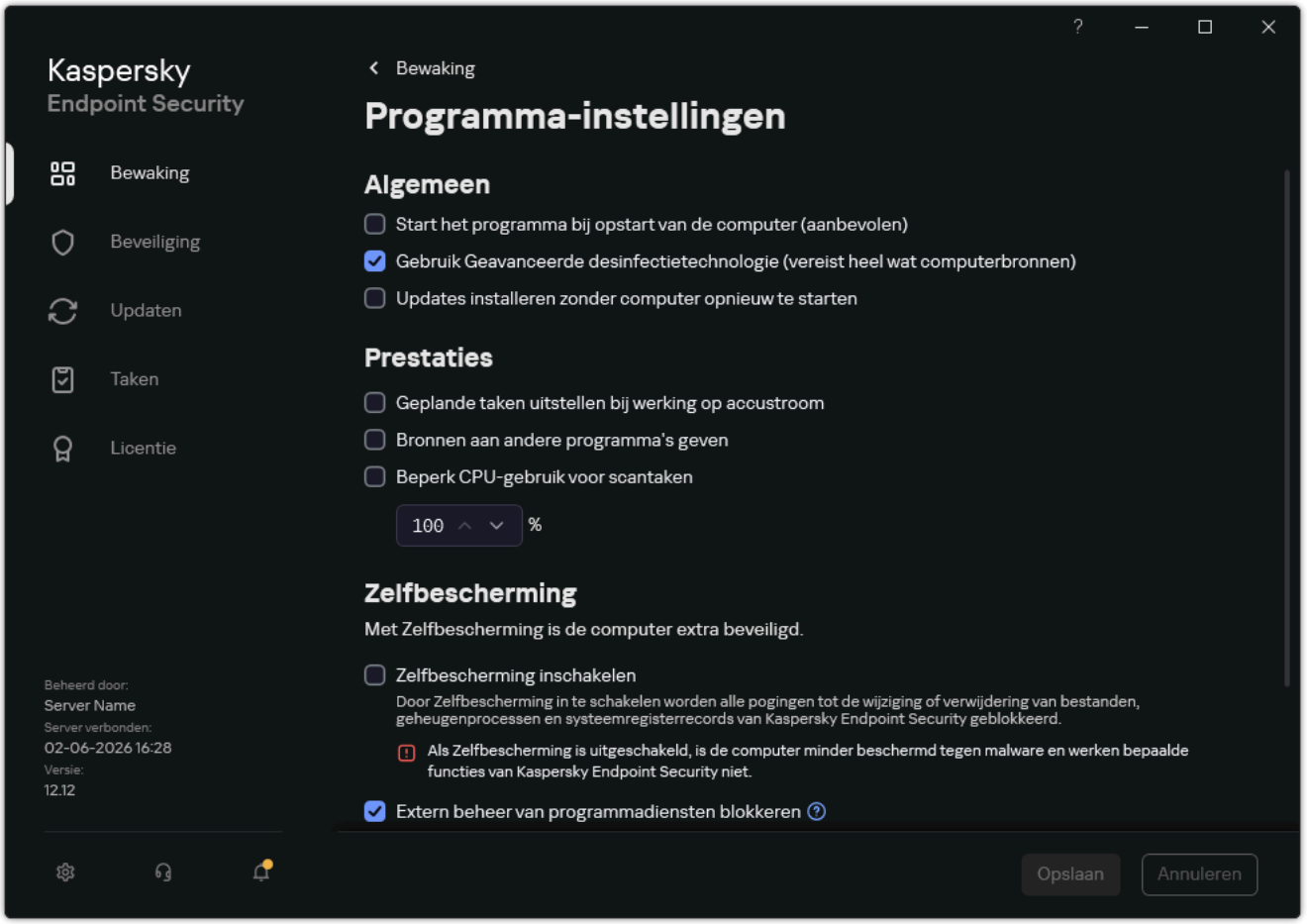
1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.

   U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Selecteer **General Settings** → **Detection Settings**.
5. In het blok **Advanced Disinfection Technology** kunt u de schakelaar **Advanced Disinfection Technology ENABLED** in- of uitschakelen.
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.



Instellingen Kaspersky Endpoint Security voor Windows

3. Selecteer of deselecteer in het blok **Algemeen** 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.

Desinfectie van actieve dreigingen op werkstations

Om te werken met actieve dreigingen op werkstations schakelt u de Geavanceerde desinfectietechnologie in de programma-instellingen. Configureer vervolgens de gebruikerservaring in de *Malware-scan*-taakeigenschappen. U ziet het selectievakje **Geavanceerde desinfectie direct uitvoeren** 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

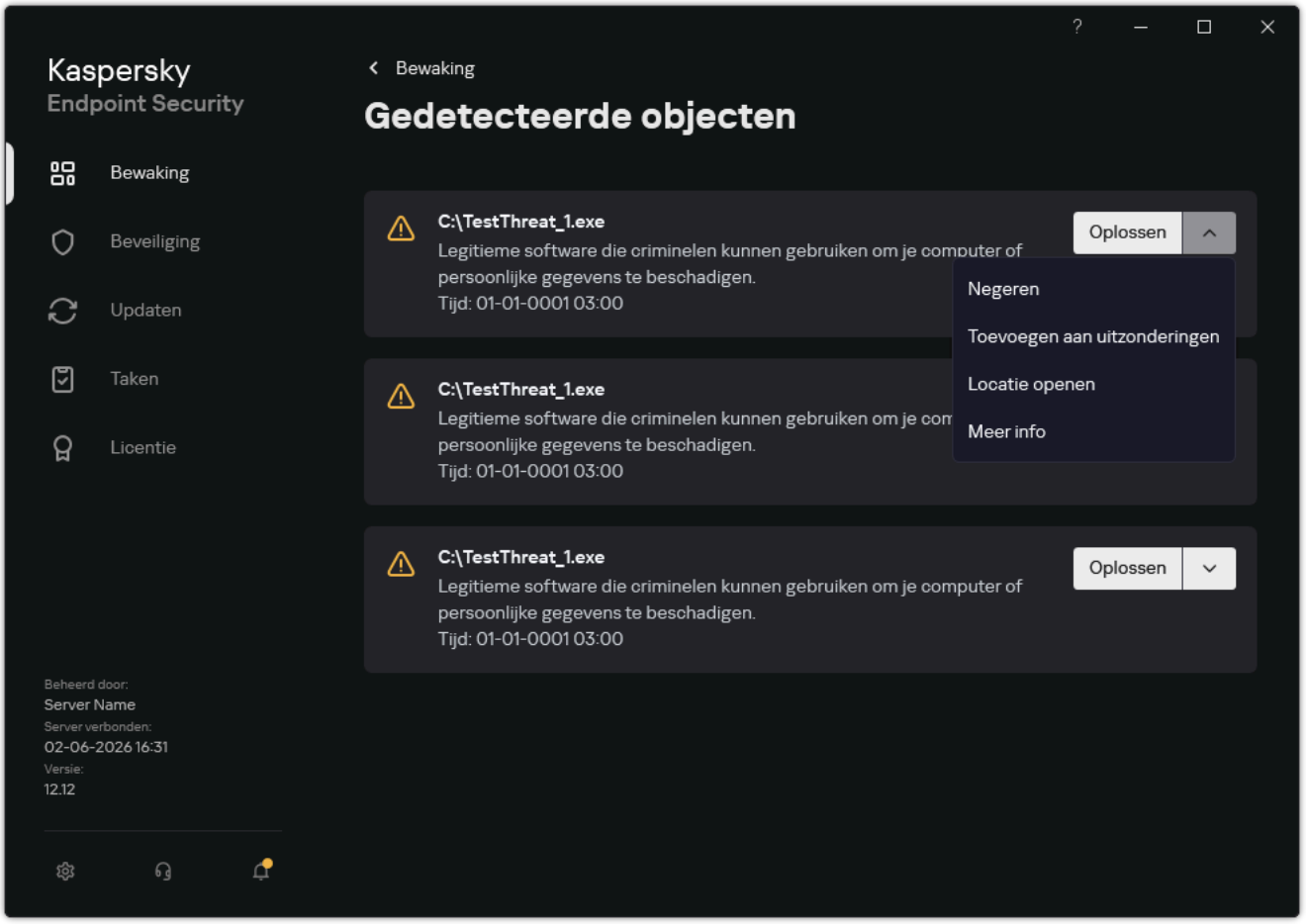
Om met actieve bedreigingen op servers te werken, moet u het volgende doen:

- De Geavanceerde desinfectietechnologie inschakelen in de programma-instellingen;
- Onmiddellijke geavanceerde desinfectie inschakelen in de taakeigenschappen van *Malware-scan*.

Als Kaspersky Endpoint Security is geïnstalleerd op een computer met Windows for Servers, toont Kaspersky Endpoint Security de melding niet. Daarom kan u 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 *Malware-scan*. Vervolgens moet u de *Malware-scan* starten.

Onverwerkte dreigingen elimineren

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).



Een lijst met actieve bedreigingen

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 *Malware-scan*-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 **Negeren**.

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: *Critical* – .

Een dreiging verwerken in de Beheerconsole (MMC)

1. Ga in de Beheerconsole naar de map **Administration Server** → **Advanced** → **Repositories** → **Active threats**.

   De lijst met actieve dreigingen wordt geopend.

2. Selecteer het object dat u wilt verwerken.

3. Kies hoe u de dreiging wilt aanpakken:

   - **Disinfect**. Als deze optie is geselecteerd, probeert het programma automatisch om ieder gevonden geïnfecteerd bestand te desinfecteren. Mocht de desinfectie mislukken, dan wordt het bestand door het programma verwijderd.

   - **Delete**. Als deze optie is geselecteerd, verwijdert het programma het geïnfecteerde bestand dat wordt gedetecteerd, uit de opslagplaats van actieve dreigingen. In dit geval bewaart het programma het gedetecteerde bestand in het geheugen van de computer. Als u de dreiging van de computer wilt verwijderen, selecteer dan **Disinfect**.

Een dreiging verwerken in de Webconsole en de Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole **Operations** → **Repositories** → **Active threats**.

   De lijst met actieve dreigingen wordt geopend.

2. Selecteer het object dat u wilt verwerken.

3. Kies hoe u de dreiging wilt aanpakken:

   - **Disinfect**. Als deze optie is geselecteerd, probeert het programma automatisch om ieder gevonden geïnfecteerd bestand te desinfecteren. Mocht de desinfectie mislukken, dan wordt het bestand door het programma verwijderd.

   - **Delete**. Als deze optie is geselecteerd, verwijdert het programma het geïnfecteerde bestand dat wordt gedetecteerd, uit de opslagplaats van actieve dreigingen. In dit geval bewaart het programma het gedetecteerde bestand in het geheugen van de computer. Als u de dreiging van de computer wilt verwijderen, selecteer dan **Disinfect**.

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 het programma automatisch om ieder gevonden geïnfecteerd bestand te desinfecteren. Mocht de desinfectie mislukken, dan wordt het bestand door het programma verwijderd.

   - **Toevoegen aan uitzonderingen**. Als deze actie is geselecteerd, stelt Kaspersky Endpoint Security voor: het bestand toevoegen aan de lijst met scanuitzonderingen. 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 geselecteerd is, opent Kaspersky Endpoint Security de website Kaspersky database van kwetsbaarheden en dreigingen.

Om actieve dreigingen in de Kaspersky Security Center-console te verwerken, moet u de overdracht van informatie over onverwerkte bestanden naar Beheerserver inschakelen. Gegevensoverdracht is standaard ingeschakeld.

De overdracht van onverwerkte bestandsgegevens in quarantaine inschakelen in de Beheerconsole (MMC)

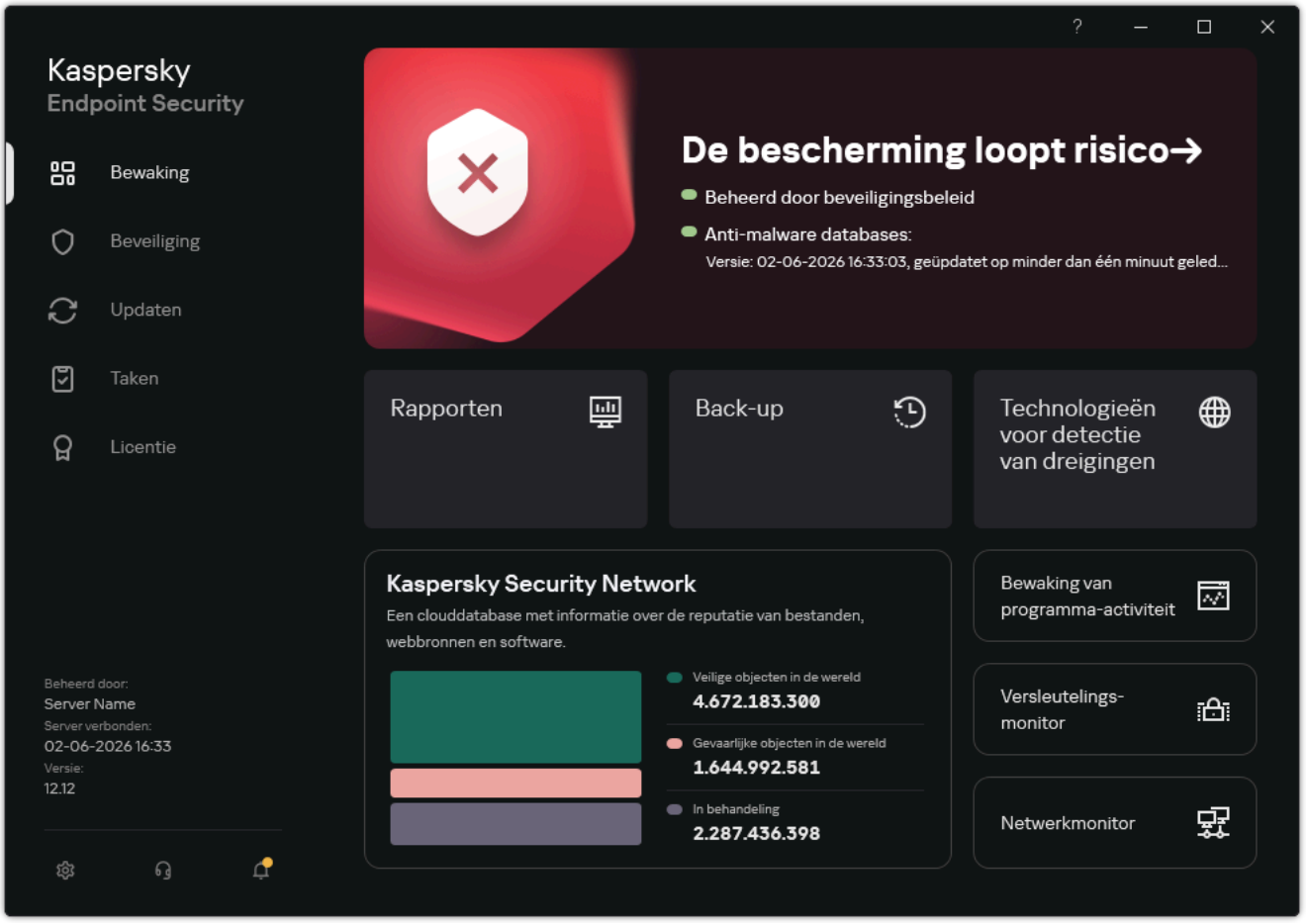
1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Algemene instellingen** → **Rapporten en Opslag** in het beleidsvenster.
4. In het blok **Gegevensoverdracht naar Administration Server**, klikt u op de knop **Instellingen**.
5. Selecteer het selectievakje **Onverwerkte bestanden**.
6. Sla uw wijzigingen op.

De overdracht van onverwerkte bestandsgegevens in quarantaine inschakelen in de Webconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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** → **KSC Integration**.

5. Schakel in het blok **Data transfer to Administration Server** het selectievakje **About unprocessed files** in.

6. Sla uw wijzigingen op.



Hoofdprogrammavenster wanneer een bedreiging wordt gedetecteerd

Computerbescherming

File Threat Protection

Met het onderdeel File Threat Protection kunt u infectie van het bestandssysteem van een computer voorkomen. Het onderdeel File Threat Protection bevindt zich standaard permanent in het RAM van de computer en scant alle bestanden die worden geopend, opgeslagen en uitgevoerd in realtime. Dit onderdeel scant bestanden op alle computerschijven, inclusief aangesloten schijven. Het onderdeel biedt computerbescherming met behulp van antivirusdatabases, de Kaspersky Security Network-cloudservice en heuristische analyse.

Het onderdeel scant de bestanden waartoe een 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 zich in de OneDrive-cloudopslag bevindt, 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.

Het onderdeel File Threat Protection gebruikt gegevens die ontvangen zijn van andere programma-onderdelen. Het inschakelen van deze componenten is optioneel. Componenten die extra gegevens leveren omvatten:

- Kaspersky Security Network.
- Host Intrusion Prevention.
- Gedragsdetectie.

Het onderdeel File Threat Protection in- of uitschakelen in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Essential Threat Protection** → **File Threat Protection** in het beleidsvenster.
4. Gebruik het selectievakje **File Threat Protection** om het onderdeel in of uit te schakelen.

5. 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.

     - **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 **Instellingen** en definieert u uw eigen onderdeelinstellingen.

     U kunt de waarden van vooraf ingestelde beveiligingsniveaus herstellen door te klikken op de knop **Standaard**.

6. Selecteer in het blok **Actie bij detectie van een dreiging** de actie die Kaspersky Endpoint Security moet uitvoeren op schadelijke objecten:

   - **Desinfecteren of verwijderen als desinfectie mislukt**. Als deze optie is geselecteerd, probeert het programma automatisch om ieder gevonden geïnfecteerd bestand te desinfecteren. Mocht de desinfectie mislukken, dan wordt het bestand door het programma verwijderd.

   - **Desinfecteren of blokkeren als desinfectie mislukt**. Als deze optie is geselecteerd, probeert het programma automatisch om ieder gevonden geïnfecteerd bestand te desinfecteren. Als de desinfectie mislukt, blokkeert het programma dit bestand.

   - **Blokkeren**. Als deze optie is geselecteerd, blokkeert het programma het geïnfecteerde bestand automatisch zonder te proberen het te desinfecteren of te verwijderen.

   - **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.

   Voordat u probeert een geïnfecteerd bestand te desinfecteren of te verwijderen, maakt het programma een reservekopie van het bestand voor het geval u het bestandmoet herstellen of als het in de toekomst kan worden gedesinfecteerd.

7. Sla uw wijzigingen op.

Het onderdeel File Threat Protection in- of uitschakelen in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Host Threat Protection** → **File Threat Protection**.
5. Gebruik de schakelaar **File Threat Protection ENABLED** om de component in of uit te schakelen.
6. Als u een nieuw object aan het beschermd bereik wilt toevoegen:

   a. Selecteer onder **Advanced settings** het tabblad **Protection scope**.

   b. Klik op **Add**.

   c. Dit opent een venster; kies in dat venster de objecten die u aan het beschermingsbereik wilt toevoegen.

   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:\Folder\**\*.txt` omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen bevinden genest in de `Folder`, uitgezonderd de `Folder` 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:\Folder\???.txt` omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam `Folder` bevinden, die een TXT-extensie hebben en die een naam met drie tekens hebben.

   U kunt maskers overal in een bestands- of mappad gebruiken. Als u bijvoorbeeld wilt dat het scanbereik de map Downloads bevat voor alle gebruikersaccounts op de computer, voert u het masker `C:\Users\*\Downloads\` uit.

   U kunt een object van bescherming uitsluiten zonder het uit de lijst met objecten in het beschermingsbereik te verwijderen. Dat doet u door de schakelaar ernaast uit te zetten.

   d. Sla uw wijzigingen op.

7. Selecteer in het blok **Action on threat detection** de actie die Kaspersky Endpoint Security moet uitvoeren op schadelijke objecten:

   - **Disinfect, delete if disinfection fails**. Als deze optie is geselecteerd, probeert het programma automatisch om ieder gevonden geïnfecteerd bestand te desinfecteren. Mocht de desinfectie mislukken, dan wordt het bestand door het programma verwijderd.

   - **Disinfect, block if disinfection fails**. Als deze optie is geselecteerd, probeert het programma automatisch om ieder gevonden geïnfecteerd bestand te desinfecteren. Als de desinfectie mislukt, blokkeert het programma dit bestand.

   - **Block**. Als deze optie is geselecteerd, blokkeert het programma het geïnfecteerde bestand automatisch zonder te proberen het te desinfecteren of te verwijderen.

   Voordat u probeert een geïnfecteerd bestand te desinfecteren of te verwijderen, maakt het programma een reservekopie van het bestand voor het geval u het bestandmoet herstellen of als het in de toekomst kan worden gedesinfecteerd.

8. Bewerk in dien nodig de geavanceerde instellingen van File Threat Protection.

9. Sla uw wijzigingen op.

Het onderdeel File Threat Protection in de programma-interface in- of uitschakelen

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.

     - **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 beveiligingsniveaus herstellen door te klikken op de knop **Aanbevolen beveiligingsniveau herstellen**.

5. Selecteer in het blok **Actie bij detectie van een dreiging** de actie die Kaspersky Endpoint Security moet uitvoeren op schadelijke objecten:

   - **Desinfecteren of verwijderen als desinfectie mislukt**. Als deze optie is geselecteerd, probeert het programma automatisch om ieder gevonden geïnfecteerd bestand te desinfecteren. Mocht de desinfectie mislukken, dan wordt het bestand door het programma verwijderd.

   - **Desinfecteren of blokkeren als desinfectie mislukt**. Als deze optie is geselecteerd, probeert het programma automatisch om ieder gevonden geïnfecteerd bestand te desinfecteren. Als de desinfectie mislukt, blokkeert het programma dit bestand.

   - **Blokkeren**. Als deze optie is geselecteerd, blokkeert het programma het geïnfecteerde bestand automatisch zonder te proberen het te desinfecteren of te verwijderen.

   - **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.

   Voordat u probeert een geïnfecteerd bestand te desinfecteren of te verwijderen, maakt het programma een reservekopie van het bestand voor het geval u het bestandmoet herstellen of als het in de toekomst kan worden gedesinfecteerd.

6. Sla uw wijzigingen op.

Instellingen voor File Threat Protection aanbevolen door Kaspersky-experts (aanbevolen beveiligingsniveau)

Parameter	Waarde	Beschrijving
Bestandstypen	**Bestanden gescand op indeling**	Als deze instelling is ingeschakeld, scant het programma alleen infecteerbare bestanden. 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.
Heuristische analyse	**Oppervlakkige scan**	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.
Scan alleen nieuwe en aangepaste bestanden	**Aan**	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.
Gebruik iSwift-technologie	**Aan**	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.

Parameter	Waarde	Beschrijving
Gebruik iChecker-technologie	**Aan**	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).
Scan Microsoft Office-bestanden	**Aan**	Scant Microsoft Office-bestanden (DOC, DOCX, XLS, PPT en andere Microsoft-extensies). Bestanden in Office-indeling bevatten ook OLE-objecten. Het programma scant office-bestanden die kleiner zijn dan 1 MB, ongeacht of het selectievakje is ingeschakeld of niet.
Bestanden in e-mailindeling scannen	**Aan**	Scant bestanden in e-mailformaat. Het programma scant MSG- en EML-bestanden. Bestanden in e-mailformaat bevatten ook OLE-objecten en MHT-bestanden. Kaspersky Endpoint Security scant bestanden in e-mailformaat die kleiner zijn dan 1 MB, ongeacht of het selectievakje is ingeschakeld of niet.
Scanmodus	**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.
Actie bij detectie van een dreiging	**Desinfecteren of verwijderen als desinfectie mislukt**	Als deze optie is geselecteerd, probeert het programma automatisch om ieder gevonden geïnfecteerd bestand te desinfecteren. Mocht de desinfectie mislukken, dan wordt het bestand door het programma 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 het programma automatisch om ieder gevonden geïnfecteerd bestand te desinfecteren. Mocht de desinfectie mislukken, dan wordt het bestand door het programma verwijderd.
   - **Desinfecteren of blokkeren als desinfectie mislukt**. Als deze optie is geselecteerd, probeert het programma automatisch om ieder gevonden geïnfecteerd bestand te desinfecteren. Als de desinfectie mislukt, blokkeert het programma dit bestand.
   - **Blokkeren**. Als deze optie is geselecteerd, blokkeert het programma het geïnfecteerde bestand automatisch zonder te proberen het te desinfecteren of te verwijderen.

   Voordat u probeert een geïnfecteerd bestand te desinfecteren of te verwijderen, maakt het programma een reservekopie van het bestand voor het geval u het bestandmoet 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, scant het programma alleen infecteerbare bestanden. 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, scant het programma alleen infecteerbare bestanden. 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. Voer in het veld **Pad** 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:\Folder\**\*.txt` omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen bevinden genest in de `Folder`, uitgezonderd de `Folder` 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:\Folder\???.txt` omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam `Folder` bevinden, die een TXT-extensie hebben en die een naam met drie tekens hebben.

U kunt maskers overal in een bestands- of mappad gebruiken. Als u bijvoorbeeld wilt dat het scanbereik de map Downloads bevat voor alle gebruikersaccounts op de computer, voert u het masker `C:\Users\*\Downloads\` uit.

Het object **Deze pc** in de lijst van bestandsbronnen van de computer omvat de volgende objecten: **Alle harde schijven**, **Alle netwerkschijven** en **Alle verwisselbare schijven**.

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 bestandsbedreigingen, 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.

   - **Gebruik 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.

   - **Gebruik 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 **Optimalisatie** het selectievakje **Scan alleen nieuwe en aangepaste 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 mail 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.

Container Scan

Een *container* is een geïsoleerde omgeving waarin een programma kan draaien zonder directe interactie met het besturingssysteem. Het gebruik van containers brengt de volgende risico's met zich mee:

- Hackers kunnen mogelijk kwetsbaarheden in containerisatie misbruiken om programma's in de container te compromitteren.
- Hackers kunnen misbruik maken van een onveilige configuratie van de containeromgeving om ongeautoriseerde toegang te krijgen tot gegevens op de computer of om de integriteit van het systeem in gevaar te brengen.
- Door een succesvolle aanval op een container kan een hacker toegang krijgen tot gegevens op de computer.
- Hackers kunnen misbruik maken van netwerkkwetsbaarheden om netwerkverkeer te onderscheppen.

Kaspersky Endpoint Security scant bestanden niet alleen op schijven, maar ook in containers. Dat wil zeggen, Kaspersky Endpoint Security is een externe tool voor het detecteren van kwaadaardige activiteiten in containers. Hierdoor kunnen de prestaties van containers behouden blijven en worden conflicten met andere programma's in de container voorkomen. Het installeren van Kaspersky Endpoint Security in de container wordt niet ondersteund.

Kaspersky Endpoint Security biedt niet alleen containerbeveiliging, maar maakt het ook mogelijk om programma's in containers te beheren met: Programmacontrole. Programmacontrole wordt voor containers op dezelfde manier geconfigureerd als voor programma's die op de computer zijn geïnstalleerd. Systeemintegriteitscontrole ondersteunt ook containers.

Containervereisten

- De container moet een Docker-container zijn. Andere containerisatietools worden niet ondersteund.
- De container moet in de procesisolatiemodus worden uitgevoerd. De Hyper-V-isolatiemodus wordt niet ondersteund.
- De container moet op een server met Windows Server 2016, 2019 of 2022 worden geplaatst (Docker Host).
- De container moet een Windows-image bevatten (Docker Image). Windows 10 en 11 worden niet ondersteund. Linux-afbeeldingen worden niet ondersteund.

Actie bij detectie van een dreiging

Als er een bedreiging in een container wordt gedetecteerd, voert het programma de actie uit die is geselecteerd voor het onderdeel File Threat Protection. Container Scan heeft aanvullende instellingen (zie de onderstaande instructies). Als er een bedreiging wordt gedetecteerd, blokkeert het programma de schadelijke activiteit en voert de geselecteerde actie uit (bijvoorbeeld pogingen om het object te desinfecteren). Kaspersky Endpoint Security kan de container stoppen als het gedetecteerde object niet kan worden gedesinfecteerd. Standaard is de functionaliteit voor het stoppen van containers uitgeschakeld.

Containers scannen configureren in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Essential Threat Protection** → **File Threat Protection** in het beleidsvenster.
4. Klik op **Instellingen**.
5. Dit opent een venster; selecteer in dat venster het tabblad **Extra**.
6. Configureer in het blok **Scan van bestandsbewerkingen uitgevoerd in Windows containers** de scaninstellingen van de containers:
   - **Stop de container als desinfectie mislukt**. Het programma beschikt mogelijk niet over voldoende lees- en schrijfrechten voor het gedetecteerde object. In dat geval is het niet mogelijk om het gedetecteerde object te desinfecteren of te verwijderen. Als dit selectievakje is ingeschakeld, blokkeert het programma het gedetecteerde object en stopt de container. Als dit selectievakje is uitgeschakeld, blokkeert het programma alleen het gedetecteerde object.
   - **Bestandsbewerkingen uitgevoerd in Windows container niet scannen**. Als het selectievakje is ingeschakeld, scant het programma de container alleen wanneer de container wordt gestart. Als het selectievakje is uitgeschakeld, scant het programma de container continu in realtime.
7. Sla uw wijzigingen op.

Containers scannen configureren in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Host Threat Protection** → **File Threat Protection**.
5. Selecteer onder **Advanced settings** het tabblad **Performance**.

6. Configureer in het blok **Scan optimization** de scaninstellingen van de containers:

   - **Stop container if disinfection fails**. Het programma beschikt mogelijk niet over voldoende lees- en schrijfrechten voor het gedetecteerde object. In dat geval is het niet mogelijk om het gedetecteerde object te desinfecteren of te verwijderen. Als dit selectievakje is ingeschakeld, blokkeert het programma het gedetecteerde object en stopt de container. Als dit selectievakje is uitgeschakeld, blokkeert het programma alleen het gedetecteerde object.

   - **Do not scan file operations executed in Windows containers**. Als het selectievakje is ingeschakeld, scant het programma de container alleen wanneer de container wordt gestart. Als het selectievakje is uitgeschakeld, scant het programma de container continu in realtime.

7. Sla uw wijzigingen op.

Containers scannen configureren in het programma-interface

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. Configureer in het blok **Scan van bestandsbewerkingen uitgevoerd in Windows-containers** de scaninstellingen van de containers:

   - **Stop de container als desinfectie mislukt**. Het programma beschikt mogelijk niet over voldoende lees- en schrijfrechten voor het gedetecteerde object. In dat geval is het niet mogelijk om het gedetecteerde object te desinfecteren of te verwijderen. Als dit selectievakje is ingeschakeld, blokkeert het programma het gedetecteerde object en stopt de container. Als dit selectievakje is uitgeschakeld, blokkeert het programma alleen het gedetecteerde object.

   - **Scan geen bestandsbewerkingen die worden uitgevoerd in Windows-containers**. Als het selectievakje is ingeschakeld, scant het programma de container alleen wanneer de container wordt gestart. Als het selectievakje is uitgeschakeld, scant het programma de container continu in realtime.

4. 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 toegangsparameters:

- Toegang tot besturingssysteembronnen (bijvoorbeeld automatische-opstartopties, registersleutels)
- Toegang tot persoonlijke gegevens (bijvoorbeeld bestanden en programma's)

De netwerkactiviteit van programma's wordt door het onderdeel firewall beheerd 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. Plaatst het programma in een van de vertrouwensgroepen: *Vertrouwd*, *Deels beperkt*, *Zeer beperkt*, *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 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.

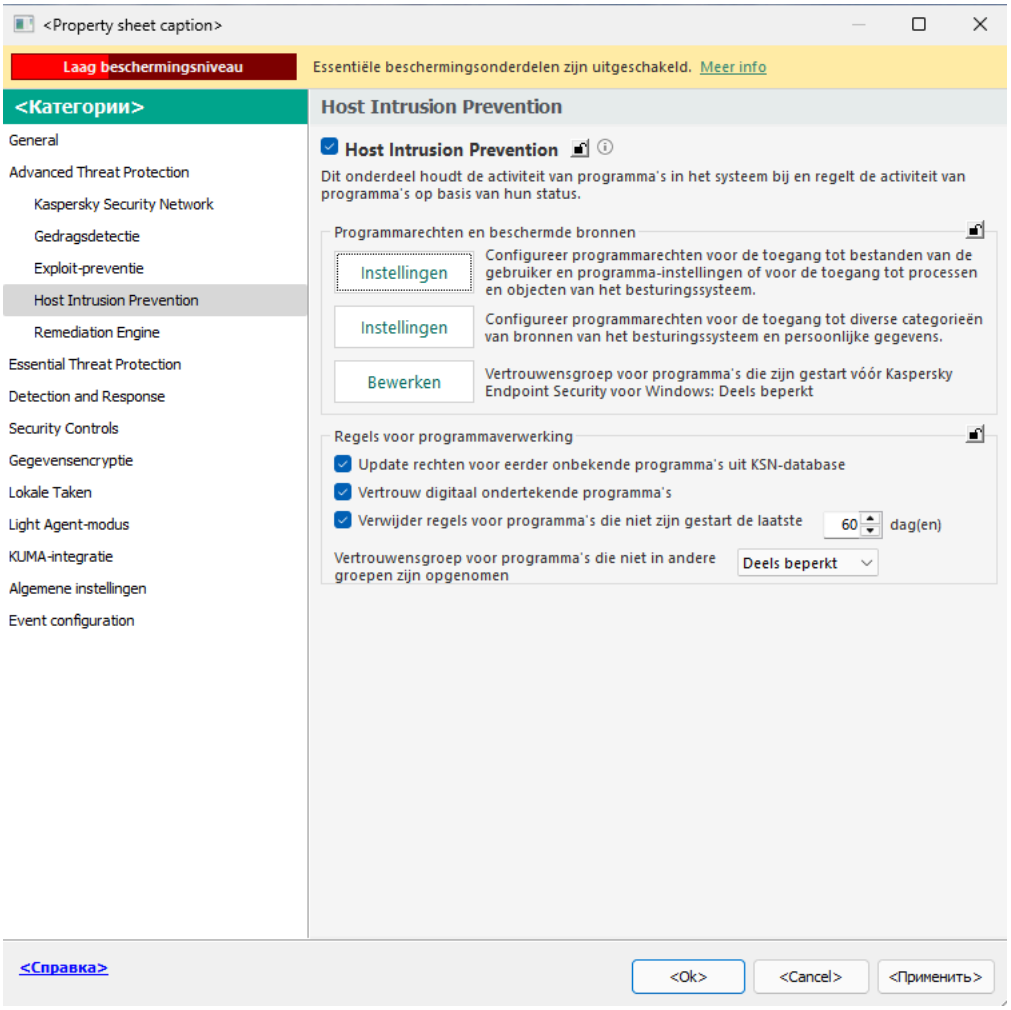
De volgende keer dat het programma wordt gestart, controleert Kaspersky Endpoint Security de integriteit van het programma. Als het programma niet is gewijzigd, gebruikt het onderdeel de huidige programmarechten ervoor. Als het programma is gewijzigd, analyseert Kaspersky Endpoint Security het programma alsof het voor het eerst wordt gestart.

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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Advanced Threat Protection** → **Host Intrusion Prevention** in het beleidsvenster.



Instellingen van Inbraakpreventie

4. Gebruik het selectievakje **Host Intrusion Prevention** om het onderdeel in of uit te schakelen.
5. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Het onderdeel Host Intrusion Prevention in- of uitschakelen in de webconsole en cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Host Threat Protection** → **Host Intrusion Prevention**.
5. Gebruik de schakelaar **Host Intrusion Prevention ENABLED** 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 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 automatisch alle onbekende programma's moet toevoegen. Programma's die actief waren voordat Kaspersky Endpoint Security werd gestart, worden automatisch in de vertrouwensgroep geplaatst ingesteld in de instellingen van Host Intrusion Prevention.

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.

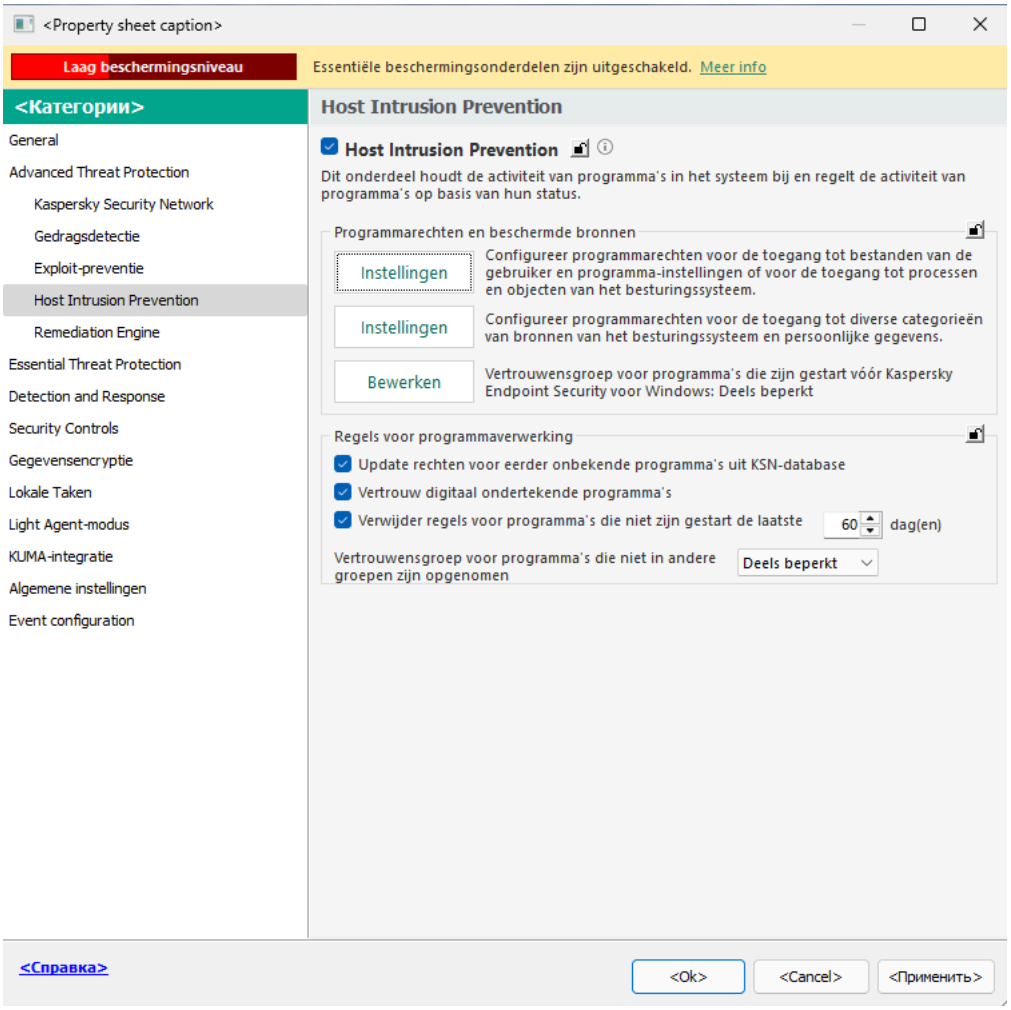
De vertrouwensgroep van een programma wijzigen

Wanneer een programma voor het eerst wordt gestart, controleert het onderdeel Host Intrusion Prevention de beveiliging van het programma en plaatst het 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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Advanced Threat Protection** → **Host Intrusion Prevention** in het beleidsvenster.



Instellingen van Inbraakpreventie

4. In het blok **Programmarechten en beschermde bronnen**, klikt u op de knop **Instellingen**.

   Dit opent het venster voor configuratie van programmarechten en de lijst met beschermde bronnen.
5. Selecteer het tabblad **Programmarechten**.
6. Klik op **Toevoegen**.
7. 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.
8. Klik op **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.
9. Selecteer het noodzakelijke programma.

10. Selecteer in de vervolgkeuzelijst **Geselecteerd programma toevoegen aan vertrouwensgroep** de benodigde vertrouwensgroep voor het programma.

11. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

De vertrouwensgroep van een programma veranderen in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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 **Host Threat Protection** → **Host Intrusion Prevention**.

5. Klik in het blok **Application rights and protected resources** op de koppeling **Application rights and protected resources**.

   Dit opent het venster voor configuratie van programmarechten 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 **Application**. Ga naar de volgende stap.

   Als u de vertrouwensgroep voor meerdere programma's wilt wijzigen, selecteert u het type **Group** en definieert u een naam voor de programmagroep.

10. Selecteer in de geopende lijst met programma's de programma's waarvan u de vertrouwensgroep wil 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. Verlaat de wizard verlaten.

    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 **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 *(gedefinieerd door gebruiker)* 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

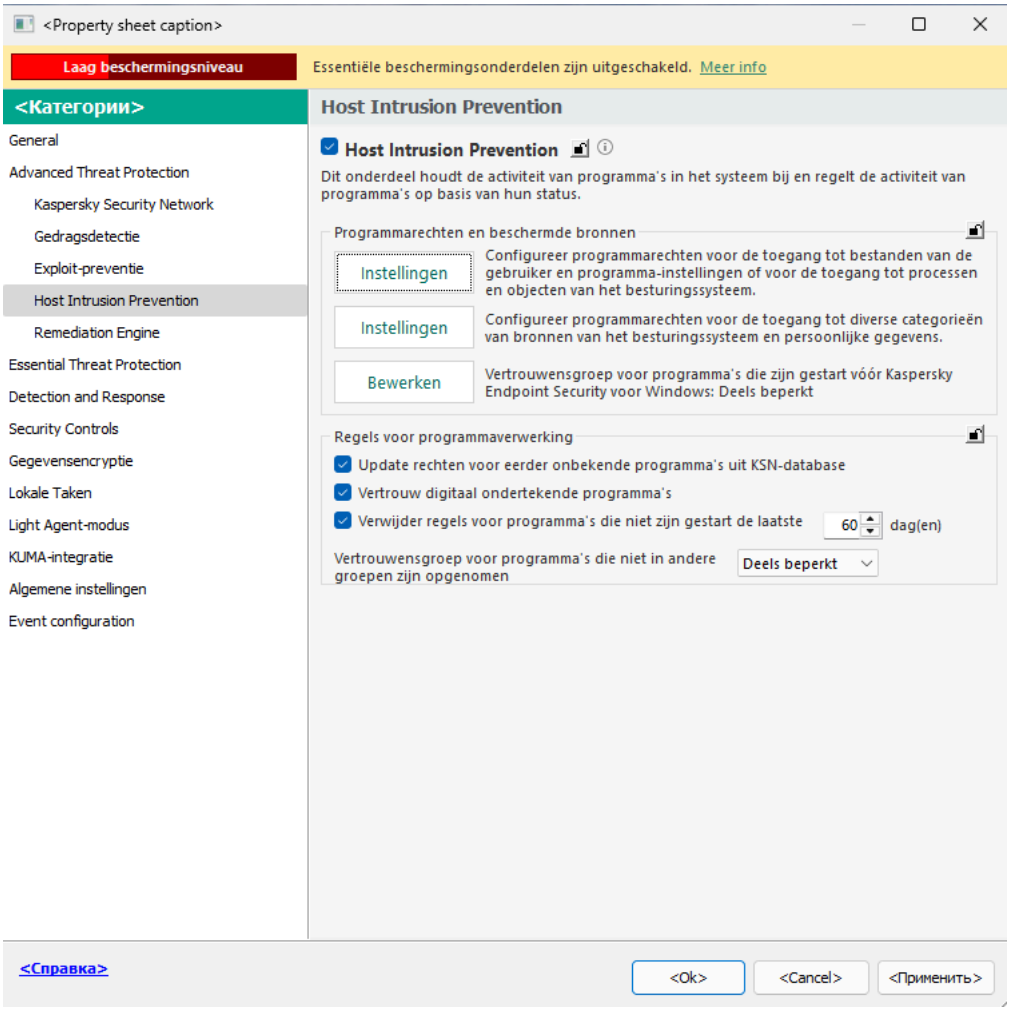
De optimale programmarechten worden standaard aangemaakt voor verschillende vertrouwensgroepen. De instellingen voor programmagroepen die zich in een vertrouwensgroep bevinden nemen de waarden over van de instellingen van de rechten van de vertrouwensgroep.

De rechten van een vertrouwensgroep veranderen in de beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.

2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

3. Selecteer **Advanced Threat Protection** → **Host Intrusion Prevention** in het beleidsvenster.



Instellingen van Inbraakpreventie

4. In het blok **Programmarechten en beschermde bronnen**, klikt u op de knop **Instellingen**.

   Dit opent het venster voor configuratie van programmarechten en de lijst met beschermde bronnen.

5. Ga naar het tabblad **Programmarechten**.
6. Selecteer de nodige vertrouwensgroep.
7. Selecteer in het contextmenu de vertrouwensgroep **Groepsrechten**.

   Dit opent de eigenschappen van de vertrouwensgroep.
8. Doe een van de volgende acties:

   - Selecteer **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 **Rechten**.

   De netwerkactiviteit van programma's wordt door het onderdeel firewall beheerd met behulp van *netwerkregels*.
9. 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** (⊘).
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. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Rechten van vertrouwensgroep maken in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Host Threat Protection** → **Host Intrusion Prevention**.
5. Klik in het blok **Application rights and protected resources** op de koppeling **Application rights and protected resources**.

   Dit opent het venster voor configuratie van programmarechten en de lijst met beschermde bronnen.
6. Ga naar 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 vertrouwensgroeprechten wilt bewerken die de toegang tot processen en objecten van het besturingssysteem regelen, selecteer dan **Rights**.

   De netwerkactiviteit van programma's wordt door het onderdeel firewall beheerd met behulp van *netwerkregels*.

9. Voor de relevante bron klikt u in de kolom van de bijbehorende actie de benodigde optie: **Inherit**, **Allow** ( ) of **Block** ( ).

10. Als u het gebruik van computerbronnen wilt bewaken, selecteert u **Log events** (/).

    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 **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 **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 **Rechten**.

   De netwerkactiviteit van programma's wordt door het onderdeel firewall beheerd met behulp van *netwerkregels*.

7. Voer 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 (*Aangepaste instellingen*) wordt toegewezen aan de vertrouwensgroep.

Een vertrouwensgroep selecteren voor programma's die vóór Kaspersky Endpoint Security worden gestart

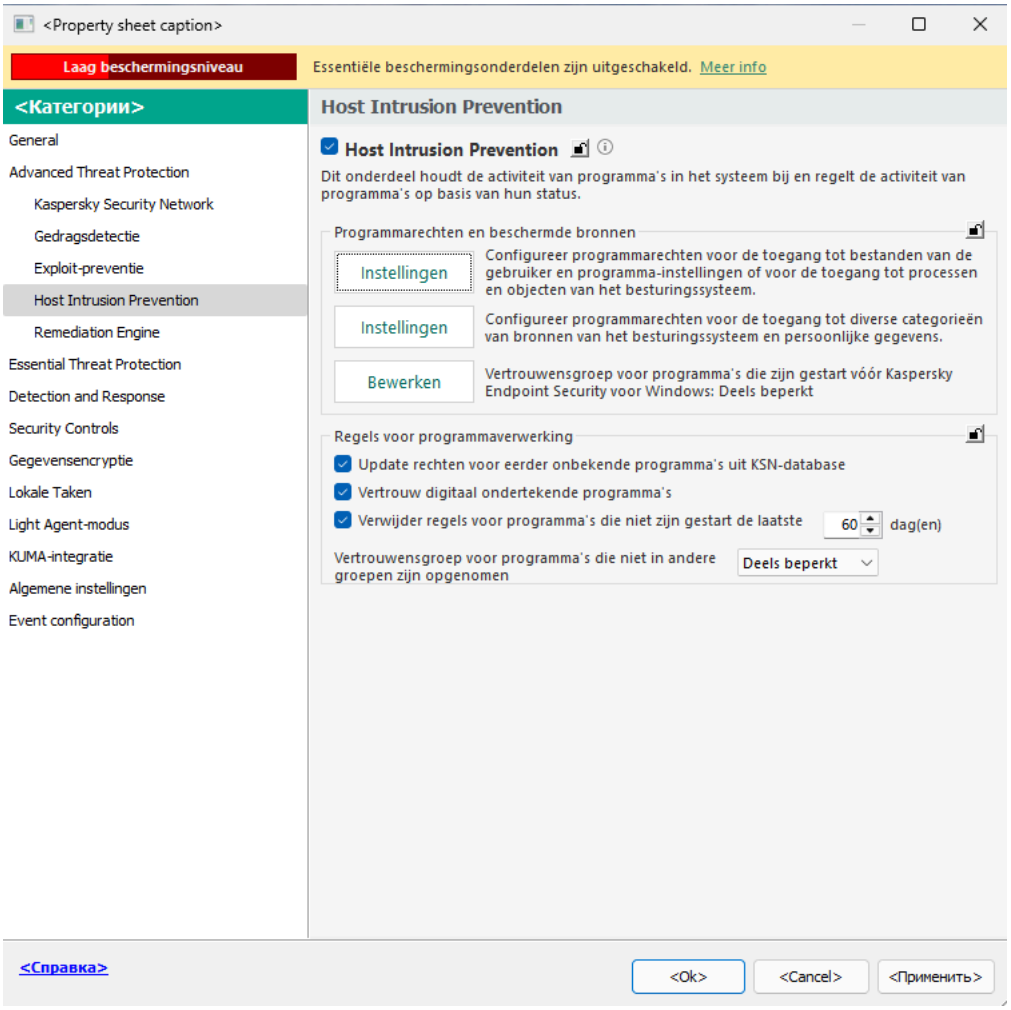
Voor programma's die vóór Kaspersky Endpoint Security zijn gestart, wordt alleen de netwerkactiviteit gecontroleerd. De controle wordt uitgevoerd met de netwerkregels die in de instellingen van Firewall zijn ingesteld. U moet een vertrouwensgroep selecteren om op te geven welke netwerkregels u wilt toepassen 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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.

2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

3. Selecteer **Advanced Threat Protection** → **Host Intrusion Prevention** in het beleidsvenster.



Instellingen van Inbraakpreventie

4. In het blok **Programmarechten en beschermde bronnen**, klikt u op de knop **Bewerken**.

5. Selecteer voor de instelling **Trust group for applications started before Kaspersky Endpoint Security** selecteert u de gepaste vertrouwensgroep.

6. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Een vertrouwensgroep selecteren voor programma's die vóór Kaspersky Endpoint Security zijn gestart in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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 **Host Threat Protection** → **Host Intrusion Prevention**.

5. Selecteer voor de instelling **Trust group for applications started before Kaspersky Endpoint Security** 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. Selecteer voor het blok **Vertrouwensgroep voor programma's gestart vóór Kaspersky Endpoint Security** 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.

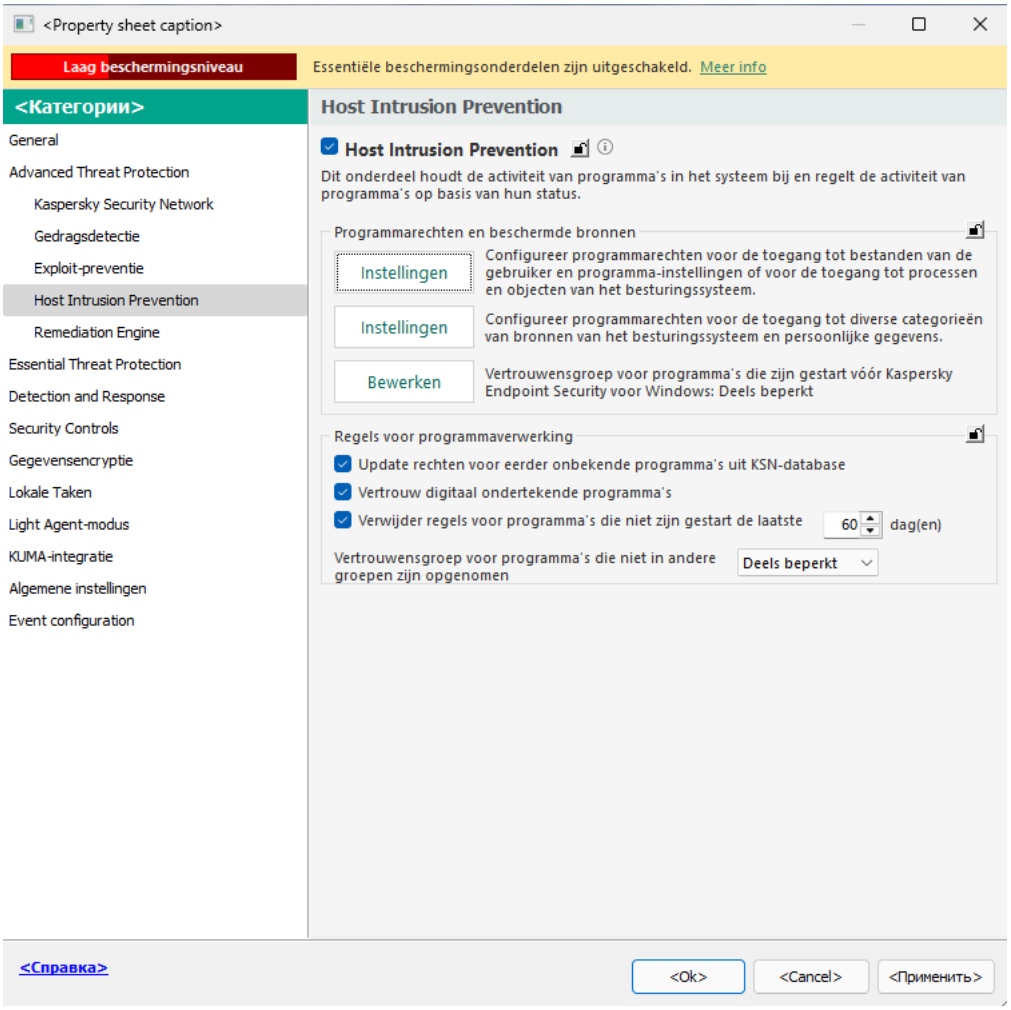
Een vertrouwensgroep selecteren voor onbekende programma's

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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

3. Selecteer **Advanced Threat Protection** → **Host Intrusion Prevention** in het beleidsvenster.



Instellingen van Inbraakpreventie

4. Gebruik in het blok **Application processing rules** de vervolgkeuzelijst **Trust group for applications not included in other groups** 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.

5. Gebruik het selectievakje **Update rights for previously unknown applications from KSN database** om de automatische update te configureren van de rechten van onbekende programma's.

6. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Een vertrouwensgroep selecteren voor onbekende programma's in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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 **Host Threat Protection** → **Host Intrusion Prevention**.

5. Gebruik in het blok **Application processing rules** de vervolgkeuzelijst **Trust group for applications not included in other groups** 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 rights for previously unknown applications from 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 voor het blok **Regels voor programmaverwerking** de gepaste 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

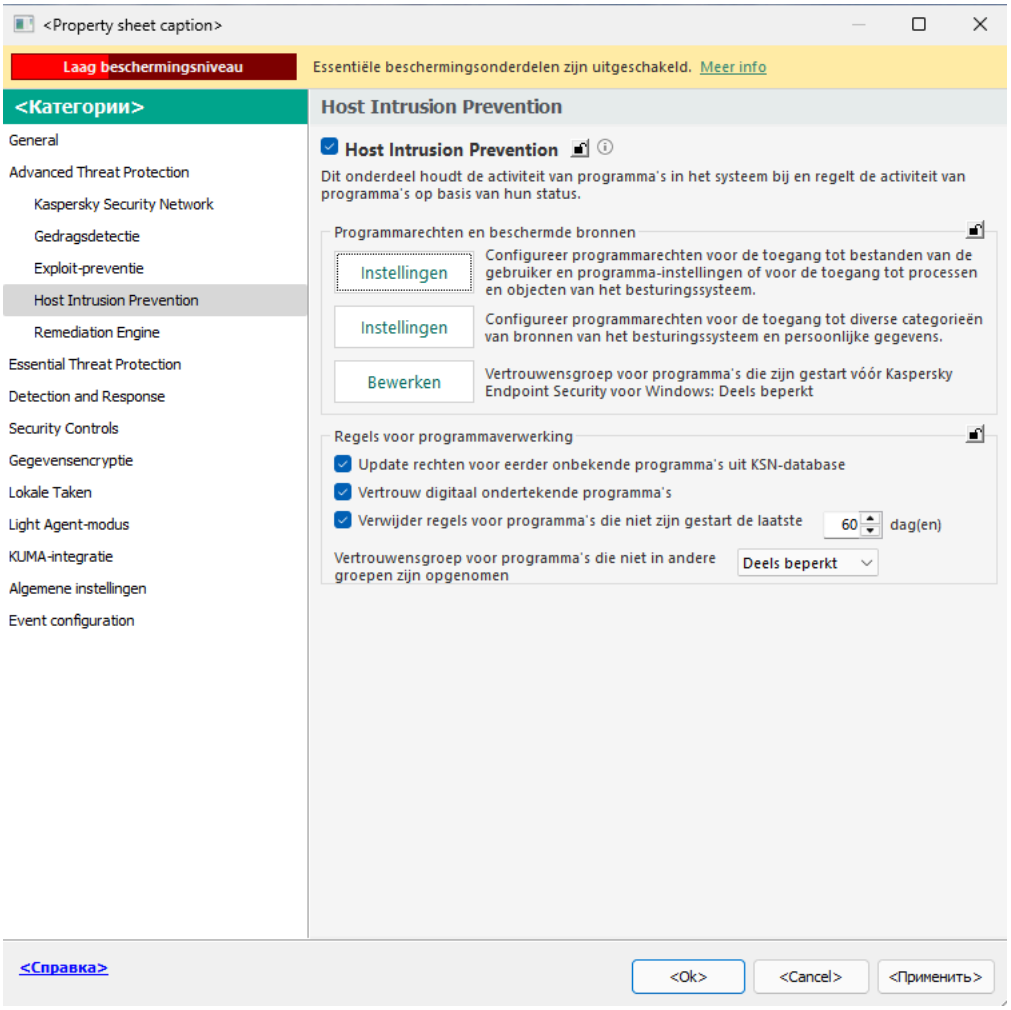
Kaspersky Endpoint Security plaatst programma's ondertekend door Microsoft- of Kaspersky-certificaten altijd in de groep *Vertrouwd*.

Een vertrouwensgroep selecteren voor digitaal ondertekende programma's in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.

2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

3. Selecteer **Advanced Threat Protection** → **Host Intrusion Prevention** in het beleidsvenster.



Instellingen van Inbraakpreventie

4. Gebruik in het blok **Application processing rules** het selectievakje **Trust digitally signed applications** om de automatische toewijzing aan de Trusted 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.

5. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Een vertrouwensgroep selecteren voor digitaal ondertekende programma's in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Host Threat Protection** → **Host Intrusion Prevention**.

5. Gebruik in het blok **Application processing rules** het selectievakje **Trust digitally signed applications** om de automatische toewijzing aan de Trusted 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 **Application processing rules** het selectievakje **Trust digitally signed applications** om de automatische toewijzing aan de Trusted 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.

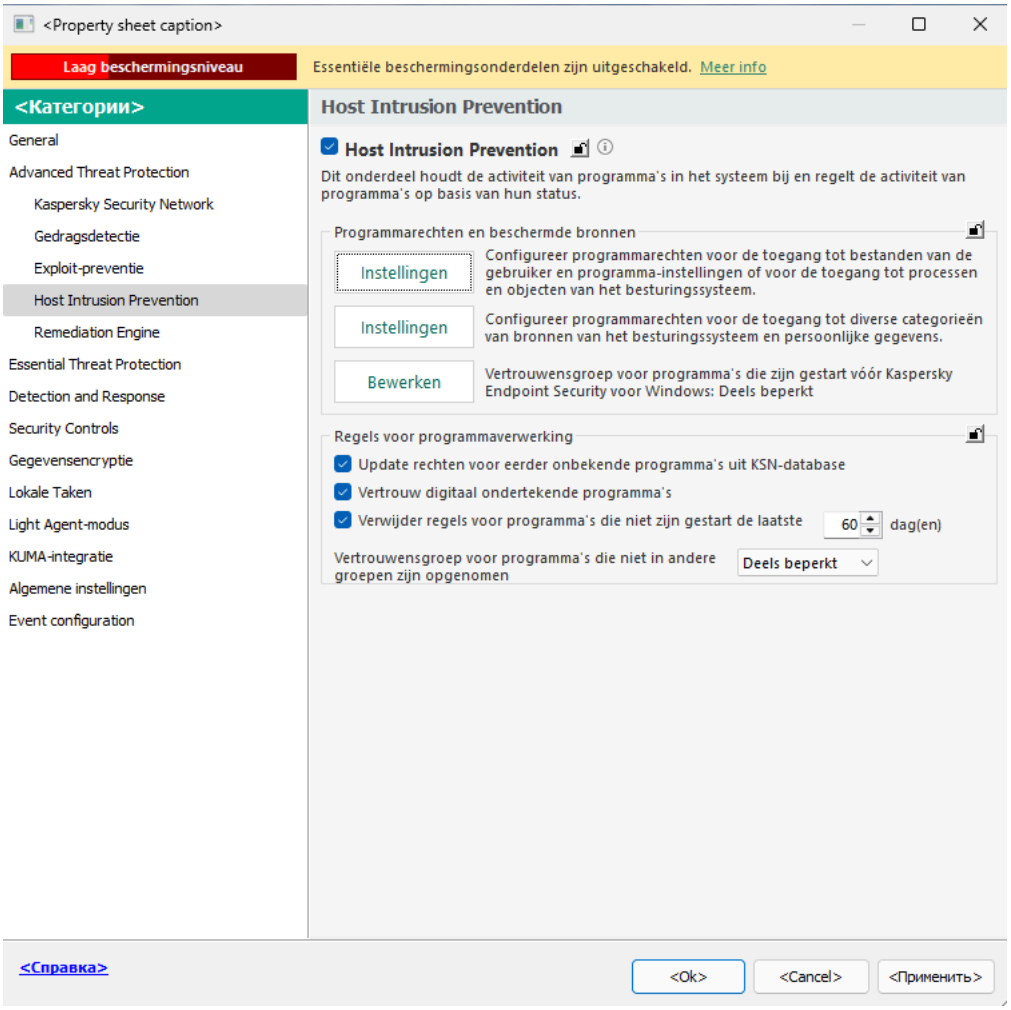
De regels die u aanmaakt voor programma's worden door de onderliggende processen overgenomen. Als u bijvoorbeeld alle netwerkactiviteit voor cmd.exe blokkeert, wordt alle netwerkactiviteit ook geblokkeerd voor notepad.exe als dat programma wordt gestart via cmd.exe. Wanneer een programma geen onderliggend proces is van een ander programma dat het heeft gestart, worden regels niet overgenomen.

Programmarechten toevoegen of verwijderen in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.

2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

3. Selecteer **Advanced Threat Protection → Host Intrusion Prevention** in het beleidsvenster.



Instellingen van Inbraakpreventie

4. In het blok **Programmarechten en beschermde bronnen**, klikt u op de knop **Instellingen**.

   Dit opent het venster voor configuratie van programmarechten en de lijst met beschermde bronnen.

5. Ga naar het tabblad **Programmarechten**.

6. Klik op **Toevoegen**.

7. Voer in het venster dat opent de criteria in om te zoeken naar het programma waarvan u de programmarechten 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.

8. Klik op **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.

9. Selecteer het noodzakelijke programma.

10. Selecteer in de vervolgkeuzelijst **Geselecteerd programma toevoegen aan vertrouwensgroep** de optie **Standaardgroepen** en klik op **OK**.

    Het programma wordt toegevoegd aan de standaard groep.

11. Selecteer het relevante programma en vervolgens **Programmarechten** in het contextmenu van het programma.

    Dit opent de programma-eigenschappen.

12. Doe een van de volgende acties:

    - Selecteer **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 **Rechten**.

    De netwerkactiviteit van programma's wordt door het onderdeel firewall beheerd met behulp van *netwerkregels*.

13. 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** (⊘).

14. 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.

15. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Programmarechten veranderen in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Host Threat Protection** → **Host Intrusion Prevention**.
5. Klik in het blok **Application rights and protected resources** op de koppeling **Application rights and protected resources**.

   Dit opent het venster voor configuratie van programmarechten en de lijst met beschermde bronnen.
6. Ga naar 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 **Application**. Ga naar de volgende stap.

   Als u de vertrouwensgroep voor meerdere programma's wilt wijzigen, selecteert u het type **Group** en definieert u een naam voor de programmagroep.

10. Selecteer in de geopende lijst met programma's de programma's waarvan u de programmarechten wil 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. Verlaat de wizard verlaten.

    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 vertrouwensgroeprechten wilt bewerken die de toegang tot processen en objecten van het besturingssysteem regelen, selecteer dan **Rights**.

    > De netwerkactiviteit van programma's wordt door het onderdeel firewall beheerd met behulp van *netwerkregels*.

14. Voor de relevante bron klikt u in de kolom van de bijbehorende actie de benodigde optie: **Inherit**, **Allow** (✓) of **Block** (✗).

15. Als u het gebruik van computerbronnen wilt bewaken, selecteert u **Log events** (/).

    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 **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 **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 **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
Scan geen bestanden die door het programma worden geopend	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.
Bewaak geen programma-activiteit	Kaspersky Endpoint Security controleert de bestands- en netwerkactiviteit van het programma in het besturingssysteem niet. U kunt het monitoren van programma-activiteit configureren voor verschillende onderdelen van Kaspersky Endpoint Security: • **Bewaak niet voor beschermings- en controleonderdelen**. De programma/activiteit wordt gecontroleerd door de volgende componenten: Gedragsdetectie, Exploit-preventie, Host Intrusion Prevention, Remediation Engine en Firewall. • **Bewaak niet voor Managed Detection and Response en Endpoint Detection and Response**. De programma/activiteit wordt gecontroleerd door ingebouwde MDR agent en ingebouwde EDR (KATA) agent. • **Interactieve console-invoer voor Endpoint Detection and Response niet onderscheppen**. Kaspersky Endpoint Security verzendt geen telemetriegegevens over het beheer van het programma op de console. Telemetriegegevens worden gebruikt door Kaspersky Anti Targeted Attack Platform (EDR).
Neem geen beperkingen van bovenliggend proces (programma) over	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 programmamachtigingen (Host Intrusion Prevention) en netwerkregels voor programma's (Firewall) zijn geconfigureerd.
Bewaak geen activiteit van onderliggende programma's	Kaspersky Endpoint Security bewaakt de bestands- of netwerkactiviteit van programma's die worden gestart door het programma niet. U kunt de uitzondering recursief toepassen. Zodat het programma niet de activiteit van de hele keten van onderliggende programma's bewaakt.
Sta interactie met de interface van Kaspersky Endpoint Security toe	Kaspersky Endpoint Security Self-Defense 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.
Scan geen versleuteld verkeer / Scan niet al het verkeer	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. Kaspersky Endpoint Security versie 14.0 of ouder ondersteunt het uitsluiten van netwerkverkeer als een hash is opgegeven voor een vertrouwd programma in plaats van een pad niet.

Bronnen van het besturingssysteem en persoonsgegevens beschermen

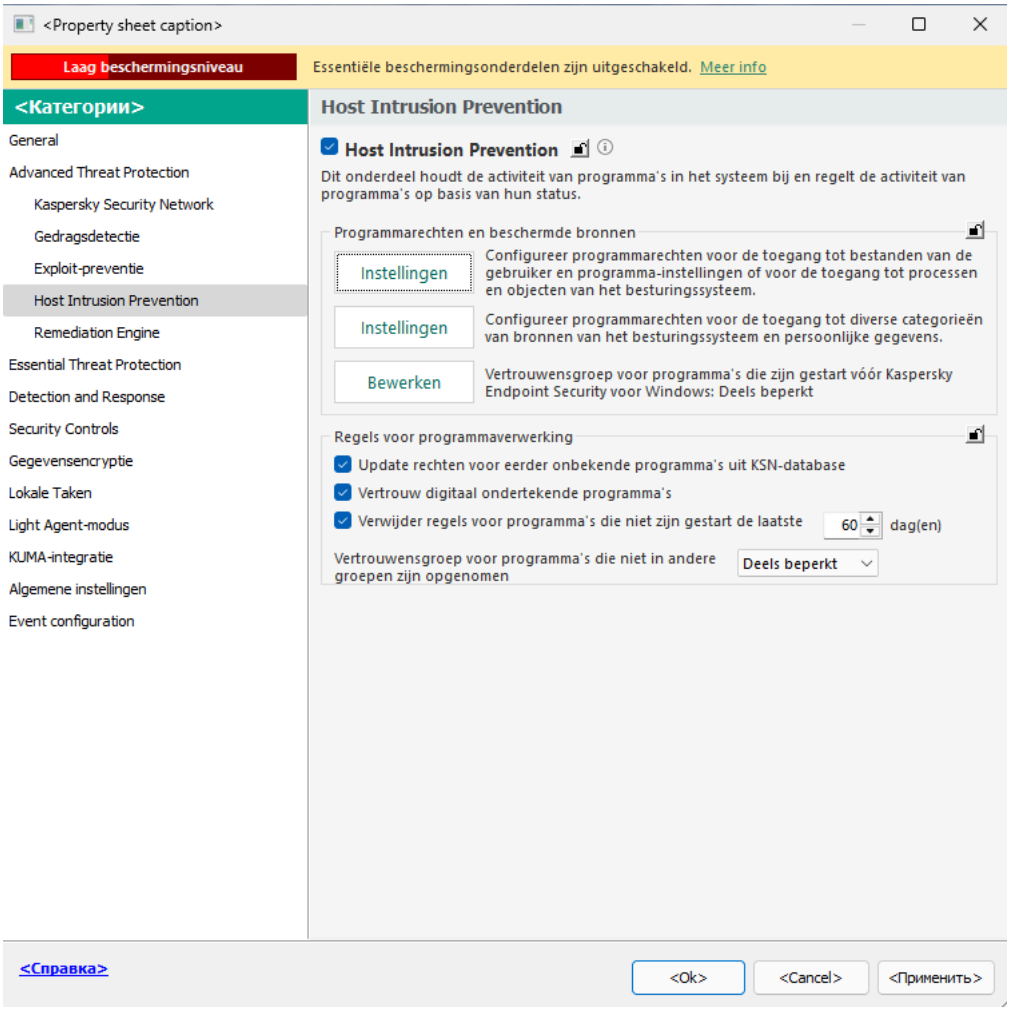
Het onderdeel Host Intrusion Prevention beheert de rechten van programma's om acties uit te voeren op diverse categorieën van bronnen van het besturingssysteem en persoonlijke gegevens. Kaspersky-experts hebben vooraf ingestelde categorieën van beschermde bronnen gemaakt. De categorie *Besturingssysteem* 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.

Een beschermde bron toevoegen in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.

2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

3. Selecteer **Advanced Threat Protection** → **Host Intrusion Prevention** in het beleidsvenster.



Instellingen van Inbraakpreventie

4. In het blok **Programmarechten en beschermde bronnen**, klikt u op de knop **Instellingen**.

   Dit opent het venster voor configuratie van programmarechten en de lijst met beschermde bronnen.

5. Ga naar 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.

6. 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**.

7. Klik op de knop **Toevoegen**. Selecteer in de vervolgkeuzelijst het type bron dat u wilt toevoegen: **Bestand of map** of **Registersleutel**.

8. 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.

9. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Een beschermde bron toevoegen in de Webconsole en de Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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 **Host Threat Protection** → **Host Intrusion Prevention**.

5. Klik in het blok **Application rights and protected resources** op de koppeling **Application rights and protected resources**.

   Dit opent het venster voor configuratie van programmarechten en de lijst met beschermde bronnen.

6. Ga naar 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 **Add**.

   De wizard Nieuwe bron wordt gestart.

8. Selecteer in het blok **Group name** de categorie beveiligde bronnen waaraan u een nieuwe beveiligde bron wilt toevoegen.

   Als u een subcategorie wilt toevoegen, selecteert u de optie **Category of protected resources**.

9. Selecteer het type bron dat u wilt toevoegen: **File or folder** of **Registry key**.

10. Selecteer een bestand, map of registersleutel.

11. Verlaat de wizard verlaten.

    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 **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 **Toevoegen**. 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 inschakelen** 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).

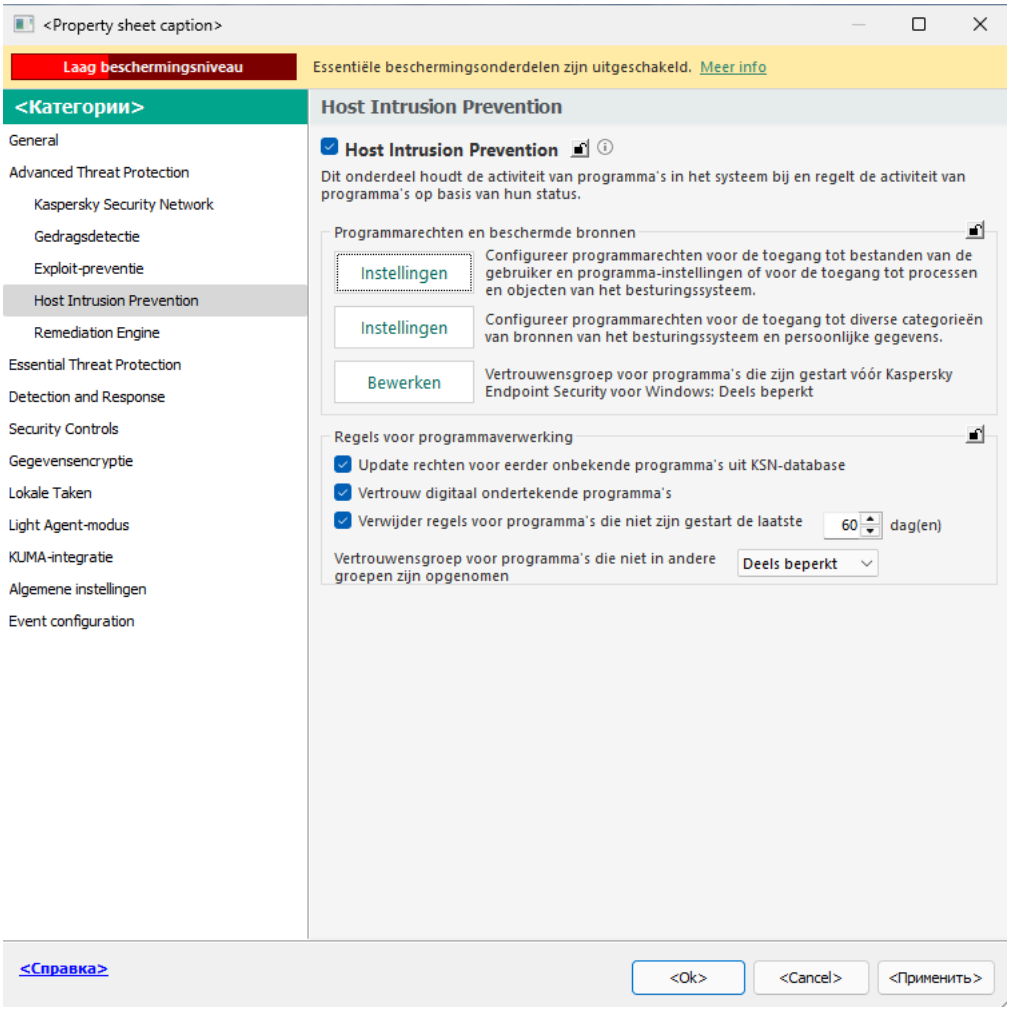
Wanneer u een programma start waarvan de informatie is verwijderd, analyseert Kaspersky Endpoint Security het programma alsof het voor de eerste keer wordt gestart.

Automatische verwijdering van informatie over ongebruikte programma's configureren in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.

2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

3. Selecteer **Advanced Threat Protection** → **Host Intrusion Prevention** in het beleidsvenster.



Instellingen van Inbraakpreventie

4. Doe in het blok **Regels voor programmaverwerking** een van het volgende:

   - Als u automatische verwijdering wilt configureren, schakel dan het selectievakje **Verwijder regels voor programma's die niet zijn gestart de laatste N dag(en)** in en voer 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 verwdering wilt uitschakelen, schakelt u het selectievakje **Verwijder regels voor programma's die niet zijn gestart de laatste N dag(en)** 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.

5. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Automatisch verwijderen van informatie over ongebruikte programma's configureren in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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 **Host Threat Protection** → **Host Intrusion Prevention**.

5. Doe in het blok **Application processing rules** een van het volgende:

   - Als u automatische verwijdering wilt configureren, schakel dan het selectievakje **Delete rules for applications that have not been started for longer than (days, 1 to 90)** in en voer 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, schakel het selectievakje **Delete rules for applications that have not been started for longer than (days, 1 to 90)** 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 automatische verwijdering wilt configureren, schakel dan het selectievakje **Verwijder regels voor programma's die niet zijn gestart de laatste N dagen (van 1 tot 90)** in en voer 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 verwdering wilt uitschakelen, schakelt u het selectievakje **Verwijder regels voor programma's die niet zijn gestart de laatste N dagen (van 1 tot 90)** 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

De functies voor bescherming van audiosignalen en bescherming van webcamtoegang worden niet ondersteund op Arm-computers.

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.

Kaspersky Endpoint Security staat standaard alleen de ontvangst van audio- en videostreams toe voor programmas uit de groep *Vertrouwd*. De programma's van *Deels beperkt*, *Zeer beperkt* en *Niet vertrouwd* groepen mogen 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.

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 een 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.

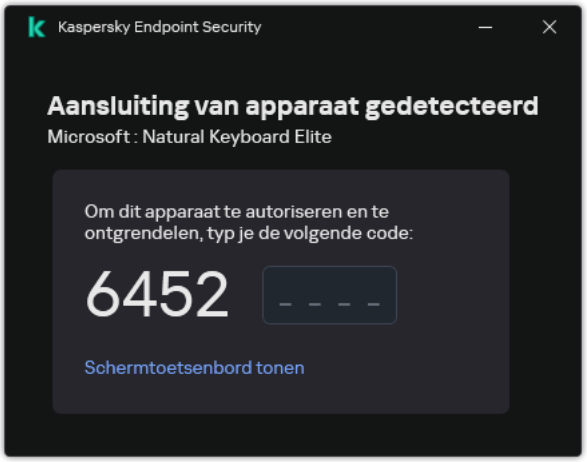
Als de code juist is ingevoerd, slaat het programma de identificatieparameters op (VID/PID van het toetsenbord en het nummer van de poort waarop het is aangesloten) in de lijst met geautoriseerde toetsenborden. U hoeft de toetsenbordautorisatie niet te herhalen wanneer het toetsenbord opnieuw wordt aangesloten of wanneer het besturingssysteem opnieuw wordt opgestart.

Wanneer het geautoriseerde toetsenbord op een andere USB-poort van de computer wordt aangesloten, wordt 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

BadUSB Attack Prevention inschakelen en uitschakelen

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.

Het onderdeel BadUSB Attack Prevention in- of uitschakelen in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Essential Threat Protection** → **BadUSB Attack Prevention** in het beleidsvenster.
4. Gebruik het selectievakje **BadUSB Attack Prevention** om het onderdeel in of uit te schakelen.

5. Pas in het blok **Autorisatie van USB-apparaat 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 vijf pogingen voor de invoer van de autorisatiecode toestaat, blokkeert het programma het USB-apparaat na de vijfde mislukte poging. Kaspersky Endpoint Security toont hoelang het USB-apparaat geblokkeerd is. Na deze tijd krijgt u opnieuw vijf pogingen om de autorisatiecode in te voeren.

   - **Time-out als max. aantal pogingen is bereikt (in minuten)**. 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).

6. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Het onderdeel BadUSB Attack Prevention in- of uitschakelen in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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 **Host Threat Protection** → **BadUSB Attack Prevention**.

5. Gebruik de schakelaar **BadUSB Attack Prevention ENABLED** om de component in of uit te schakelen.

6. Pas in het blok **Authorization of USB devices** de beveiligingsinstellingen voor de invoer van de autorisatiecode aan:

   - **Maximum number of USB device authorization attempts**. 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 vijf pogingen voor de invoer van de autorisatiecode toestaat, blokkeert het programma het USB-apparaat na de vijfde mislukte poging. Kaspersky Endpoint Security toont hoelang het USB-apparaat geblokkeerd is. Na deze tijd krijgt u opnieuw vijf pogingen om de autorisatiecode in te voeren.

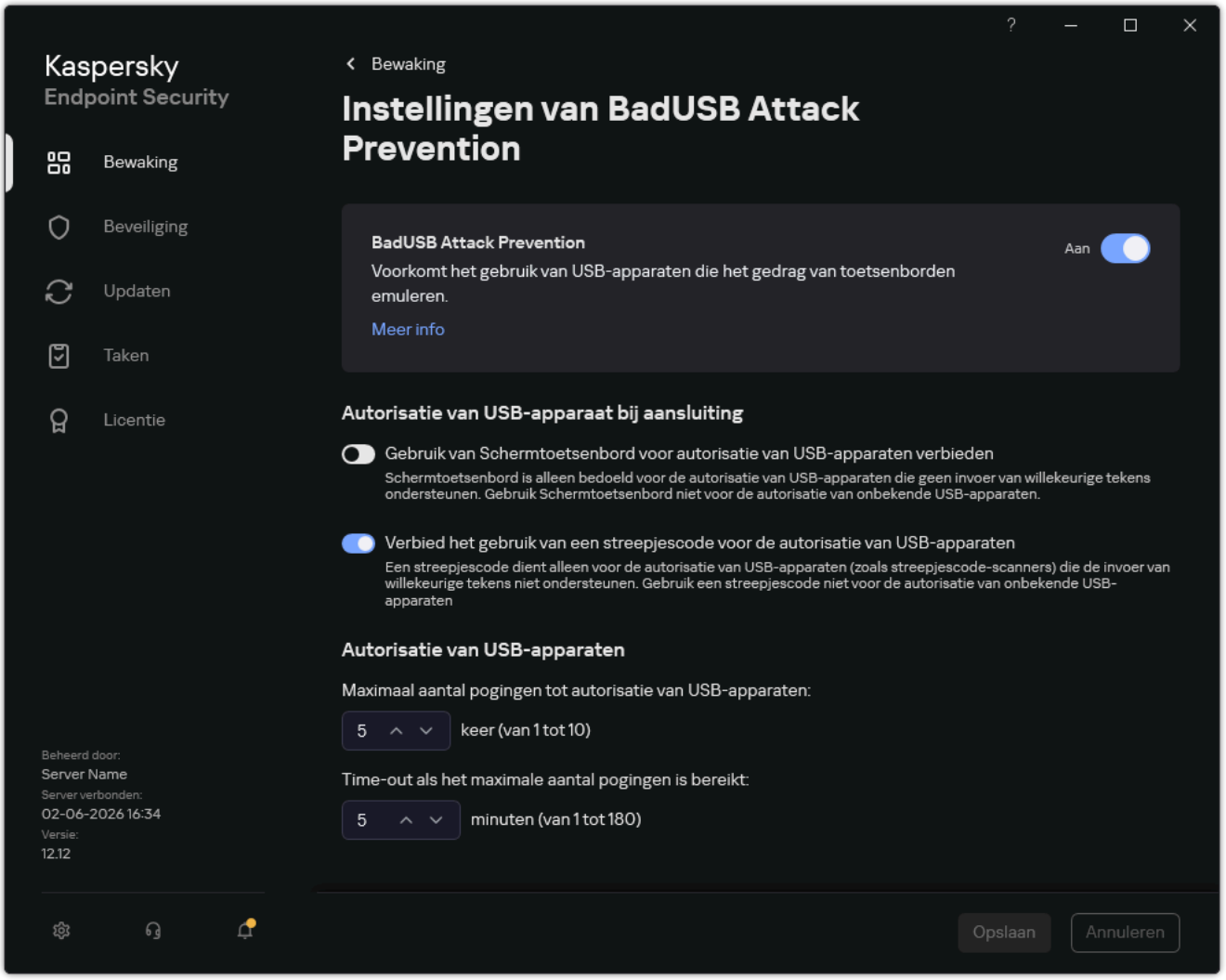
   - **Timeout when reaching the maximum number of attempts (min)**. Duur van de blokkering van het USB-apparaat na het opgegeven aantal mislukte pogingen om de autorisatiecode in te voeren. Geldige waarden zijn 1 tot en met 180 (minuten).

7. Sla uw wijzigingen op.

Het onderdeel BadUSB Attack Prevention in de programma-interface in- of uitschakelen

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.



Instellingen van het onderdeel BadUSB Attack Prevention

3. Gebruik de schakelaar **BadUSB Attack Prevention** om de component in of uit te schakelen.

4. Pas in het blok **Autorisatie van USB-apparaat 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 vijf pogingen voor de invoer van de autorisatiecode toestaat, blokkeert het programma het USB-apparaat na de vijfde mislukte poging. Kaspersky Endpoint Security toont hoelang het USB-apparaat geblokkeerd is. Na deze tijd krijgt u opnieuw vijf pogingen om de autorisatiecode in te voeren.

   - **Time-out als het maximale aantal pogingen is bereikt**. 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.

Schermtoetsenbord gebruiken voor autorisatie van USB-apparaten

Schermtoetsenbord mag alleen worden gebruikt voor de autorisatie van USB-apparaten die de invoer van willekeurige tekens niet ondersteunen (bijvoorbeeld barcodescanners). U wordt afgeraden om Schermtoetsenbord te gebruiken voor de autorisatie van onbekende USB-apparaten.

Het gebruik van Schermtoetsenbord voor autorisatie in de Beheerdersconsole (MMC) toestaan of verbieden

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Essential Threat Protection** → **BadUSB Attack Prevention** in het beleidsvenster.
4. Gebruik het selectievakje **Gebruik van Schermtoetsenbord voor autorisatie van USB-apparaten verbieden** als u het gebruik van Schermtoetsenbord voor autorisaties wilt blokkeren of toestaan.
5. Sla uw wijzigingen op.

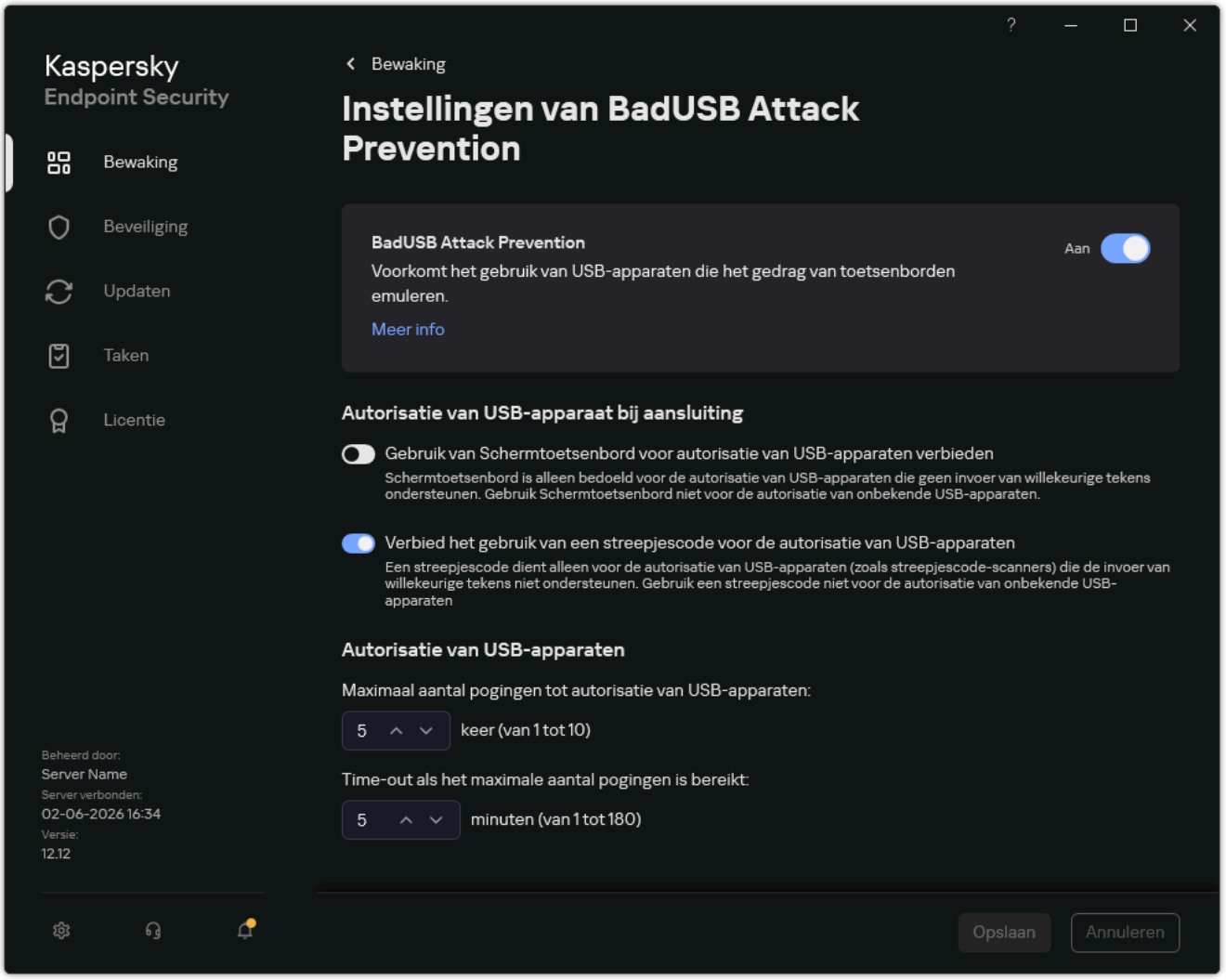
Het gebruik van Schermtoetsenbord voor autorisatie toestaan of verbieden in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Host Threat Protection** → **BadUSB Attack Prevention**.
5. Gebruik de schakelaar **Prohibit use of On-Screen Keyboard for authorization of USB devices** als u het gebruik van Schermtoetsenbord voor autorisaties wilt blokkeren of toestaan.
6. Sla uw wijzigingen op.

het gebruik van het schermtoetsenbord voor autorisatie in het programma-interface toestaan of verbieden

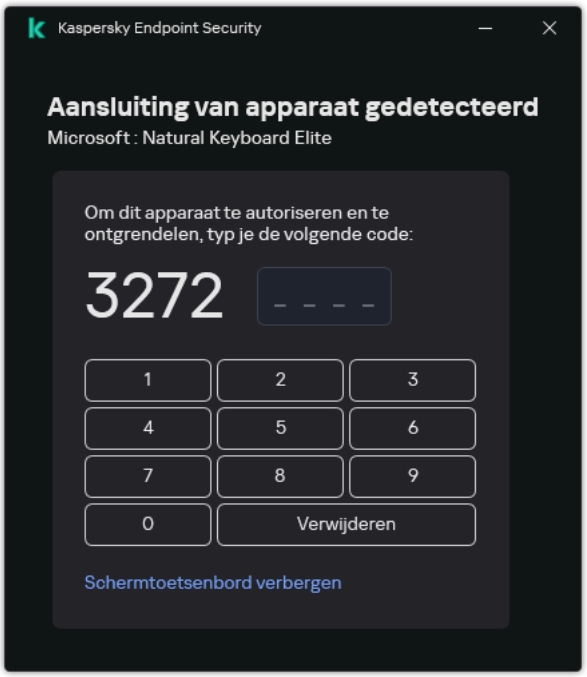
1. Klik in het hoofdvenster van het programma op de knop ⚙.
2. Selecteer **Essential Threat Protection** → **BadUSB Attack Prevention** in het venster met de programma-instellingen.



Instellingen van het onderdeel BadUSB Attack Prevention

3. Gebruik de schakelaar **Gebruik van Schermtoetsenbord voor autorisatie van USB-apparaten verbieden** als u het gebruik van Schermtoetsenbord voor autorisaties wilt blokkeren of toestaan.

4. Sla uw wijzigingen op.



Autorisatie van USB-apparaten

Autorisatie van barcodescanner

Wanneer u een barcodescanner aansluit op de computer, identificeert het onderdeel BadUSB Attack Prevention dit apparaat als een invoerapparaat en wordt u gevraagd om de autorisatie uit te voeren. Om de barcodescanner te autoriseren, moet u een streepjescode scannen die op het scherm wordt weergegeven. Het programma genereert een streepjescode in het formaal Code39 dat door de meeste scanners voor streepjescodes en QR-codes wordt ondersteund.

Kaspersky Endpoint Security ondersteunt ook een andere autorisatiemethode voor streepjescodes. Als u apparaten met een touchscreen gebruikt, kunt u een schermtoetsenbord gebruiken om een code te typen. Hiervoor moet je: het schermtoetsenbord toestaan. Deze methode is bijvoorbeeld handig bij stationaire barcodescanners die in kassa's zijn ingebouwd. Andere autorisatiemethoden voor barcodescanners zijn verboden.

Het programma gebruikt standaard geen streepjescode voor de autorisatie van USB-apparaten.

USB-apparaatautorisatie via streepjescode inschakelen in de beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.

2. Selecteer in de beheerconsole **Policies**.

3. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

4. Selecteer **Essential Threat Protection** → **BadUSB Attack Prevention** in het beleidsvenster.

5. Gebruik het selectievakje **Gebruik van een streepjescode voor autorisatie van USB-apparaten verbieden** als u het gebruik van streepjescodes voor autorisaties wilt blokkeren of toestaan.

6. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

USB-apparaatautorisatie via streepjescode inschakelen in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de Webconsole het tabblad **Asset management** → **Policies**.

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 **Host Threat Protection** → **BadUSB Attack Prevention**.

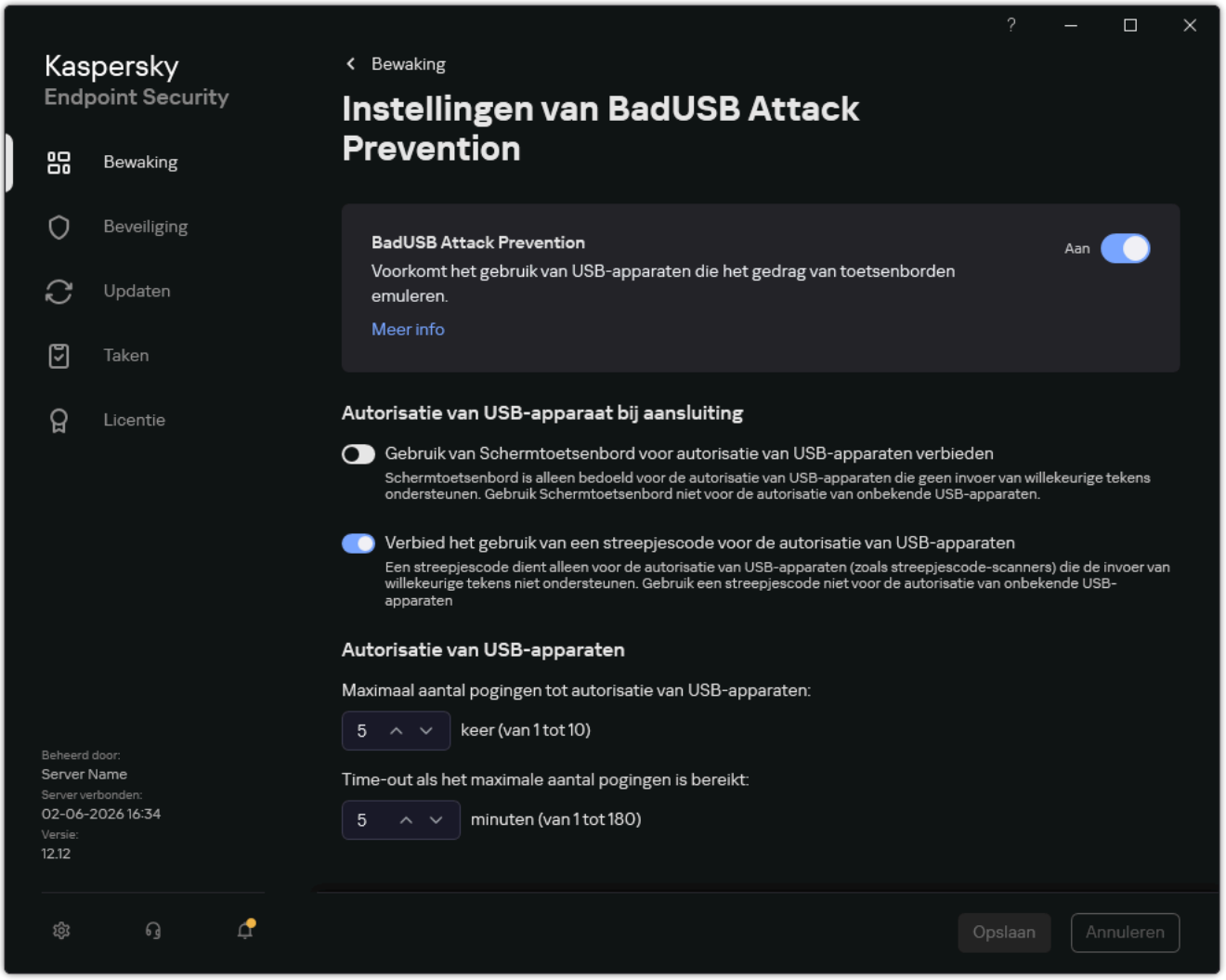
5. Gebruik de schakelaar **Prohibit use of a barcode for authorization of USB devices** als u het gebruik van streepjescodes voor autorisaties wilt blokkeren of toestaan.

6. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Autorisatie van USB-apparaten met streepjescode inschakelen in de programma-interface

1. Klik in het hoofdvenster van het programma op de knop ⚙.

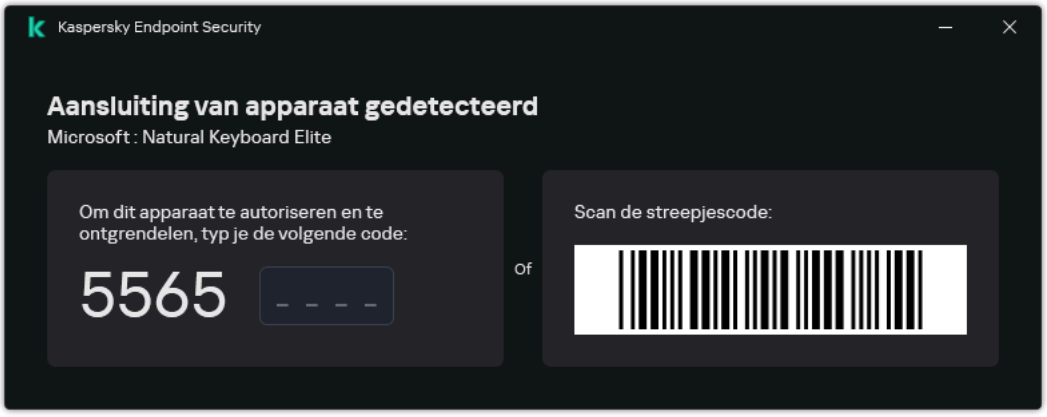
2. Selecteer **Essential Threat Protection** → **BadUSB Attack Prevention** in het venster met de programma-instellingen.



Instellingen van het onderdeel BadUSB Attack Prevention

3. Gebruik de schakelaar **Verbied het gebruik van een streepjescode voor de autorisatie van USB-apparaten** als u het gebruik van streepjescodes voor autorisaties wilt blokkeren of toestaan.

4. Sla uw wijzigingen op.

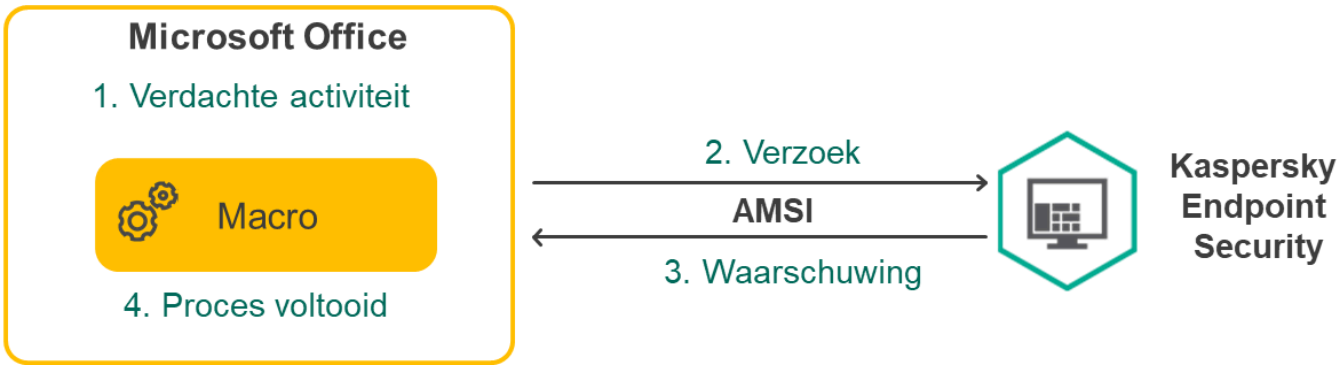


Autorisatie van barcodescanner

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. Een programma van een derde partij staat, na ontvangst van een melding van een dreiging, de kwaadaardige acties niet toe (bijvoorbeeld door de actie te beëindigen).



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 verstuurt 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 / Enterprise multi-sessie
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise
- Windows Server 2016 Essentials / Standard / Datacenter (including Server Core mode)
- Windows Server 2019 Essentials / Standard / Datacenter (including Server Core mode)
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (including Server Core mode)
- Windows Server 2025 Standard / Datacenter

AMSI-bescherming inschakelen en uitschakelen

AMSI-bescherming is standaard ingeschakeld en werkt in de modus die wordt aanbevolen door Kaspersky (zie de onderstaande tabel).

AMSI-bescherming inschakelen of uitschakelen in de Beheerconsole (MMC)

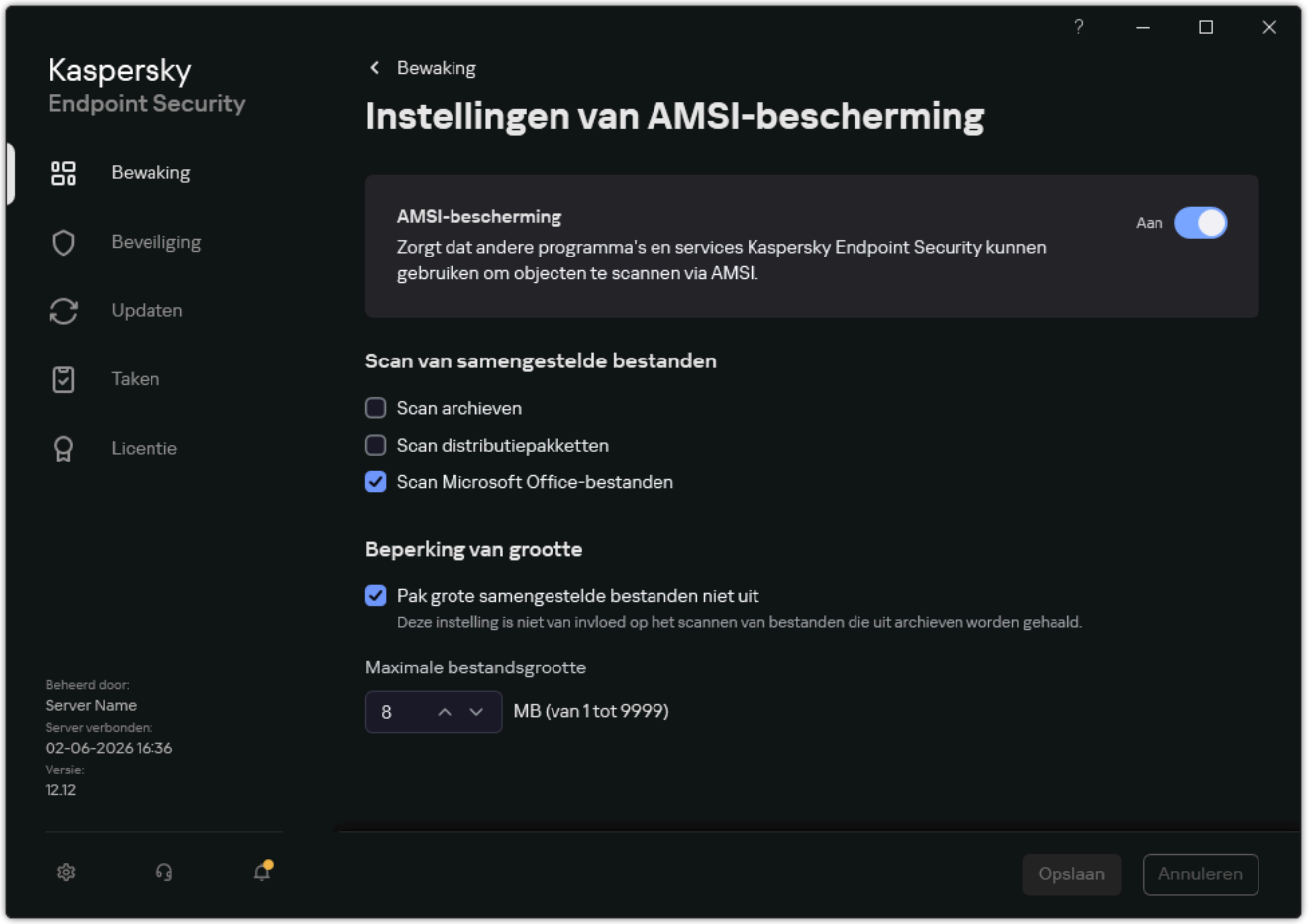
1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Essential Threat Protection** → **AMSI-scanner** in het beleidsvenster.
4. Gebruik het selectievakje **AMSI-scanner** om het onderdeel in of uit te schakelen.
5. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

AMSI-bescherming in- of uitschakelen in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Host Threat Protection** → **AMSI Protection**.
5. Gebruik de schakelaar **AMSI Protection ENABLED** om de component in of uit te schakelen.
6. Sla uw wijzigingen op. Om het beleid op computers toe te passen, sluit de hangsloten.

AMSI-bescherming in- of uitschakelen in de programma-interface

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.



Instellingen van AMSI-bescherming

3. Gebruik de schakelaar **AMSI-bescherming** om de component in of uit te schakelen.
4. Sla uw wijzigingen op.

AMSI Protection-instellingen aanbevolen door Kaspersky-experts

Parameter	Waarde	Beschrijving
Scan archieven	**Uit**	ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE en andere bestanden scannen. Het programma 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 (een archief in een archief).
Scan distributiepakketten	**Uit**	Distributiepakketten van programma's van derden scannen.
Scan Microsoft Office-bestanden	**Aan**	Scant Microsoft Office-bestanden (DOC, DOCX, XLS, PPT en andere Microsoft-extensies). Bestanden in Office-indeling bevatten ook OLE-objecten. Het programma scant office-bestanden die kleiner zijn dan 1 MB, ongeacht of het selectievakje is ingeschakeld of niet.
Pak grote samengestelde bestanden niet uit	**Maximale bestandsgrootte 8 MB**	Als dit selectievakje is ingeschakeld, scant het programma geen samengestelde bestanden als ze groter zijn dan de opgegeven waarde. Als dit selectievakje is uitgeschakeld, worden samengestelde bestanden van alle grootten gescand door het programma. Het programma scant grote bestanden die uit archieven worden gehaald, ongeacht of het selectievakje is ingeschakeld of niet.

Scannen van bestanden optimaliseren door AMSI Protection

U kunt het scannen van bestanden optimaliseren: kort de duur van scans in en laat Kaspersky Endpoint Security sneller werken. U kunt de samengestelde bestanden selecteren die moeten worden gescand: archieven, distributiepakketten of bestanden in Office-indeling. U kunt ook de grootte van samengestelde bestanden die moeten worden gescand, beperken. Het AMSI-beschermingsonderdeel pakt geen samengestelde bestanden uit die groter zijn dan de opgegeven grootte.

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.

Optimaliseer het scannen van bestanden door AMSI-bescherming in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Essential Threat Protection** → **AMSI-scanner** in het beleidsvenster.
4. Geef in het blok **Scan van samengestelde bestanden** op welke soorten samengestelde bestanden u wilt scannen: archieven, distributiepakketten of Office-bestanden.
5. Doe in het blok **Maximale grootte** een van het volgende:
   - Om het AMSI-beschermingsonderdeel geen grote samengestelde bestanden te laten uitpakken, schakel het selectievakje **Grote samengestelde bestanden niet uitpakken** in en voer de vereiste waarde in het veld 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 **Grote samengestelde bestanden niet uitpakken**.

   Het AMSI-beschermingsonderdeel scant grote bestanden die uit archieven zijn uitgepakt, ongeacht of het selectievakje **Grote samengestelde bestanden niet uitpakken** is ingeschakeld.
6. Sla uw wijzigingen op. Om het beleid op computers toe te passen, sluit de hangsloten .

Optimaliseer het scannen van bestanden door AMSI-bescherming in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Host Threat Protection** → **AMSI Protection**.

5. Geef in het blok **Scan of compound files** op welke soorten samengestelde bestanden u wilt scannen: archieven, distributiepakketten of Office-bestanden.

6. Doe in het blok **Scan optimization** een van het volgende:

   - Om het AMSI-beschermingsonderdeel geen grote samengestelde bestanden te laten uitpakken, schakel het selectievakje **Size limits enabled** in en voer de vereiste waarde in het veld 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 **Size limits enabled**.

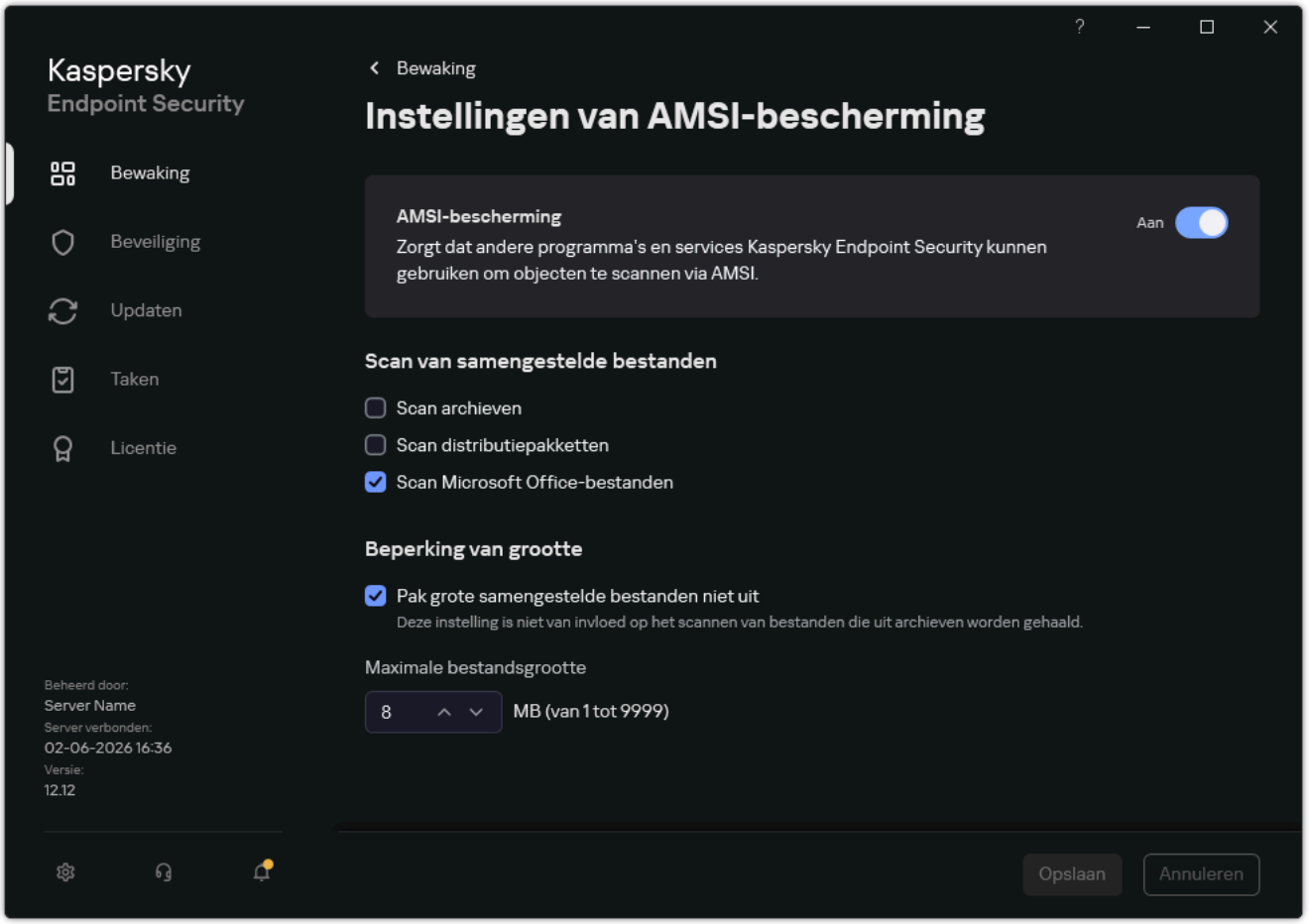
   Het AMSI-beschermingsonderdeel scant grote bestanden die uit archieven zijn uitgepakt, ongeacht of het selectievakje **Size limits enabled** is ingeschakeld.

7. Sla uw wijzigingen op. Om het beleid op computers toe te passen, sluit de hangsloten .

Optimaliseer het scannen van bestanden door AMSI-bescherming in de programma-interface

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.



Instellingen van AMSI-bescherming

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, schakel het selectievakje **Pak grote samengestelde bestanden niet uit** in en voer de vereiste waarde in het veld 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**.

   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.

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.

Om Web Threat Protection te kunnen gebruiken, moet u de initiële configuratie van het programma voltooien:

- Voor de bewaking van HTTPS-verkeer, schakel het scannen van versleutelde verbindingen in (standaard ingeschakeld).
- Selecteer de poorten die: Kaspersky Endpoint Security moet monitoren (standaard bewaakt het programma alle poorten).
- Selecteer het programma waarvan u wilt dat Kaspersky Endpoint Security het verkeer bewaakt. De meeste browsers staan al in de lijst met door Kaspersky aanbevolen programma's. Als uw browser niet in de lijst staat, kunt u deze handmatig toevoegen.
- Wij adviseren om een script voor webpagina-interactie in het webverkeer te injecteren (scriptinjectie is standaard uitgeschakeld). Met dit script kunnen Web Threat Protection-gebeurtenissen voor het programmagebeurtenislogboek, het OS-gebeurtenislogboek en rapporten worden geregistreerd.

Wanneer een gebruiker een schadelijke website of phishingwebsite probeert te openen, blokkeert Kaspersky Endpoint Security de toegang en wordt er een waarschuwing weergegeven.

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 het programma 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.

U 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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Essential Threat Protection** → **Web Threat Protection** in het beleidsvenster.
4. Gebruik het selectievakje **Web Threat Protection** om het onderdeel in of uit te schakelen.
5. 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 waarop het onderdeel Web Threat Protection het webverkeer dat een computer via HTTP en FTP ontvangt, maximaal scant. 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 het programma 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 oppervlakkige 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 beveiligingsniveaus herstellen door te klikken op de knop **Standaard**.

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:

   - **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.

Het onderdeel Web Threat Protection in- of uitschakelen in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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 **Communication & Web Protection** → **Web Threat Protection**.

5. Gebruik de schakelaar **Web Threat Protection ENABLED** om de component in of uit te schakelen.

6. Selecteer in het blok **Action on threat detection** de actie die Kaspersky Endpoint Security moet uitvoeren op schadelijke objecten uit het internetverkeer:

   - **Block**. 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.

   - **Allow, inform, or prompt for action (depends on OS)**. 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. Maak indien nodig een lijst met vertrouwde webadressen.

8. 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 waarop het onderdeel Web Threat Protection het webverkeer dat een computer via HTTP en FTP ontvangt, maximaal scant. 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 het programma 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 oppervlakkige 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 beveiligingsniveaus herstellen door te klikken op de knop **Aanbevolen beveiligingsniveau herstellen**.

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:

   - **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
Controleer of het webadres voorkomt in de database met schadelijke webadressen	**Aan**	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.
Controleer of het webadres voorkomt in de database met phishingadressen	**Aan**	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.

Parameter	Waarde	Beschrijving
Gebruik heuristische analyse (Web Threat Protection)	**Gemiddelde scan**	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. 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.
Gebruik heuristische analyse (anti-phishing)	**Aan**	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.
Actie bij detectie van een dreiging	**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.

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 Security scant alle links 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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Essential Threat Protection** → **Web Threat Protection** in het beleidsvenster.
4. In het blok **Beveiligingsniveau**, klikt u op de knop **Instellingen**.
5. 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.
6. 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 in het blok **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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Essential Threat Protection** → **Web Threat Protection** in het beleidsvenster.

4. In het blok **Beveiligingsniveau**, klikt u op de knop **Instellingen**.

5. Selecteer in het geopende venster 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.

6. 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.

7. 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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Essential Threat Protection** → **Web Threat Protection** in het beleidsvenster.
4. In het blok **Beveiligingsniveau**, klikt u op de knop **Instellingen**.
5. In het venster dat opent, in het blok **Instellingen van Anti-Phishing** selecteer of verwijder de selectie van het selectievakje **Controleer of het webadres voorkomt in de database met phishingadressen** om anti-phishing in te schakelen 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.
6. 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.
7. 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 de databases met phishing-webadressen, schakelt u het selectievakje **Controleer of het webadres voorkomt in de database met phishingadressen** 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.

Het wijzigen van de lijst met vertrouwde webadressen in een beleid wordt mogelijk geblokkeerd door de eigenschappen van het bovenliggende beleid. Om de lijst te wijzigen, moet u toestaan dat de instellingen van vertrouwde zone in de Webconsole (het "hangslot" moet ontgrendeld zijn).

Vertrouwde zones zijn verschillend gegroepeerd in de Beheerconsole (MMC) en de Webconsole. Ook de manier waarop wijziging in de parameters voor de vertrouwde zone worden voorkomen, verschilt (verschillende "hangsloten"). We raden aan dat u alleen de Webconsole gebruikt om het programma te beheren. Als u de vertrouwde zone in verschillende consoles configureert, kan de beheerplug-in het "hangslot" terugzetten naar de standaardstatus.

Een vertrouwd webadres toevoegen in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Essential Threat Protection** → **Web Threat Protection** in het beleidsvenster.
4. In het blok **Beveiligingsniveau**, klikt u op de knop **Instellingen**.
5. Selecteer in het geopende venster het tabblad **Vertrouwde webadressen**.
6. Selecteer het selectievakje **Scan geen internetverkeer van vertrouwde webadressen**.

   Als deze optie 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.

7. 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.

8. Sla uw wijzigingen op.

Een vertrouwd webadres toevoegen in de Webconsole en de Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Communication & Web Protection** → **Web Threat Protection**.
5. Klik op **Trusted web addresses**.
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 JSON-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 deze optie 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 onderdelen Web Threat Protection, Mail Threat Protection en 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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Essential Threat Protection** → **Web Threat Protection** in het beleidsvenster.
4. In het blok **Beveiligingsniveau**, klikt u op de knop **Instellingen**.
5. Selecteer in het geopende venster het tabblad **Vertrouwde webadressen**.
6. 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 koppeling **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.
7. De lijst met vertrouwde webadressen importeren:
    a. Klik op de koppeling **Importeren**.

       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 u er nieuwe items aan wilt toevoegen vanuit het XML-bestand.
8. Sla uw wijzigingen op.

Een lijst met vertrouwde webadressen exporteren en importeren in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Communication & Web Protection** → **Web Threat Protection**.
5. De lijst met uitzonderingen in het blok **Rules list** exporteren:

   a. Selecteer de vertrouwde webadressen die u wilt exporteren.

   b. Klik op de knop → **Export**.

   Kaspersky Endpoint Security exporteert de lijst met vertrouwde webadressen naar een JSON-bestand in de standaard downloadmap.
6. De lijst met uitzonderingen in het blok **Rules list** importeren:

   a. Klik op de knop → **Import**.

   Selecteer in het geopende venster het JSON-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 u er nieuwe items aan wilt toevoegen vanuit het JSON-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
- Windows Mail

- MyOffice Mail
- R7-Office Organizer

Om verkeer in Mozilla Thunderbird, MyOffice Mail en R7-Office Organizer e-mailprogramma's te scannen, moet u het Kaspersky-certificaat toevoegen aan het certificaatarchief en het eigen certificaatarchief selecteren.

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 Mail Threat Protection-extensie ondersteunt de 32-bit en 64-bit versies van Outlook 2010, 2013, 2016, 2019, 2021, 2024 en 365. Op Arm-computers ondersteunt de Mail Threat Protection-extensie de 32-bit en 64-bit versies van Outlook 2016, Outlook 2021, Outlook 2024 en Outlook 365 voor Arm64.

Het onderdeel Mail Threat Protection scant geen berichten als de e-mailclient in een browser is geopend.

Wanneer een schadelijk bestand wordt gedetecteerd in een bijlage, voegt Kaspersky Endpoint Security informatie over de uitgevoerde actie toe aan het onderwerp van het bericht, bijvoorbeeld *[Bericht is verwerkt] <onderwerp van 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 kan het programma verschillende groepen instellingen toepassen. 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.

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.

Het onderdeel Mail Threat Protection in- of uitschakelen in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Essential Threat Protection** → **Mail Threat Protection** in het beleidsvenster.
4. Gebruik het selectievakje **Mail Threat Protection** om het onderdeel in of uit te schakelen.

5. 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 het programma 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 **Instellingen** en definieert u uw eigen onderdeelinstellingen.

     U kunt de waarden van vooraf ingestelde beveiligingsniveaus herstellen door te klikken op de knop **Standaard**.

6. Selecteer in het blok **Actie bij detectie van een dreiging** de actie die Kaspersky Endpoint Security moet uitvoeren op schadelijke objecten:

   - **Desinfecteren of verwijderen als desinfectie mislukt**. Wanneer een geïnfecteerd object wordt gedetecteerd in een inkomend of uitgaand bericht, probeert het programma 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 het programma het geïnfecteerde object. Het programma voegt informatie over de uitgevoerde actie toe aan het onderwerp van het bericht, bijvoorbeeld *[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 het programma een waarschuwing toe aan het onderwerp van het bericht. De gebruiker krijgt dan toegang tot het bericht met de originele bijlage. Wanneer een geïnfecteerd object wordt gedetecteerd in een inkomend bericht, probeert Kaspersky Endpoint Security het gedetecteerde object te desinfecteren. Als het object niet kan worden gedesinfecteerd, blokkeert het programma de verzending van het bericht en toont het e-mailprogramma een fout.

   - **Blokkeren**. Als een geïnfecteerd object wordt gedetecteerd in een inkomend bericht, voegt het programma een waarschuwing toe aan het onderwerp van het bericht. De gebruiker krijgt dan toegang tot het bericht met de originele bijlage. Als een geïnfecteerd object wordt gedetecteerd in een uitgaand bericht, blokkeert het programma de verzending van het bericht en toont het e-mailprogramma een fout.

7. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Het onderdeel Mail Threat Protection in- of uitschakelen in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Communication & Web Protection** → **Mail Threat Protection**.
5. Gebruik de schakelaar **Mail Threat Protection ENABLED** om de component in of uit te schakelen.
6. Selecteer in het blok **Action on threat detection** de actie die Kaspersky Endpoint Security moet uitvoeren op schadelijke objecten:

   - **Disinfect, delete if disinfection fails**. Wanneer een geïnfecteerd object wordt gedetecteerd in een inkomend of uitgaand bericht, probeert het programma 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 het programma het geïnfecteerde object. Het programma voegt informatie over de uitgevoerde actie toe aan het onderwerp van het bericht, bijvoorbeeld *[Bericht is verwerkt] <onderwerp van bericht>*.

   - **Disinfect, block if disinfection fails**. 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 het programma een waarschuwing toe aan het onderwerp van het bericht. De gebruiker krijgt dan toegang tot het bericht met de originele bijlage. Wanneer een geïnfecteerd object wordt gedetecteerd in een inkomend bericht, probeert Kaspersky Endpoint Security het gedetecteerde object te desinfecteren. Als het object niet kan worden gedesinfecteerd, blokkeert het programma de verzending van het bericht en toont het e-mailprogramma een fout.

   - **Block**. Als een geïnfecteerd object wordt gedetecteerd in een inkomend bericht, voegt het programma een waarschuwing toe aan het onderwerp van het bericht. De gebruiker krijgt dan toegang tot het bericht met de originele bijlage. Als een geïnfecteerd object wordt gedetecteerd in een uitgaand bericht, blokkeert het programma de verzending van het bericht en toont het e-mailprogramma een fout.
7. Bewerk in dien nodig de geavanceerde instellingen van Mail Threat Protection.
8. Sla uw wijzigingen op.

Het onderdeel Mail Threat Protection in de programma-interface in- of uitschakelen

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 het programma 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 beveiligingsniveaus herstellen door te klikken op de knop **Aanbevolen beveiligingsniveau herstellen**.

5. Selecteer in het blok **Actie bij detectie van een dreiging** de actie die Kaspersky Endpoint Security moet uitvoeren op schadelijke objecten:

   - **Desinfecteren of verwijderen als desinfectie mislukt**. Wanneer een geïnfecteerd object wordt gedetecteerd in een inkomend of uitgaand bericht, probeert het programma 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 het programma het geïnfecteerde object. Het programma voegt informatie over de uitgevoerde actie toe aan het onderwerp van het bericht, bijvoorbeeld *[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 het programma een waarschuwing toe aan het onderwerp van het bericht. De gebruiker krijgt dan toegang tot het bericht met de originele bijlage. Wanneer een geïnfecteerd object wordt gedetecteerd in een inkomend bericht, probeert Kaspersky Endpoint Security het gedetecteerde object te desinfecteren. Als het object niet kan worden gedesinfecteerd, blokkeert het programma de verzending van het bericht en toont het e-mailprogramma een fout.

   - **Blokkeren**. Als een geïnfecteerd object wordt gedetecteerd in een inkomend bericht, voegt het programma een waarschuwing toe aan het onderwerp van het bericht. De gebruiker krijgt dan toegang tot het bericht met de originele bijlage. Als een geïnfecteerd object wordt gedetecteerd in een uitgaand bericht, blokkeert het programma de verzending van het bericht en toont het e-mailprogramma een fout.

6. Sla uw wijzigingen op.

Instellingen voor Mail Threat Protection aanbevolen door Kaspersky-experts (aanbevolen beveiligingsniveau)

Parameter	Waarde	Beschrijving
Beschermd bereik	**Inkomende en uitgaande berichten**	Het *Beschermd bereik* omvat objecten die door het onderdeel worden gecontroleerd wanneer het wordt uitgevoerd: inkomende en uitgaande berichten of 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.
Verbind Microsoft Outlook-extensie	**Aan**	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. Als e-mail wordt gescand met de extensie voor Microsoft Outlook, wordt u aanbevolen de Cached Exchange Mode te gebruiken. Voor meer gedetailleerde informatie over de Exchange-modus met cache en aanbevelingen voor het gebruik ervan, raadpleegt u de Microsoft Knowledge Base.
Scan toegevoegde archieven	**Aan**	ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE en andere bestanden scannen. Het programma 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 (een archief in een archief).
Scan Microsoft Office-bijlagen	**Aan**	Scant Microsoft Office-bestanden (DOC, DOCX, XLS, PPT en andere Microsoft-extensies). Bestanden in Office-indeling bevatten ook OLE-objecten. Het programma scant office-bestanden die kleiner zijn dan 1 MB, ongeacht of het selectievakje is ingeschakeld of niet.
Filter voor bijlagen	**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 onderstrepingsteken (bijvoorbeeld bijlage.doc_). Dus om het bestand te openen, moet de gebruiker het bestand hernoemen.
Heuristische analyse	**Gemiddelde scan**	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.
Actie bij detectie van een dreiging	**Desinfecteren of verwijderen als desinfectie mislukt**	Wanneer een geïnfecteerd object wordt gedetecteerd in een inkomend of uitgaand bericht, probeert het programma 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 het programma het geïnfecteerde object. Het programma voegt informatie over de uitgevoerde actie toe aan het onderwerp van het bericht, bijvoorbeeld *[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 het programma 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 het programma het geïnfecteerde object. Het programma voegt informatie over de uitgevoerde actie toe aan het onderwerp van het bericht, bijvoorbeeld *[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 het programma een waarschuwing toe aan het onderwerp van het bericht. De gebruiker krijgt dan toegang tot het bericht met de originele bijlage. Wanneer een geïnfecteerd object wordt gedetecteerd in een inkomend bericht, probeert Kaspersky Endpoint Security het gedetecteerde object te desinfecteren. Als het object niet kan worden gedesinfecteerd, blokkeert het programma de verzending van het bericht en toont het e-mailprogramma een fout.

   - **Blokkeren**. Als een geïnfecteerd object wordt gedetecteerd in een inkomend bericht, voegt het programma een waarschuwing toe aan het onderwerp van het bericht. De gebruiker krijgt dan toegang tot het bericht met de originele bijlage. Als een geïnfecteerd object wordt gedetecteerd in een uitgaand bericht, blokkeert het programma 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 vab 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 **Essential Threat Protection** → **Mail Threat Protection** in het venster met de programma-instellingen.
3. Klik op **Geavanceerde instellingen**.
4. Configureer in het blok **Scan van samengestelde bestanden** de scaninstellingen:
   - **Scan Microsoft Office-bijlagen**. Scant Microsoft Office-bestanden (DOC, DOCX, XLS, PPT en andere Microsoft-extensies). Bestanden in Office-indeling bevatten ook OLE-objecten. Het programma scant office-bestanden die kleiner zijn dan 1 MB, ongeacht of het selectievakje is ingeschakeld of niet.
   - **Scan toegevoegde archieven**. ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE en andere bestanden scannen. Het programma 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 (een archief in een archief).

     Als het programma tijdens de scan een wachtwoord voor een archief detecteert in de tekst van het bericht, wordt dit wachtwoord gebruikt om de inhoud van het archief te scannen op schadelijke programma's. In dit geval wordt het wachtwoord niet opgeslagen. Tijdens het scannen wordt een archief uitgepakt. Als er een programmafout optreedt tijdens het uitpakken, kunt u de uitgepakte bestanden die zijn opgeslagen op het volgende pad handmatig verwijderen: %systemroot%\temp. De bestanden hebben de PR-prefix.

   - **Scan geen archiefbestanden groter dan N MB (van 1 tot 9999)**. 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.
   - **Scan archieven niet langer dan N s (van 1 tot 9999)**. 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

Het bijlagenfilter 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 onderstrepingsteken (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. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Communication & Web 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 koppeling **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 u er nieuwe items aan wilt toevoegen vanuit het XML-bestand.

7. Sla uw wijzigingen op.

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.

2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

3. Selecteer **Essential Threat Protection** → **Mail Threat Protection** in het beleidsvenster.

4. In het blok **Beveiligingsniveau**, klikt u op de knop **Instellingen**.

5. Dit opent een venster; selecteer in dat venster het tabblad **Filter voor bijlagen**.

6. 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 koppeling **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.

7. De lijst met extensies importeren:

a. Klik op de koppeling **Importeren**.

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 u er nieuwe items aan wilt toevoegen vanuit het XML-bestand.

8. 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). Met de extensie kunnen berichten worden gescand op het niveau van een e-mailclient in plaats van op protocolniveau. Naast berichten kunt u met de extensie ook objecten scannen die via de MAPI-interface zijn ontvangen vanuit Microsoft Exchange-opslagplaatsen (bijvoorbeeld objecten in de kalender). Dit scannen vindt plaats in de e-mailprogramma's.

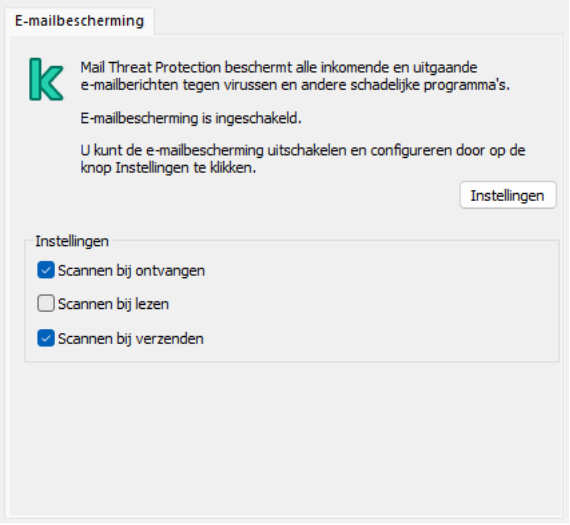
U kunt de instellingen van Mail Threat Protection vanuit Outlook openen en opgeven welke e-mailberichten moeten worden gescand op virussen en andere dreigingen.

De Mail Threat Protection-extensie ondersteunt de 32-bit en 64-bit versies van Outlook 2010, 2013, 2016, 2019, 2021, 2024 en 365.

Op Arm-computers ondersteunt de Mail Threat Protection-extensie de 32-bit en 64-bit versies van Outlook 2016, Outlook 2021, Outlook 2024 en Outlook 365 voor Arm64.

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 (zie de onderstaande afbeelding).



Instellingen van het onderdeel Mail Threat Protection in Outlook

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:

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Essential Threat Protection** → **Mail Threat Protection** in het beleidsvenster.
4. In het blok **Beveiligingsniveau**, klikt u op de knop **Instellingen**.
5. Klik in het venster dat opent in het blok **Connectiviteit** op de knop **Instellingen**.
6. 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.
7. Sla uw wijzigingen op.

E-mails scannen in Thunderbird, MyOffice, R7-Office

Het onderdeel Mail Threat Protection scant de bijlagen van inkomende en uitgaande e-mailberichten op virussen en andere dreigingen. Voor e-mailclients van Mozilla Thunderbird, MyOffice Mail en R7-Office Organizer krijgt het programma alleen toegang tot berichten op het *protocolniveau* (POP3, SMTP, IMAP, NNTP).

Om verkeer in Mozilla Thunderbird, MyOffice Mail en R7-Office Organizer e-mailprogramma's te scannen, moet u het Kaspersky-certificaat toevoegen aan het certificaatarchief en het eigen certificaatarchief selecteren.

Het onderdeel Mail Threat Protection scant geen berichten als de e-mailclient in een browser is geopend.

Realtime Mail Threat Protection

Mail Threat Protection kan zowel inkomende als uitgaande berichten scannen. 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. Wanneer een schadelijk bestand wordt gedetecteerd in een bijlage, voegt Kaspersky Endpoint Security informatie over de uitgevoerde actie toe aan het onderwerp van het bericht, bijvoorbeeld *[Bericht is verwerkt] <onderwerp van bericht>*.

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.

Malware-scan in e-maildatabases

De *Malware-scan* taak staat toe bestanden in e-mailindeling scannen. Als een kwaadaardig object wordt gedetecteerd in bestanden van deze e-mailclients, voegt Kaspersky Endpoint Security alleen informatie over gedetecteerde objecten toe aan de lijst met actieve dreigingen. Het programma desinfecteert of verwijdert geen geïnfecteerde bestanden in e-maildatabases, ongeacht de taakinstellingen.

Actieve dreigingen elimineren

Mail Threat Protection voorkomt de infectie van de computer op protocolniveau, maar als de computer was geïnfecteerd voordat Kaspersky Endpoint Security werd geïnstalleerd, detecteert het programma de dreiging mogelijk alleen in e-maildatabases. Mail Threat Protection bevat geen onderdelen die het specifiek mogelijk maken om een bericht in delen (koptekst, hoofdtekst, bijlagen) te splitsen, zoals Microsoft Office Outlook. Daarom kan het programma de gedetecteerde objecten niet verwijderen of desinfecteren. Kaspersky Endpoint Security voegt alleen informatie over gedetecteerde objecten toe aan het lijst met actieve dreigingen.

Zo verwijdert u actieve dreigingen:

1. Zoek en verwijder het bericht met het gedetecteerde object handmatig in de interface van de e-mailclient.

   Het programma geeft informatie weer over gedetecteerde object in de lijst met actieve dreigingen.

   Voorbeeld van een gedetecteerde objectkaart:

!	**HEUR:Trojan.PDF.Phish.gen** Object: `C:\Users\admin\AppData\Roaming\Thunderbird\Profiles\ov56jpz0.default-release\Mail\mail.company.ru\Inbox// [From USER NAME <company@mail.com>][Date 25 Sep 2025 20:05:36] [Subj Mail title X] Object.pdf`

2. Voer de bewerking voor het comprimeren van de database uit.

   Wanneer een bericht in de gebruikersinterface wordt verwijderd, voegt de e-mailclient alleen een verwijdermarkering toe. De e-mailclient verwijdert het bericht pas echt na het comprimeren van de database. Voor meer informatie over het comprimeren van databases raadpleeg de Help van uw e-mailclient (bijvoorbeeld Mozilla Thunderbird).

3. Start de *Malware-scan* taak opnieuw en zorg ervoor dat de dreiging niet langer aanwezig is.

Network Threat Protection

Het onderdeel *Network Threat Protection* (ook wel Intrusion Detection System (IDS) genoemd) controleert inkomend netwerkverkeer op activiteiten die kenmerkend zijn voor netwerkaanvallen. Wanneer het programma 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 het programma 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. Kaspersky Endpoint Security controleert inkomend netwerkverkeer op activiteiten die kenmerkend zijn voor netwerkaanvallen en blokkeert de aanvallen.

Hoe de escherming tegen Network Threat Protection in- of uit te schakelen in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Essential Threat Protection** → **Network Threat Protection** in het beleidsvenster.
4. Gebruik het selectievakje **Network Threat Protection** om het onderdeel in of uit te schakelen.
5. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

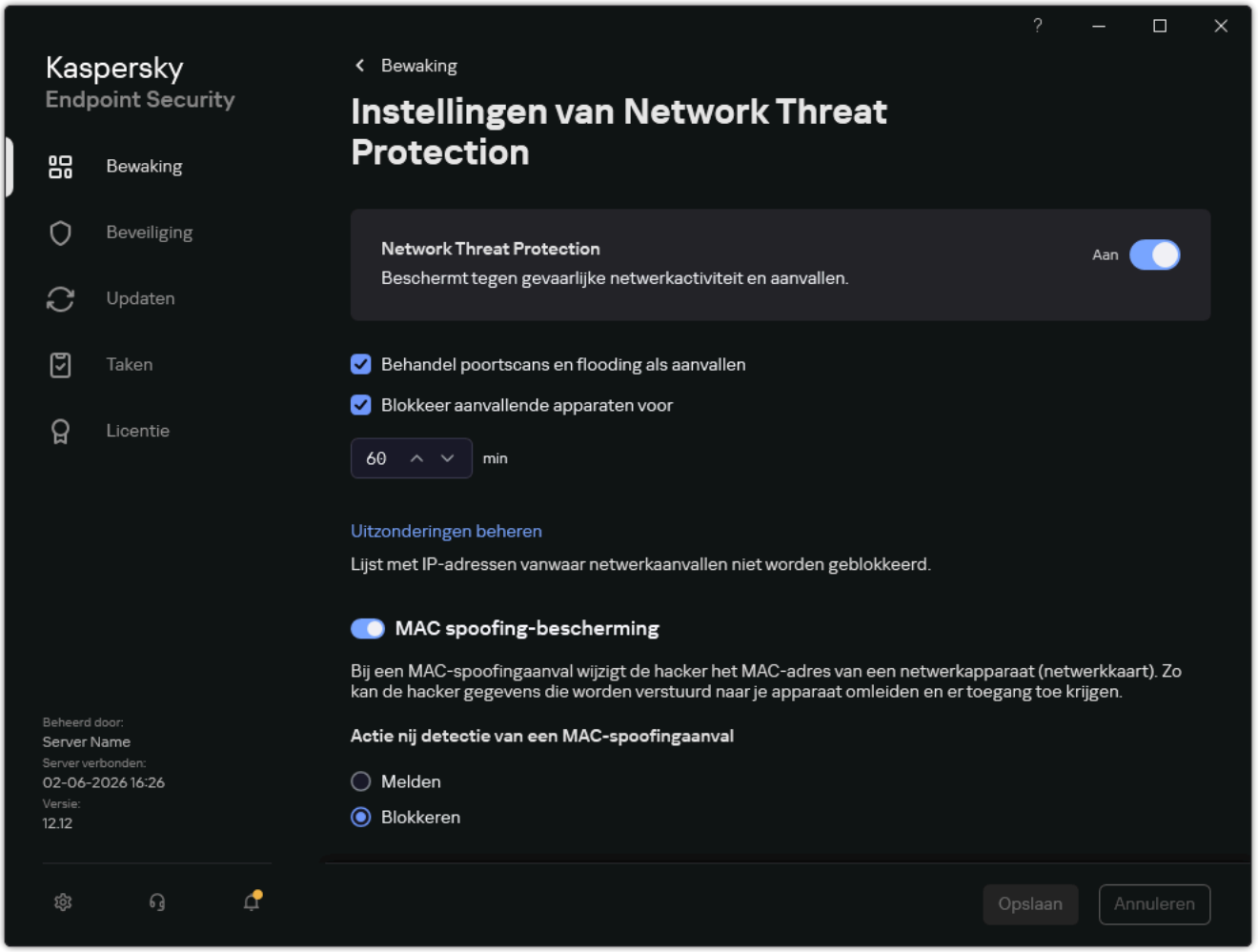
How het onderdeel Web Threat Protection in- of uit te schakelen in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Communication & Web Protection** → **Network Threat Protection**.
5. Gebruik de schakelaar **Network Threat Protection ENABLED** om de component in of uit te schakelen.
6. Sla uw wijzigingen op.

Hoe het onderdeel Anti-Phishing in het programma-interface in- of uit te schakelen

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.



Instellingen van Network Threat Protection

3. Gebruik de schakelaar **Network Threat Protection** om de component in of uit te schakelen.
4. Sla uw wijzigingen op.

Een aanvallende computer blokkeren

Als het onderdeel Network Threat Protection is ingeschakeld, blokkeert Kaspersky Endpoint Security automatisch netwerkbedreigingen. Bovendien kan het programma de aanvallende computer blokkeren en het verzenden van netwerkpakketten voor een bepaalde tijd beperken. Kaspersky Endpoint Security blokkeert standaard de computer gedurende een uur.

Hoe een aanvallende computer te blokkeren in Administration Console (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Essential Threat Protection → Network Threat Protection** in het beleidsvenster.
4. Onder **Instellingen van Network Threat Protection**, selecteer de **Blokkeer aanvallende apparaten voor N min** selectievakje.

   Als deze optie is ingeschakeld, voegt de Network Threat Protection-component de aanvallende computer toe aan de geblokkeerde lijst. 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 999 minuten.
5. Stel een andere blokkeringsduur in voor een aanvallende computer in het veld rechts van het selectievakje **Blokkeer aanvallende apparaten voor N min**.
6. Sla uw wijzigingen op.

Een aanvallende computer blokkeren in Web Console en Cloud Console

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management → Policies**.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.

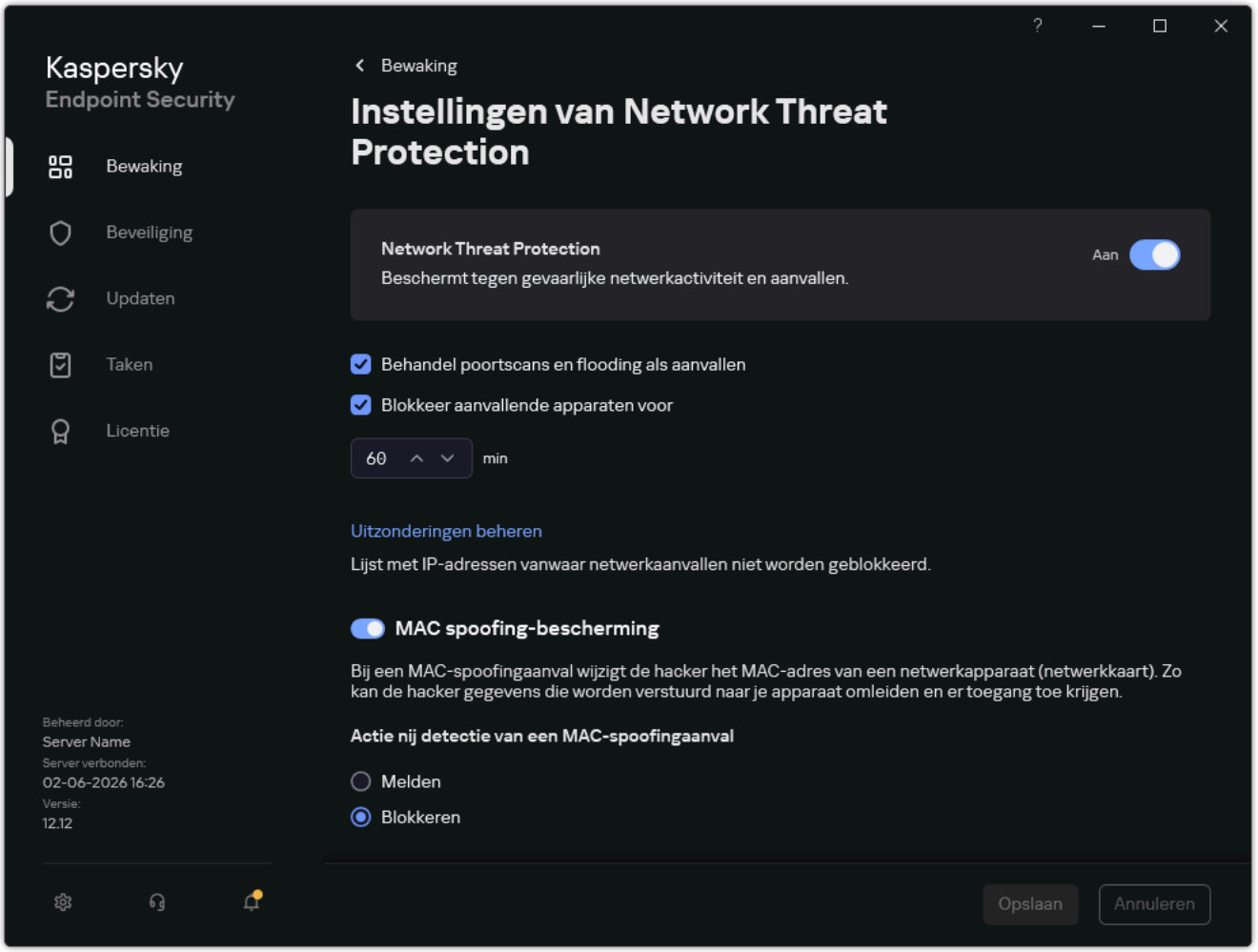
   U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Communication & Web Protection → Network Threat Protection**.
5. Schakel in het blok **Action on threat detection** het selectievakje **Block attack and attacking device for (min)** in.

   Als deze optie is ingeschakeld, voegt de Network Threat Protection-component de aanvallende computer toe aan de geblokkeerde lijst. 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 999 minuten.
6. Wijzig de blokkeringsduur van de aanvallende computer.
7. Sla uw wijzigingen op.

Hoe een aanvallende computer te blokkeren in de gebruikersinterface van het programma

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.



Instellingen van Network Threat Protection

3. Zet de schakelaar **Blokkeer aanvallende apparaten voor N min** aan.

   Als deze optie is ingeschakeld, voegt de Network Threat Protection-component de aanvallende computer toe aan de geblokkeerde lijst. 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 999 minuten.

4. Stel een andere blokkeringsduur in voor een aanvallende computer in het veld onder de schakelaar **Blokkeer aanvallende apparaten voor N min**.

5. 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. Kaspersky Endpoint Security creëert de *Network attack detected* gebeurtenis. De gebeurtenis bevat informatie over de aanvallende computer: IP- en MAC-adressen.

U kunt het MAC-adres van de aanvallende computer bekijken in de gebruikersinterface van het programma of in de Kaspersky Security Center-consoleversie 15.1 of hoger.



Melding over detectie van netwerkaanvallen

Kaspersky Endpoint Security deblokkeert de computer wanneer de opgegeven tijd om is. De Kaspersky Security Center-console biedt geen andere hulpmiddelen voor het bewaken van geblokkeerde computers dan *Network attack detected* gebeurtenissen in het rapport. U kunt alleen een lijst met geblokkeerde computers bekijken in de interface van het programma. Deze functionaliteit wordt geleverd door de *Netwerkmonitor* tool. U kunt ook de Network Monitor-tool gebruiken om een computer te deblokkeren.

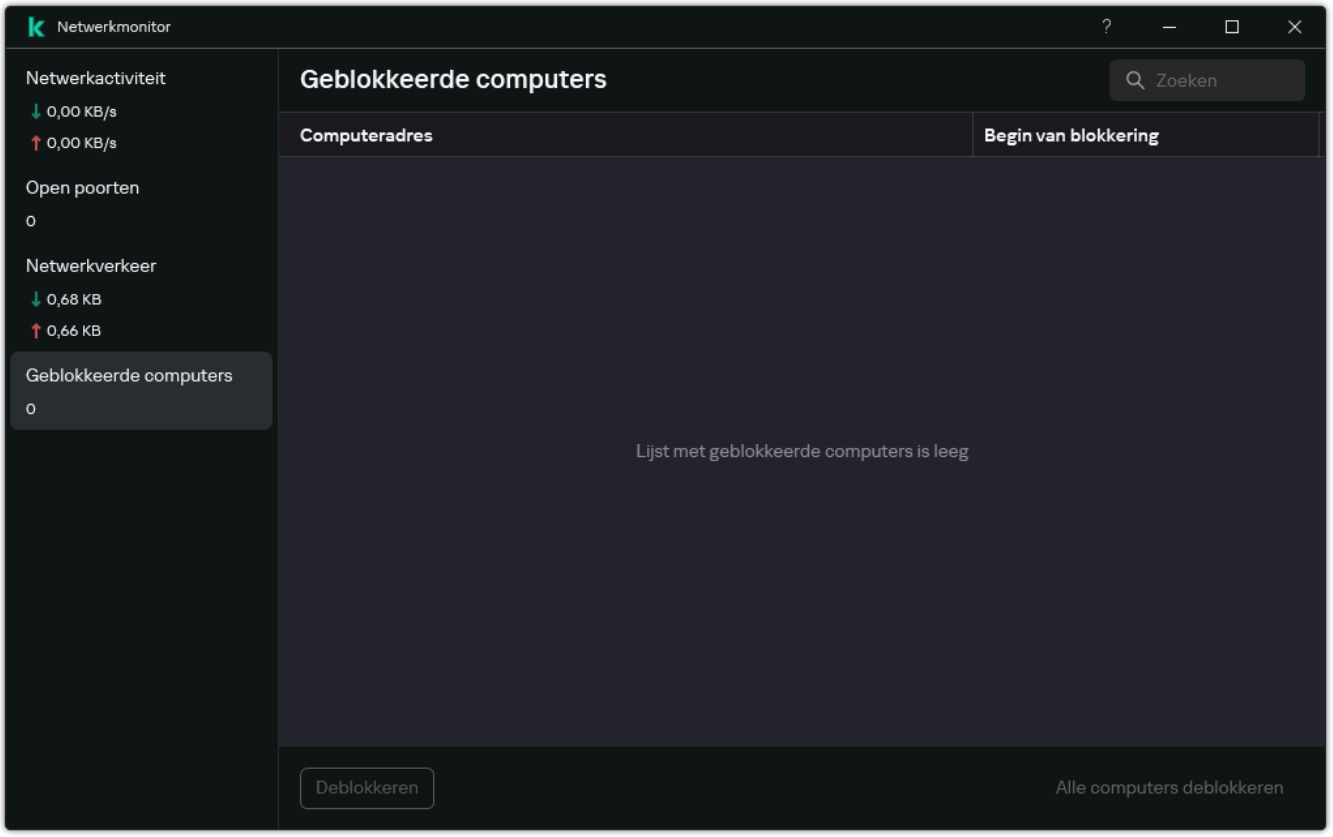
Om een computer te deblokkeren:

1. Ga in het hoofdvenster van het programma naar **Bewaking** en klik op de tegel **Netwerkmonitor**.
2. Ga naar het tabblad **Geblokkeerde computers**.

   Dit opent een lijst met geblokkeerde computers (zie onderstaande afbeelding).

   Kaspersky Endpoint Security wist de blokkeerlijst wanneer het programma opnieuw wordt opgestart en wanneer de instellingen voor Network Threat Protection worden gewijzigd.

3. Selecteer de computer die u wilt deblokkeren en klik **Deblokkeren**.



Lijst met geblokkeerde computers

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. U kunt ook het protocol en de poort selecteren die worden gebruikt voor communicatie en specifieke netwerkactiviteiten toestaan.

De mogelijkheid om protocollen en poorten te selecteren voor uitsluitingen is toegevoegd in Kaspersky Endpoint Security 12.2. Zorg ervoor dat de applicatie en de beheerplug-in zijn bijgewerkt naar versie 12.2 of hoger. Als u een eerdere versie van het programma of de beheerplug-in gebruikt, kan Kaspersky Endpoint Security alleen netwerkactiviteiten per IP-adres toestaan.

Het wijzigen van de lijst met uitgezonderde blokkeringen kan worden geblokkeerd door de eigenschappen van het bovenliggende beleid. Om de lijst te wijzigen, moet u toestaan dat de instellingen van vertrouwde zone in de Webconsole (het "hangslot" moet ontgrendeld zijn).

Vertrouwde zones zijn verschillend gegroepeerd in de Beheerconsole (MMC) en de Webconsole. Ook de manier waarop wijziging in de parameters voor de vertrouwde zone worden voorkomen, verschilt (verschillende "hangsloten"). We raden aan dat u alleen de Webconsole gebruikt om het programma te beheren. Als u de vertrouwde zone in verschillende consoles configureert, kan de beheerplug-in het "hangslot" terugzetten naar de standaardstatus.

Hoe adressen van uitsluitingen van blokkeren configureren in Administration Console (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Essential Threat Protection** → **Network Threat Protection** in het beleidsvenster.
4. In het blok **Instellingen van Network Threat Protection**, klikt u op de knop **Uitzonderingen**.
5. Klik in het venster op de knop **Toevoegen**.
6. Voer het IP-adres van de computer dat niet moet worden geblokkeerd als er netwerkaanvallen vanaf dat adres plaatsvinden.

   Selecteer indien nodig het protocol en de poorten waarmee gegevens worden verzonden.
7. Sla uw wijzigingen op.

Hoe adressen van uitsluitingen te configureren van blokkeren in Web Console en Cloud Console

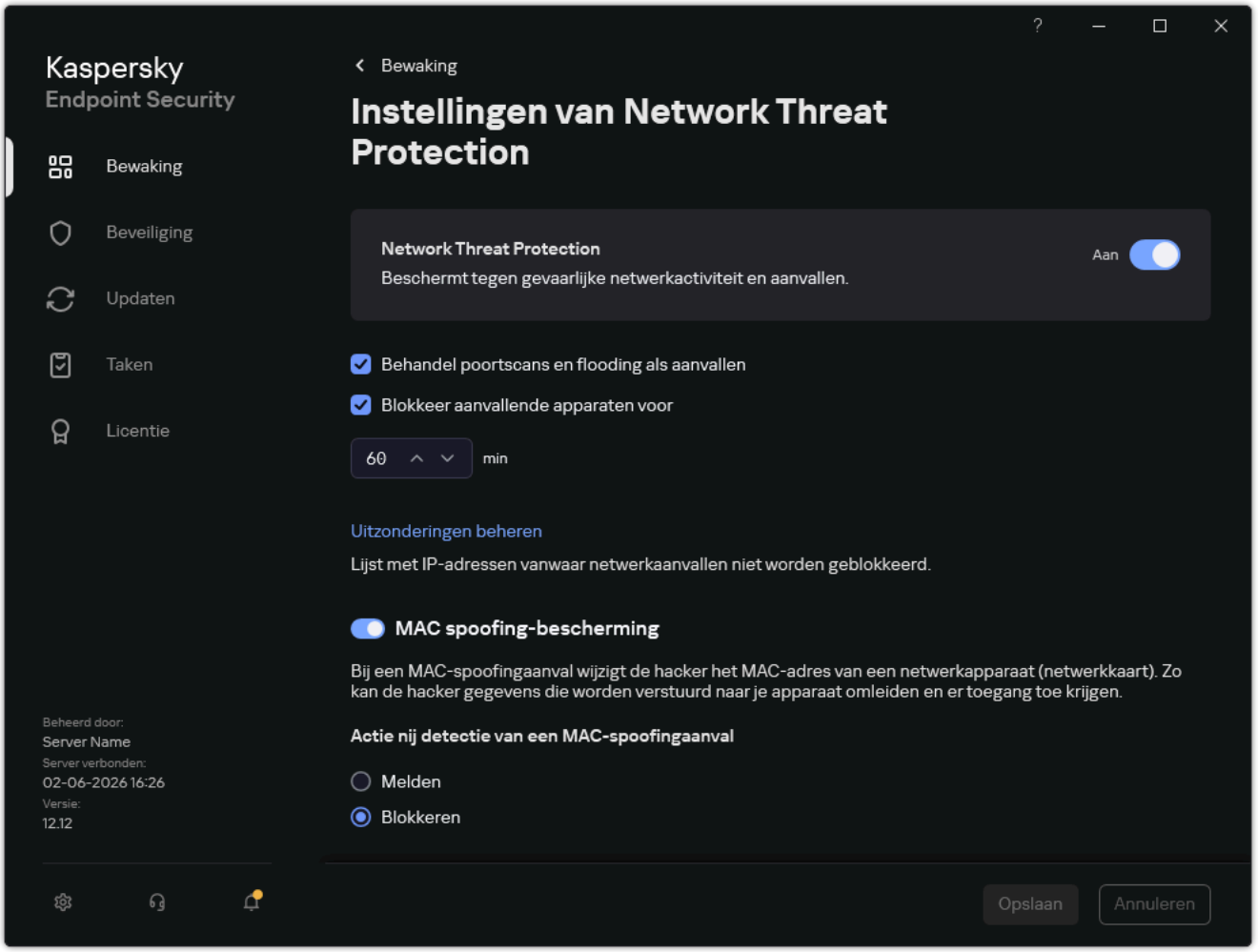
1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.

   U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Communication & Web Protection** → **Network Threat Protection**.
5. Klik in het bovenste gedeelte van het venster op de link **Trusted IP addresses**.
6. Klik in het venster op de knop **Add**.
7. Voer het IP-adres van de computer dat niet moet worden geblokkeerd als er netwerkaanvallen vanaf dat adres plaatsvinden.

   Geef indien nodig het subnet op.
8. Sla uw wijzigingen op.

Hoe adressen van uitsluitingen van blokkering te configureren in de gebruikersinterface van het programma

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.



Instellingen van Network Threat Protection

3. Klik op de koppeling **Uitzonderingen beheren**.
4. Klik in het 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.

   Selecteer indien nodig het protocol en de poorten waarmee gegevens worden verzonden.
6. Sla uw wijzigingen op.

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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Essential Threat Protection** → **Network Threat Protection** in het beleidsvenster.
4. In het blok **Instellingen van Network Threat Protection**, klikt u op de knop **Uitzonderingen**.
5. 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 knop → **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.
6. De lijst met uitzonderingen importeren:
   a. Klik op de knop → **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.
7. Sla uw wijzigingen op.

Een lijst met uitzonderingen exporteren en importeren in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Communication & Web Protection** → **Network Threat Protection**.
5. Klik in het bovenste gedeelte van het venster op de link **Trusted IP addresses**.
   De lijst met uitzonderingen wordt geopend.

6. De lijst met regels exporteren:

   a. Selecteer de uitzonderingen die u wilt exporteren.

   b. Klik op de knop → **Export**.

      Kaspersky Endpoint Security exporteert de lijst met uitzonderingen naar een JSON-bestand in de standaard downloadmap.

7. De lijst met uitzonderingen importeren:

   a. Klik op de knop → **Import**.

      Selecteer in het geopende venster het JSON-bestand waaruit u de lijst met uitzonderingen wil importeren.

   b. 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 JSON-bestand.

8. Sla uw wijzigingen op.

Network Threat Protection 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 (netwerkkaart) 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.

We raden af om de bescherming tegen MAC spoofing in te schakelen op virtuele machines in de Microsoft Hyper-V -infrastructuur. Vanwege de specifieke kenmerken van het Microsoft Hyper-V -platform kan Kaspersky Industrial CyberSecurity for Nodes de hypervisor blokkeren vanwege fout-positieve resultaten.

Bescherming tegen Network Threat Protection configureren op type in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Essential Threat Protection** → **Network Threat Protection** in het beleidsvenster.
4. Gebruik de selectievakje **Poortscans en flooding behandelen als aanvallen** om detectie van deze aanvallen in of uit te schakelen.

   Als deze functionaliteit is ingeschakeld, controleert Kaspersky Endpoint Security het netwerkverkeer op port scanning en network flooding. Als dergelijk gedrag wordt gedetecteerd, waarschuwt het programma de gebruiker en stuurt de desbetreffende gebeurtenis naar Kaspersky Security Center. Het programma biedt informatie over de computer die de verzoeken doet. Deze informatie is nodig voor een tijdige reactie. Echter, Kaspersky Endpoint Security blokkeert de computer die de verzoeken doet niet, omdat dergelijk verkeer normaal kan zijn op het bedrijfsnetwerk.
5. Selecteer in het blok **Mac-adresvervalsing beschermingsmodus** een van de volgende opties:
   - **Aanvallen met MAC-adresvervalsing niet bijhouden**.
   - **Melden**.
   - **Blokkeren**.
6. Sla uw wijzigingen op.

Hoe Network Threat Protection per type te configureren in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.

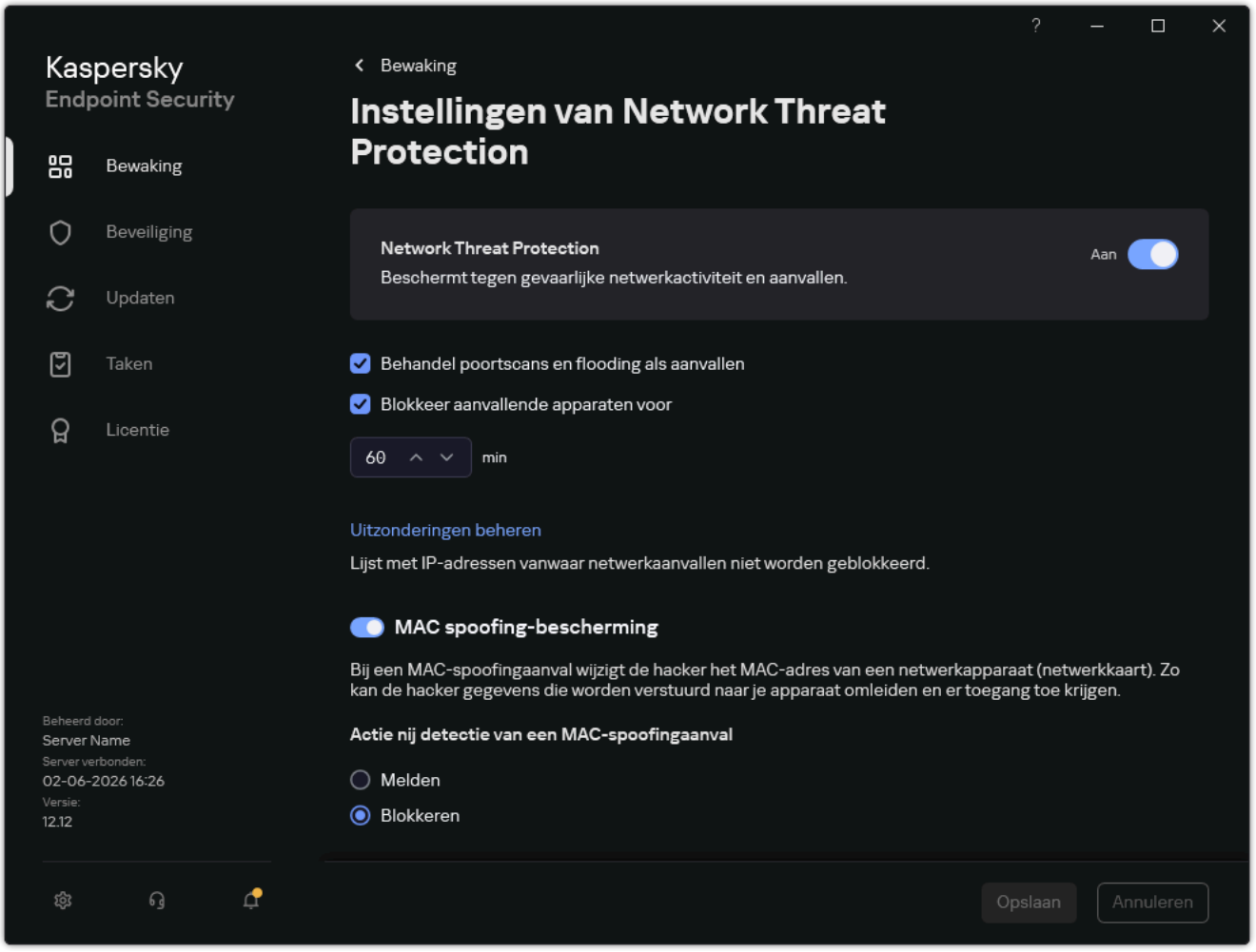
   U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **Communication & Web Protection** → **Network Threat Protection**.
5. Gebruik de selectievakje **Treat port scanning and network flooding as attacks** om detectie van deze aanvallen in of uit te schakelen.

   Als deze functionaliteit is ingeschakeld, controleert Kaspersky Endpoint Security het netwerkverkeer op port scanning en network flooding. Als dergelijk gedrag wordt gedetecteerd, waarschuwt het programma de gebruiker en stuurt de desbetreffende gebeurtenis naar Kaspersky Security Center. Het programma biedt informatie over de computer die de verzoeken doet. Deze informatie is nodig voor een tijdige reactie. Echter, Kaspersky Endpoint Security blokkeert de computer die de verzoeken doet niet, omdat dergelijk verkeer normaal kan zijn op het bedrijfsnetwerk.

6. Selecteer in het blok **MAC Spoofing Protection** een van de volgende opties:
   - **MAC Spoofing Protection ENABLED**.
   - **Inform**.
   - **Block**.
7. Sla uw wijzigingen op.

Bescherming tegen Network Threat Protection configureren op type in de programma-interface

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.



Instellingen van Network Threat Protection

3. Gebruik de schakelaar **Behandel poortscans en flooding als aanvallen** om detectie van deze aanvallen in of uit te schakelen.

   Als deze functionaliteit is ingeschakeld, controleert Kaspersky Endpoint Security het netwerkverkeer op port scanning en network flooding. Als dergelijk gedrag wordt gedetecteerd, waarschuwt het programma de gebruiker en stuurt de desbetreffende gebeurtenis naar Kaspersky Security Center. Het programma biedt informatie over de computer die de verzoeken doet. Deze informatie is nodig voor een tijdige reactie. Echter, Kaspersky Endpoint Security blokkeert de computer die de verzoeken doet niet, omdat dergelijk verkeer normaal kan zijn op het bedrijfsnetwerk.

4. Gebruik de schakelaar **MAC spoofing-bescherming** om detectie van deze aanvallen in of uit te schakelen.

5. Selecteer in het blok **Actie nij detectie van een MAC-spoofingaanval** een van de volgende opties:

   - **Melden**.
   - **Blokkeren**.

6. Sla uw wijzigingen op.

Firewall

Het onderdeel Firewall blokkeert ongeautoriseerde verbindingen met een 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. Plaatst het programma in een van de vertrouwensgroepen: *Vertrouwd*, *Deels beperkt*, *Zeer beperkt*, *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 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 op een bepaalde manier. Netwerkregel voor programma's omvat toegangsregels op basis van de netwerkstatus: *Openbaar netwerk*, *Lokaal netwerk*, *Vertrouwd netwerk*. 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.

Typen netwerkverbinding

U kunt met de Firewall de netwerkactiviteit beheren, afhankelijk van het type van de netwerkverbinding. Kaspersky Endpoint Security ontvangt het type netwerkverbinding van het besturingssysteem van de computer. Het type van de netwerkverbinding in het besturingssysteem wordt door de gebruiker ingesteld bij het opzetten van de verbinding. U kunt het type van de netwerkverbinding wijzigen in de instellingen van Kaspersky Endpoint Security. De firewall controleert de netwerkactiviteit afhankelijk van het type netwerk gespecificeerd in de Kaspersky Endpoint Security-instellingen en niet in het besturingssysteem.

De volgende typen netwerkverbindingen zijn beschikbaar:

- **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 het type *Openbaar netwerk* toe aan het internet. U kunt het type 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 een 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.

De Firewall in- of uitschakelen in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer in het beleidsvenster **Essential Threat Protection** → **Firewall**.
4. Gebruik het selectievakje **Firewall** om het onderdeel in of uit te schakelen.
5. Sla uw wijzigingen op.

De Firewall in- of uitschakelen in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Communication & Web Protection** → **Firewall**.

5. Gebruik de schakelaar **Firewall ENABLED** om de component in of uit te schakelen.

6. Sla uw wijzigingen op.

De Firewall in- of uitschakelen 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. Gebruik de schakelaar **Firewall** om de component 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 (ook wel Intrusion Detection System (IDS) genoemd) controleert inkomend netwerkverkeer op activiteiten die kenmerkend zijn 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.

Type van de netwerkverbinding wijzigen

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

Wijzig het type 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 het type wilt wijzigen.

5. Selecteer in de kolom **Netwerktype** het type 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 een 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

Firewall filtert alle netwerkactiviteit op de computer in overeenstemming met de regels voor netwerkpakketten. Regels voor netwerkpakketten bevatten voorwaarden (bijvoorbeeld richting, protocol) die Firewall toepast om netwerkverbindingen van de computer te beheren. Regels voor netwerkpakketten specificeren ook de actie die Firewall moet uitvoeren met de verbinding die overeenkomt met de regel (de verbinding toestaan of blokkeren).

Aanbevelingen voor het maken van regels voor netwerkpakketten

U kunt een IP-adres of een reeks IP-adressen opgeven om netwerkactiviteit te filteren. U kunt ook een DNS-naam opgeven, maar we raden aan om IP-adressen en IP-adresbereiken te gebruiken. Het gebruik van DNS-namen in namen van netwerkpakketten kan onveilig zijn omdat de eigenaar van de DNS-server de parameters van het DNS-record kan wijzigen. Een kwaadwillende kan ook DNS-berichten vervalsen en de regels van de Firewall omzeilen.

U kunt netwerkverbindingen via DNS-namen beheren met Regels voor Webcontrole. Als u een DNS-naam moet opgeven in de Firewall-regels:

- Zorg voor de beveiliging van het bedrijfs-LAN.
- Zorg voor de beveiliging van caching en gezaghebbende DNS-servers.
- Schakel de bescherming van het DNS-record tegen wijzigingen in.

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

Methoden voor het maken van regels voor netwerkpakketten

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.

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. Ga naar 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** 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. Gebruik de **Toevoegen** vervolgkeuzelijst, selecteer de locatie van de regel in de lijst: bovenaan de lijst, onderaan de lijst of naast de geselecteerde regel.

   De positie van de regel in de lijst bepaalt de prioriteit van de regel. De regel bovenaan de lijst heeft de hoogste prioriteit.
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** 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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.

2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

3. Selecteer in het beleidsvenster **Essential Threat Protection** → **Firewall**.

4. 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.

5. Ga naar het tabblad **Regels voor netwerkpakketten**.

   Dit opent een lijst met standaard netwerkregels die door Firewall zijn ingesteld.

6. Gebruik de **Toevoegen** vervolgkeuzelijst, selecteer de locatie van de regel in de lijst: bovenaan de lijst, onderaan de lijst of naast de geselecteerde regel.

   De positie van de regel in de lijst bepaalt de prioriteit van de regel. De regel bovenaan de lijst heeft de hoogste prioriteit.

7. Voer de naam van de netwerkservice handmatig in het veld **Naam** in.

8. 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.

9. Als u wilt dat de acties van de netwerkregel worden opgenomen in het rapport, schakelt u het selectievakje **Gebeurtenissen registreren** in.

10. Sla de nieuwe netwerkregel op.

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. Schakel hiervoor het selectievakje naast het object uit.

Een regel voor netwerkpakketten maken in de webconsole en de cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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 **Communication & Web Protection** → **Firewall**.
5. Selecteer het tabblad **Network packet rules**.

   Dit opent een lijst met standaard netwerkregels die door Firewall zijn ingesteld.
6. Klik op **Add**.

   Dit opent het formulier voor een nieuwe netwerkregel.
7. Voer de naam van de netwerkservice handmatig in het veld **Rule name** in.
8. Configureer de netwerkregelinstellingen (zie onderstaande tabel).

   U kunt een vooraf gedefinieerd regelsjabloon selecteren door op de koppeling **Select rule 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 knop **Move** 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 pakketregel in of uit te schakelen.

Het tabblad Regels voor netwerkpakketten

Parameter	Beschrijving
Actie	**Toestaan**. **Blokkeren**. **Volgens programmaregels**. Als deze optie is geselecteerd, past Firewall de Netwerkregels voor programma's toe op de netwerkverbinding
Protocol	Beheer de netwerkactiviteit via het geselecteerde protocol: TCP, UDP, ICMP, ICMPv6, IGMP en GRE. Als ICMP of ICMPv6 als het protocol is geselecteerd, kunt u het ICMP-pakkettype en de pakketcode definiëren. Als TCP of UDP als het type protocol is geselecteerd, kunt u de door poortnummers van de lokale en externe computers opgeven waartussen de verbinding moet worden bewaakt. Bereik van mogelijke waarden voor de poortnummers: 0–65535. In elk veld kunt u meerdere waarden invoeren, gescheiden door `,` of geef een waardenbereik op met `-`. Bijvoorbeeld: • `100,101` • `100-130` • `100,110-130`
Richting	**Inkomend (pakket)**. Firewall past de netwerkregel toe op alle inkomende netwerkpakketten. **Inkomend**. De netwerkregel wordt door Firewall toegepast op alle netwerkpakketten die door een externe computer geactiveerd zijn. **Inkomend / Uitgaand**. Firewall past de netwerkregel toe op alle inkomende en uitgaande netwerkpakketten. **Uitgaand (pakket)**. Firewall past de netwerkregel toe op alle uitgaande netwerkpakketten. **Uitgaand**. De netwerkregel wordt door Firewall toegepast op alle netwerkpakketten die door de computer van de gebruiker tot stand is gebracht.
Netwerkadapters	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.

Parameter	Beschrijving
Time to live (TTL)	Beperking van de controle van netwerkpakketten door hun levensduur (Time to Live, TTL).
Externe adressen	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. Als u in de netwerkpakketregel een DNS-naam hebt toegevoegd waarvan het IP-adres niet kon worden bepaald, geeft Kaspersky Endpoint Security een waarschuwing weer. In de lijst met netwerkpakketregels in de Webconsole wordt er een kolom toegevoegd met een beschrijving van de fout. De foutbeschrijving is niet beschikbaar in de Beheerconsole (MMC). Zulke pakketregels zijn gemarkeerd in kleur.
Lokale adressen	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. Het programma slaat alleen lokale adressen op als een lijst met externe adressen is opgegeven. Dat wil zeggen, de **Adressen uit de lijst** waarde is geselecteerd voor **Externe adressen** en er is ten minste één adres toegevoegd. Soms kan het lokale adres voor programma's niet worden verkregen. Als dit het geval is, wordt deze parameter genegeerd.

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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer in het beleidsvenster **Essential Threat Protection → Firewall**.
4. 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.
5. Ga naar het tabblad **Regels voor netwerkpakketten**.
6. 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 koppeling **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 netwerkpakketregels importeren:

   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.
8. Sla uw wijzigingen op.

Een lijst met netwerkpakketregels exporteren en importeren in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management → Policies**.
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 **Communication & Web Protection** → **Firewall**.

5. U exporteert de lijst met regels door het volgende te doen in het blok **Network packet rules**:

   a. Selecteer de regels die u wilt exporteren.

   b. Klik op de knop → **Export**.

      Kaspersky Endpoint Security exporteert de lijst met regels naar een JSON-bestand in de standaard downloadmap.

6. U importeert de lijst met regels door het volgende te doen in het blok **Network packet rules**:

   a. Klik op de knop → **Import**.

      Selecteer in het geopende venster het JSON-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 JSON-bestand.

7. Sla uw wijzigingen op.

Regels voor netwerkpakketten definiëren in XML

Met Firewall kunnen regels voor netwerkpakketten in XML-indeling worden geëxporteerd. Vervolgens kunt u het bestand aanpassen om bijvoorbeeld een groot aantal regels van hetzelfde type toe te voegen.

Het XML-bestand bevat twee hoofd-nodes: `Rules` en `Resources`. De node `Rules` geeft netwerkpakketregels. Deze node bevat regels die standaard geconfigureerd zijn (*voorgedefinieerde regels*) en regels die door de gebruiker zijn toegevoegd (*aangepaste regels*).

Netwerkpakketregel markering

```
<key name="0000">
        <tDWORD name="RuleId">100</tDWORD>
        <tDWORD name="RuleState">1</tDWORD>
        <tDWORD name="RuleTypeId">4</tDWORD>
        <tQWORD name="AppIdEx">0</tQWORD>
        <tDWORD name="ResIdEx">812</tDWORD>
        <tDWORD name="ResIdEx2">0</tDWORD>
        <tDWORD name="AccessFlag">2</tDWORD>
</key>
```

Instellingen netwerkpakketregel in XML-indeling

Parameter	Beschrijving	Waarde
`<key name="0000">`	Prioriteit van de regel. Hoe lager de waarde, hoe hoger de prioriteit.	Integer De prioriteitswaarde moet uit 4 cijfers bestaan. De nodes in het XML-bestand moeten worden gerangschikt op prioriteitswaarde, te beginnen met `0000`.
`RuleId`	ID van de regel.	**Voorgedefinieerde regels** `100` – **TCP-aanvragen voor DNS-server**. `101` – **UDP-aanvragen voor DNS-server**. `102` – **E-mailberichten versturen**. `110` – **Elke netwerkactiviteit** (Vertrouwde netwerken). `125` – **Elke netwerkactiviteit** (Lokale netwerken). `130` – **Netwerkactiviteit van Extern Bureaublad**. `131` – **TCP-verbindingen via lokale poorten**. `132` – **UDP-verbindingen via lokale poorten**. `133` – **Inkomende TCP-stroom**. `134` – **Inkomende UDP-stroom**. `137` – **Binnenkomende antwoorden van ICMP-berichten met een onbereikbare bestemming**. `138` – **Inkomende pakketten van ICMP-echoantwoord**. `140` – **Binnenkomende antwoorden van ICMP-berichten die verzonden zijn met tijdsoverschrijding**. `142` – **Inkomende ICMP-stroom**. `266` – **Inkomende pakketten van ICMPv6-echoaanvraag**.
`RuleState`	Status van de regel.	`0` – de voorgedefinieerde regel is uitgeschakeld. `1` – de voorgedefinieerde regel is ingeschakeld. `2` – de aangepaste regel is uitgeschakeld. `3` – de aangepaste regel is ingeschakeld.
`RuleTypeId`	ID van het regeltype	`4` – een regel voor netwerkpakketten.
`AppIdEx`	ID van het programma waarbij de netwerkpakketregel hoort.	Als de regel bij geen enkel programma behoort, is de waarde `0`.
`ResIdEx`	Hoofd-ID van de bron met regelinstellingen. U kunt deze id gebruiken om een blok met regelinstellingen te zoeken in de node `Resources`.	Integer
`ResIdEx2`	ID van het netwerktype	`0` – **Elk adres**. `50` – **Vertrouwde netwerken**. `51` – **Lokale netwerken**. `52` – **Openbare netwerken**. `<Network Identifier>` – **Adressen uit de lijst** (adressen worden handmatig gedefinieerd).
`AccessFlag`	Waarde van de parameter **Actie**.	`0` – **Toestaan**. `2` – **Volgens programmaregels**. `3` – **Blokkeren**. `4` – **Toestaan** en **Gebeurtenissen registreren**. `6` – **Volgens programmaregels** en **Gebeurtenissen registreren**. `7` – **Blokkeren** en **Gebeurtenissen registreren**.
`</key>`		

De node `Resources` geeft instellingen voor netwerkpakketregel. Aangepaste instellingen netwerkpakketregel staan vermeld in het `<key name="0004">` blok.

Aangepaste netwerkpakketregel marketing

```
<key name="0026">
        <key name="Data">
                <key name="RemotePorts"> </key>
                <key name="LocalPorts"> </key>
                <key name="AdapterBindings">
                        <key name="0000">
                                <key name="IpAddresses">
                                        <key name="0000">
                                                <key name="IP">
                                                        <key name="V6">
                                                                <tQWORD name="Hi">0</tQWORD>
                                                                <tQWORD name="Lo">0</tQWORD>
                                                                <tDWORD name="Zone">0</tDWORD>
                                                                <tSTRING name="ZoneStr"/>
                                                        </key>
                                                        <tBYTE name="Version">4</tBYTE>
                                                        <tDWORD name="V4">16909060</tDWORD>
                                                        <tBYTE name="Mask">32</tBYTE>
                                                </key>
                                                <key name="AddressIP"> </key>
                                                <tSTRING name="Address"/>
                                        </key>
                                </key>
                                <key name="MacAddresses">
                                        <key name="0000">
                                                <tDWORD name="Type">0</tDWORD>
                                                <tQWORD name="AddressData0">1108152157446</tQWORD>
                                                <tQWORD name="AddressData1">0</tQWORD>
                                        </key>
                                </key>
                                <tSTRING name="AdapterName">ADAPTER TEST 123</tSTRING>
                                <tDWORD name="InterfaceType">3</tDWORD>
                        </key>
                </key>
                <tTYPE_ID name="unique">3213697024</tTYPE_ID>
                <tBYTE name="Proto">2</tBYTE>
                <tBYTE name="Direction">2</tBYTE>
                <tBYTE name="IcmpType">0</tBYTE>
                <tBYTE name="IcmpCode">0</tBYTE>
                <tDWORD name="Flags">1</tDWORD>
                <tBYTE name="TTL">255</tBYTE>
        </key>
        <key name="Childs"> </key>
        <tDWORD name="Id">1073747214</tDWORD>
        <tDWORD name="ParentID">7</tDWORD>
        <tDWORD name="Flags">38</tDWORD>
        <tSTRING name="Name">TEST1</tSTRING>
</key>
```

Aangepaste instellingen netwerkpakketregel

Parameter	Beschrijving	Waarde
`<key name="Data">`	ID van het parameterblok.	Integer
`RemotePorts`	Waarde van de parameter **Externe poorten**.	Lijst van externe poortbereiken.
`LocalPorts`	Waarde van de parameter **Lokale poorten**.	Lijst van locale poortbereiken.

Parameter	Beschrijving	Waarde
`AdapterBindings`	Waarde van de parameter **Netwerkadapters**.	`IpAddresses` – waarde van de parameter **IP-adressen**. `MacAddresses` – waarde van de parameter **MAC-adressen**. `AdapterName` – naam van de netwerkadapter. `InterfaceType` – waarde van de parameter **Interfacetype**: • `0` – **Overige**. • `1` – **LoopBack**. • `2` – **Bedraad netwerk (Ethernet)**. • `3` – **Draadloos netwerk (Wifi)**. • `4` – **Tunnel**. • `5` – **PPP-verbinding**. • `6` – **PPPoE-verbinding**. • `7` – **VPN-verbinding**. • `8` – **Modemverbinding**.
`unique`	Interne ID van de structuur.	Integer Het is aanbevolen om deze parameter ongewijzigd te laten.
`Proto`	Waarde van de parameter **Protocol**.	`0` – uitgeschakeld. `1` – **ICMP**. `2` – **IGMP**. `6` – **TCP**. `17` – **UDP**. `47` – **GRE**. `58` – **ICMPv6**.
`Direction`	Waarde van de parameter **Richting**.	`1` – **Inkomend (pakket)**. `2` – **Uitgaand (pakket)**. `3` – **Inkomend/Uitgaand**. `4` – **Inkomend**. `5` – **Uitgaand**.

Parameter	Beschrijving	Waarde
`IcmpType`	Waarde van de parameter **ICMP-type**.	**ICMP-protocol** `0` – **Antwoord op echo** (ICMP) of uitgeschakeld. `3` – **Bestemming onbereikbaar** (ICMP). `4` – **Bron afgesloten**. `5` – **Omleiden**. `6` – **Alternatief hostadres**. `8` – **Echoaanvraag**. `9` – **Router-advertisement**. `10` – **Routeraanvraag**. `11` – **Tijd verstreken**. `12` – **Parameterprobleem**. `13` – **Tijdstempel**. `14` – **Antwoord op tijdstempel**. `15` – **Aanvraag voor informatie**. `16` – **Antwoord op informatie**. `17` – **Aanvraag voor adresmasker**. `18` – **Antwoord op adresmasker**. `30` – **Traceroute**. `31` – **Fout bij conversie van datagram**. `32` – **Omleiding van mobiele host**. `33` – **IPv6Where-Are-You**. `34` – **IPv6I-Am-Here**. `35` – **Aanvraag voor mobiele registratie**. `36` – **Antwoord op mobiele registratie**. `37` – **Aanvraag voor domeinnaam**. `38` – **Antwoord op domeinnaam**. `40` – **Photuris**. **ICMPv6-protocol** `1` – **Bestemming onbereikbaar**. `2` – **Pakket te groot**. `3` – **Tijd verstreken**. `4` – **Parameterprobleem**. `128` – **Echoaanvraag**. `129` – **Antwoord op echo**. `130` – **Query voor multicastlistener**. `131` – **Rapport voor multicastlistener**. `132` – **Multicastlistener gereed**. `133` – **Routeraanvraag**. `134` – **Router-advertisement**. `135` – **Neighboraanvraag**. `136` – **Neighbor-advertisement**. `137` – **Omleidingsbericht**. `138` – **Hernummeren router**. `139` – **Vraag naar ICMP-knooppuntgegevens**. `141` – **Bericht aanvraag voor omgekeerde neighbor-detectie**. `142` – **Bericht advertisement voor omgekeerde neighbor-detectie**. `143` – **Rapport van versie 2 multicastlistener**.

Parameter	Beschrijving	Waarde
		`144` – **Bericht aanvraag voor adresdetectie van interne agent**. `145` – **Antwoord aanvraag voor adresdetectie van interne agent**. `146` – **Aanvraag voor mobiele prefix**. `147` – **Advertisement voor mobiele prefix**. `148` – **Bericht aanvraag voor certificeringspad**. `149` – **Bericht advertisement voor certificeringspad**. `151` – **Advertisement voor multicastrouter**. `152` – **Aanvraag voor multicastrouter**. `153` – **Beëindiging van multicastrouter**.
`IcmpCode`	Waarde van de parameter **ICMP-code**.	`0` – **Code 0** of uitgeschakeld. `1` – **Code 1**. `2` – **Code 2**.
`Flags`	Aanwijzer van het structuurattribuut.	Integer Het is aanbevolen om deze parameter ongewijzigd te laten.
`TTL`	Waarde van de parameter **Time to live (TTL)**.	Waarde in seconden Indien uitgeschakeld is de waarde `0`.
`</key>`		
`Id`	Hoofd-ID van de bron (zie de node `Rules`).	Integer
`ParentID`	ID van de bovenliggende groep.	Integer Het is aanbevolen om deze parameter ongewijzigd te laten.
`Flags`	Status van de regel.	`6` – de regel is uitgeschakeld. `38` – de regel is ingeschakeld.
`Name`	Naam van de netwerkpakketregel.	String

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 hoger 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. Ga naar 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** 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** 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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.

2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

3. Selecteer in het beleidsvenster **Essential Threat Protection** → **Firewall**.

4. 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.

5. Ga naar het tabblad **Netwerkregels voor programma's**.

6. Klik op **Toevoegen**.

7. 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.

8. Klik op **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.

9. Selecteer het noodzakelijke programma.

10. Selecteer in de vervolgkeuzelijst **Geselecteerd programma toevoegen aan vertrouwensgroep** de optie **Standaardgroepen** en klik op **OK**.

    Het programma wordt toegevoegd aan de standaard groep.

11. Selecteer het relevante programma en vervolgens **Programmarechten** in het contextmenu van het programma.

    Het venster met toepassingsregels en eigenschappen wordt geopend.

12. Selecteer het tabblad **Netwerkregels**.

    Dit opent een lijst met standaard netwerkregels die door Firewall zijn ingesteld.

13. Klik op **Toevoegen**.

    Dit opent de eigenschappen van de netwerkregel.

14. Voer de naam van de netwerkservice handmatig in het veld **Naam** in.

15. 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.

16. Als u wilt dat de acties van de netwerkregel worden opgenomen in het rapport, schakelt u het selectievakje **Gebeurtenissen registreren** in.

17. Sla de nieuwe netwerkregel op.

18. Gebruik de knoppen **Omhoog**/**Omlaag** om de prioriteit van de netwerkregel in te stellen.

19. Sla uw wijzigingen op.

Een netwerkregel voor programma's maken in de webconsole en de cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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 **Communication & Web Protection** → **Firewall**.

5. Klik in het blok **Application rights and protected resources** op de koppeling **Application rights**.

   Dit opent het venster voor configuratie van programmarechten en de lijst met beschermde bronnen.

6. Ga naar het tabblad **Application rights**.

   U ziet een lijst met vertrouwensgroepen aan de linkerkant van het venster en hun eigenschappen aan de rechterkant.

7. In het blok **Applications**, klikt u 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 **Application**. Ga naar de volgende stap.

   Als u een netwerkregel wil maken voor meerdere programma's, selecteert u het type **Group** 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. Verlaat de wizard verlaten.

    Het programma wordt toegevoegd aan de vertrouwensgroep.

12. Selecteer links in het venster het relevante programma.

13. Selecteer in het rechterdeel van het venster **Network rules** uit de vervolgkeuzelijst.

    Dit opent een lijst met standaard netwerkregels die door Firewall zijn ingesteld.

14. Klik op **Add**.

    Dit opent de eigenschappen voor programmaregels.

15. Voer de naam van de netwerkservice handmatig in het veld **Rule name** in.

16. Configureer de netwerkregelinstellingen (zie onderstaande tabel).

    U kunt een vooraf gedefinieerd regelsjabloon selecteren door op de koppeling **Select rule template** 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 knop **Move** om de prioriteit van de netwerkregel in te stellen.

20. Sla uw wijzigingen op.

Instellingen Netwerkregels voor programma's

Parameter	Beschrijving
Actie	**Toestaan**. **Blokkeren**.
Protocol	Beheer de netwerkactiviteit via het geselecteerde protocol: TCP, UDP, ICMP, ICMPv6, IGMP en GRE. Als ICMP of ICMPv6 als het protocol is geselecteerd, kunt u het ICMP-pakkettype en de pakketcode definiëren. Als TCP of UDP als het type protocol is geselecteerd, kunt u de door poortnummers van de lokale en externe computers opgeven waartussen de verbinding moet worden bewaakt. Bereik van mogelijke waarden voor de poortnummers: 0–65535. In elk veld kunt u meerdere waarden invoeren, gescheiden door `,` of geef een waardenbereik op met `-`. Bijvoorbeeld: • `100,101` • `100-130` • `100,110-130`

Parameter	Beschrijving
Richting	**Inkomend**. **Inkomend / Uitgaand**. **Uitgaand**.
Externe adressen	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. Als u in de netwerkpakketregel een DNS-naam hebt toegevoegd waarvan het IP-adres niet kon worden bepaald, geeft Kaspersky Endpoint Security een waarschuwing weer. In de lijst met netwerkpakketregels in de Webconsole wordt er een kolom toegevoegd met een beschrijving van de fout. De foutbeschrijving is niet beschikbaar in de Beheerconsole (MMC). Zulke pakketregels zijn gemarkeerd in kleur.
Lokale adressen	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. Het programma slaat alleen lokale adressen op als een lijst met externe adressen is opgegeven. Dat wil zeggen, de **Adressen uit de lijst** waarde is geselecteerd voor **Externe adressen** en er is ten minste één adres toegevoegd. Soms kan het lokale adres voor programma's niet worden verkregen. Als dit het geval is, wordt deze parameter genegeerd.

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 in het hoofdvenster van het programma naar **Bewaking** 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.

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.

Het onderdeel Exploit-preventie bewaakt bovendien netwerkpoorten op processen van programma's die de beveiliging van de computer kunnen bedreigen. Het programma verkrijgt informatie over dergelijke processen met antivirusdatabases.

Exploit-preventie inschakelen en uitschakelen

Exploit-preventie is standaard ingeschakeld en werkt in de optimale modus. Kaspersky Endpoint Security controleert 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).

Exploit-preventie in- of uitschakelen in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Advanced Threat Protection** → **Exploit-preventie** in het beleidsvenster.
4. Gebruik het selectievakje **Exploit-preventie** om het onderdeel in of uit te schakelen.
5. Selecteer de relevante actie in het blok **Bij detectie van exploit**:
   - **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.
6. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Hoe Exploit-preventie in- of uit te schakelen in de webconsole en cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Host Threat Protection** → **Behavior Analysis** → **Exploit Prevention**.
5. Gebruik de schakelaar **Exploit Prevention** om de component in of uit te schakelen.

6. Selecteer de relevante actie in het blok **Action on threat detection**:

   - **Block**. 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.

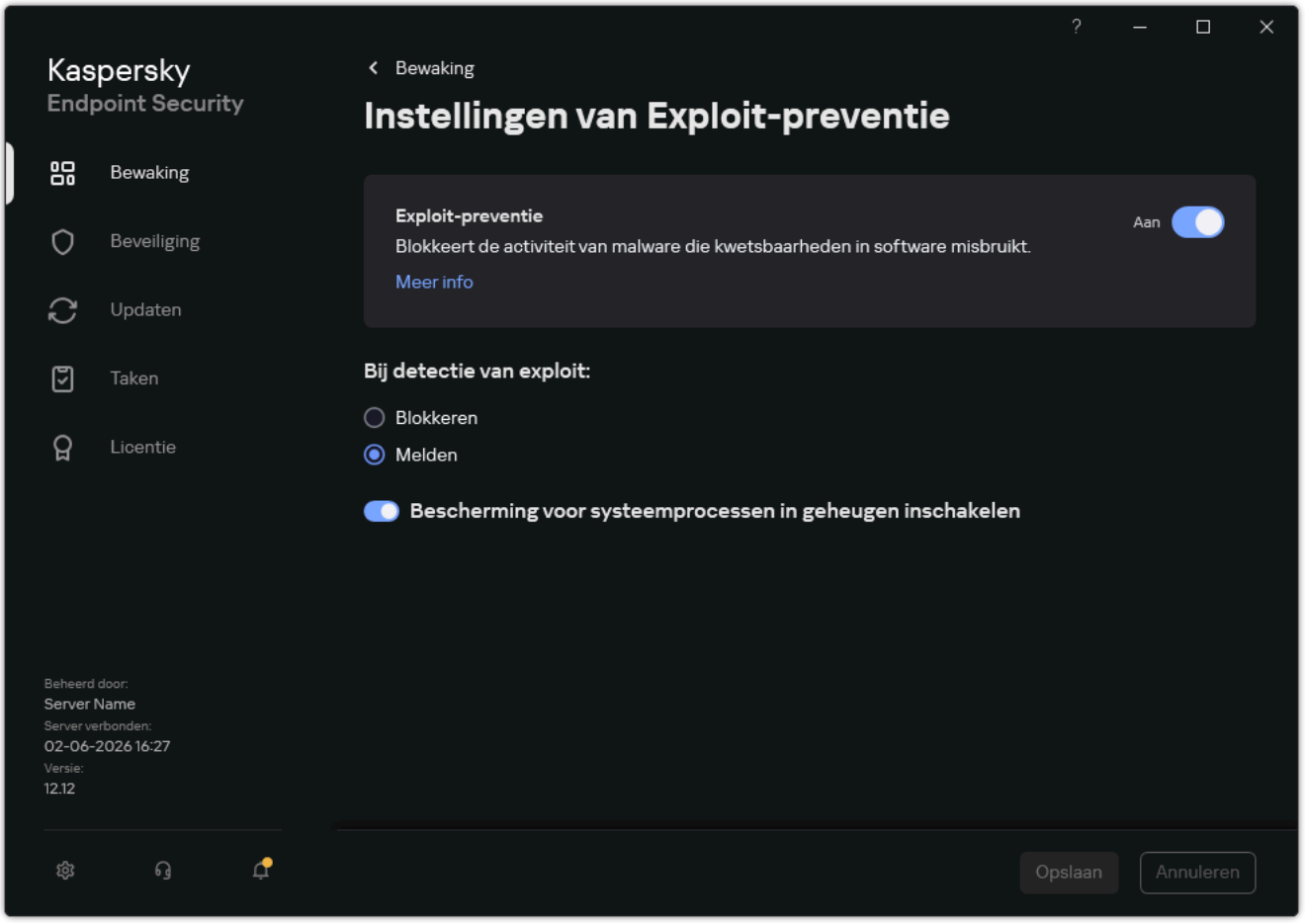
   - **Inform**. Als deze optie wordt geselecteerd wanneer een exploit wordt gedetecteerd, registreert Kaspersky Endpoint Security informatie over de exploit en voegt het informatie over deze exploit toe aan de lijst met actieve dreigingen.

7. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Hoe het onderdeel Anti-Phishing in de programma-interface in- of uitschakelen

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.



Instellingen van Exploit-preventie

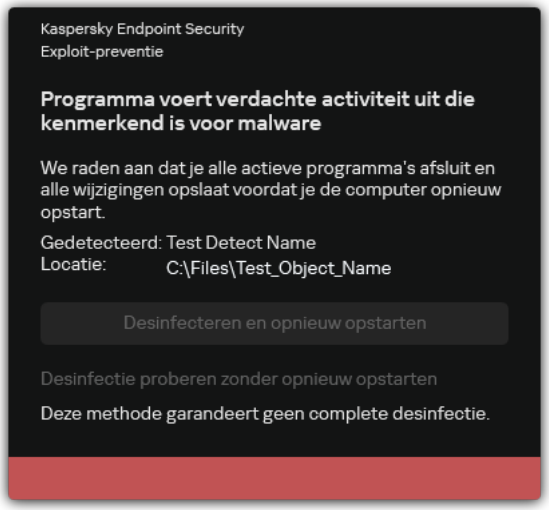
3. Gebruik de schakelaar **Exploit-preventie** om de component in of uit te schakelen.

4. Selecteer de relevante actie in het blok **Bij detectie van exploit**:

   - **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.

5. Sla uw wijzigingen op.



Melding over actieve dreiging

Bescherming voor systeemprocessen in geheugen

De bescherming van systeemprocessen in het geheugen is standaard ingeschakeld. Kaspersky Endpoint Security blokkeert externe processen die toegang proberen te krijgen tot systeemprocessen.

Hoe de geheugenbeveiliging van het systeemproces in- of uitschakelen in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.

2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

3. Selecteer **Advanced Threat Protection** → **Exploit-preventie** in het beleidsvenster.

4. Gebruik het selectievakje **Bescherming voor systeemprocessen in geheugen inschakelen** om het onderdeel in of uit te schakelen.

5. Sla uw wijzigingen op.

Hoe de bescherming van het geheugen van het systeemproces in- of uitschakelen in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

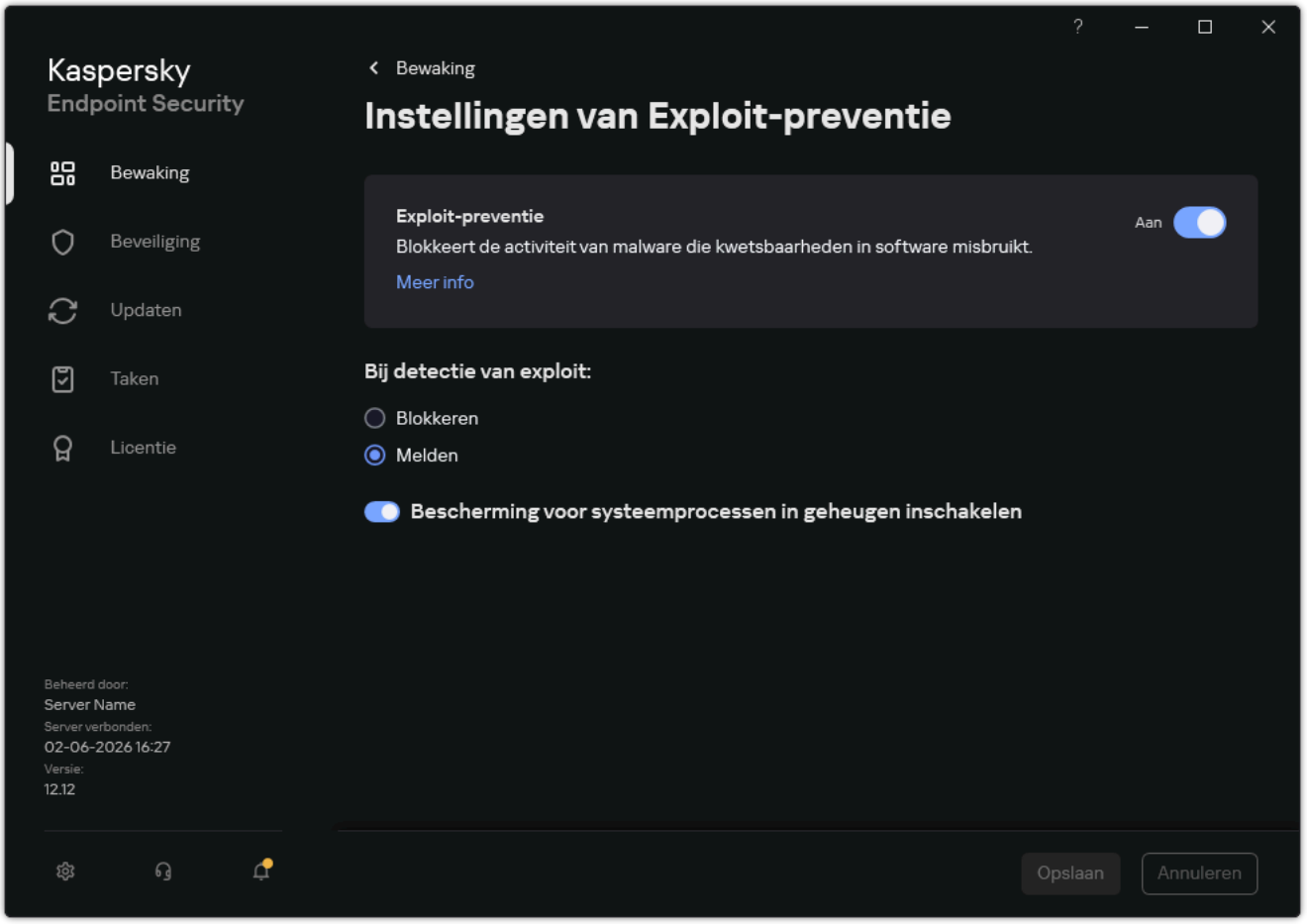
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.

   U ziet nu het venster met de beleidseigenschappen.

3. Selecteer het tabblad **Application settings**.
4. Ga naar **Host Threat Protection → Behavior Analysis → Exploit Prevention**.
5. Gebruik de schakelaar **System process memory protection ENABLED** om deze functie in of uit te schakelen.
6. Sla uw wijzigingen op.

Hoe de geheugenbeveiliging van het systeemproces in- of uitschakelen in de programma-interface

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.



Instellingen van Exploit-preventie

3. Gebruik de schakelaar **Bescherming voor systeemprocessen in geheugen inschakelen** om deze functie in of uit te schakelen.
4. Sla uw wijzigingen op.

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 is gebaseerd op de definities van gedragspatronen en levert een proactieve bescherming voor de computer.

Het onderdeel Gedragsdetectie bewaakt bovendien netwerkpoorten op processen van programma's die de beveiliging van de computer kunnen bedreigen. Het programma verkrijgt informatie over dergelijke processen met antivirusdatabases.

Gedragsdetectie is standaard ingeschakeld en werkt in de modus die door experts van Kaspersky is aanbevolen. Wanneer kwaadaardige activiteit wordt gedetecteerd, verwijdert Kaspersky Endpoint Security het uitvoerbare bestand van het kwaadaardige programma.

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.

Gedragsdetectie inschakelen of uitschakelen in de Beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de beheerconsole **Policies**.
3. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
4. Selecteer **Advanced Threat Protection** → **Gedragsdetectie** in het beleidsvenster.
5. Gebruik het selectievakje **Gedragsdetectie** om het onderdeel in of uit te schakelen.
6. Selecteer de relevante actie in het blok **Actie bij detectie van malware-activiteit**:
   - **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.
   - **Blokkeren**. 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.
7. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Gedragsdetectie in- of uitschakelen in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Host Threat Protection** → **Behavior Analysis** → **Behavior Detection**
5. Gebruik de schakelaar **Behavior Detection ENABLED** om de component in of uit te schakelen.

6. Selecteer de relevante actie in het blok **Action on threat detection**:

   - **Delete**. 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.

   - **Block**. Als deze optie wordt geselecteerd wanneer schadelijke activiteit wordt gedetecteerd, beëindigt Kaspersky Endpoint Security dit programma.

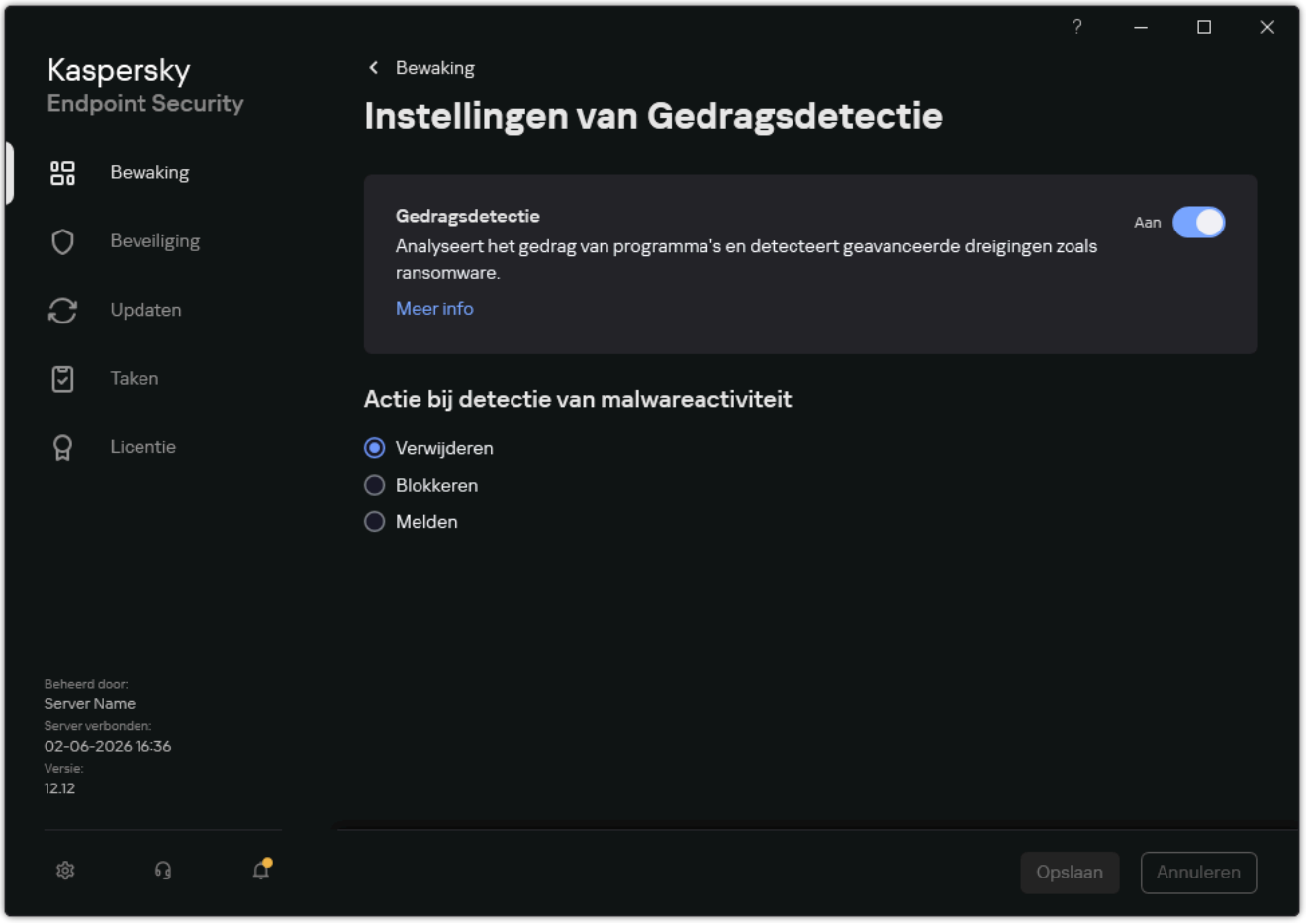
   - **Inform**. Als deze optie is geselecteerd wanneer malware-activiteit van een programma wordt gedetecteerd, voegt Kaspersky Endpoint Security informatie over de malware-activiteit van het programma toe aan de lijst met actieve dreigingen.

7. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Gedragsdetectie in- of uitschakelen in de programma-interface

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

2. Selecteer **Advanced Threat Protection** → **Gedragsdetectie** in het venster met de programma-instellingen.



Instellingen van Gedragsdetectie

3. Gebruik de schakelaar **Gedragsdetectie** om de component in of uit te schakelen.

4. Selecteer de relevante actie in het blok **Actie bij detectie van malwareactiviteit**:

   - **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.

   - **Blokkeren**. 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.

5. 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.

Anti-Cryptor

Vanaf Kaspersky Endpoint Security 12.12 voor Windows wordt de bescherming van gedeelde mappen tegen externe encryptie die vroeger deel uitmaakte van het Gedragsdetectie onderdeel is een afzonderlijk onderdeel, Anti-Cryptor.

Alleen bewerkingen met bestanden op apparaten voor massaopslag met het NTFS-bestandssysteem en die niet met EFS zijn geëncrypt, worden door het onderdeel gemonitord.

Het onderdeel Anti-Cryptor 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.

Om het onderdeel Anti-Cryptor te laten werken, moet u: het onderdeel Gedragsdetectie inschakelen.

Als Kaspersky Endpoint Security een poging detecteert om bestanden in gedeelde mappen te wijzigen, worden de volgende acties ondernomen:

- 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.

- Voegt een item toe aan rapporten in de lokale programma-interface en stuurt 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.

Bescherming van gedeelde mappen tegen externe encryptie inschakelen en uitschakelen

Standaard is de bescherming van gedeelde mappen tegen externe encryptie ingeschakeld en werkt deze zoals aanbevolen door Kaspersky-experts. Om deze functionaliteit te configureren, kunt u een beschermd bereik maken en indien nodig uitzonderingen configureren. Standaard identificeert het programma automatisch gedeelde mappen en controleert de bestandsactiviteit in alle mappen. Wanneer een poging tot externe encryptie van bestanden in gedeelde mappen wordt gedetecteerd, blokkeert Kaspersky Endpoint Security de sessie van de externe gebruiker gedurende één uur (standaard).

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 in of uitschakelen in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Advanced Threat Protection** → **Anti-Cryptor** in het beleidsvenster.
4. Gebruik het selectievakje **Anti-Cryptor** om de detectie van activiteit die typisch is voor externe encryptie in of uit te schakelen.
5. Selecteer de relevante actie die het programma moet ondernemen wanneer er een poging wordt gedetecteerd om bestanden in gedeelde mappen te wijzigen:
   - **Blokkeer verbinding N min**. Als Kaspersky Endpoint Security een poging tot wijziging van bestanden in gedeelde mappen detecteert wanneer deze optie is geselecteerd, blokkeert het toegang tot bestandswijziging voor de sessie die de kwaadaardige activiteit heeft gestart en maakt back-ups van de gewijzigde bestanden.

     Als het onderdeel Remediation Engine is ingeschakeld en de optie **Blokkeer verbinding N min** is geselecteerd, worden gewijzigde bestanden teruggezet vanuit back-ups.

   - **Melden**. Als deze optie is geselecteerd, voegt Kaspersky Endpoint Security bij het detecteren van een poging om bestanden in gedeelde mappen te wijzigen, informatie over deze poging toe aan de lijst met actieve bedreigingen, voegt een item toe aan lokale programma-interface rapporten en stuurt informatie over de gedetecteerde kwaadaardige activiteit naar Kaspersky Security Center.
6. Indien nodig bewerk een beschermd bereik en definieer uitzonderingen.
7. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Schakel de bescherming van gedeelde mappen tegen externe encryptie in of uit in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Host Threat Protection** → **Behavior Analysis** → **Anti-Cryptor**.
5. Gebruik de schakelaar **Anti-Cryptor ENABLED** om de detectie van activiteit die typisch is voor externe encryptie in of uit te schakelen.
6. Selecteer de relevante actie die het programma moet ondernemen wanneer er een poging wordt gedetecteerd om bestanden in gedeelde mappen te wijzigen:

   - **Block connection for (min) N min**. Als Kaspersky Endpoint Security een poging tot wijziging van bestanden in gedeelde mappen detecteert wanneer deze optie is geselecteerd, blokkeert het toegang tot bestandswijziging voor de sessie die de kwaadaardige activiteit heeft gestart en maakt back-ups van de gewijzigde bestanden.

     Als het onderdeel Remediation Engine is ingeschakeld en de optie **Block connection for (min) N min** is geselecteerd, worden gewijzigde bestanden teruggezet vanuit back-ups.

   - **Inform**. Als deze optie is geselecteerd, voegt Kaspersky Endpoint Security bij het detecteren van een poging om bestanden in gedeelde mappen te wijzigen, informatie over deze poging toe aan de lijst met actieve bedreigingen, voegt een item toe aan lokale programma-interface rapporten en stuurt informatie over de gedetecteerde kwaadaardige activiteit naar Kaspersky Security Center.
7. Indien nodig bewerk een beschermd bereik en definieer uitzonderingen.
8. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Schakel de beveiliging van gedeelde mappen tegen externe encryptie in of uit in de programma-interface

1. Klik in het hoofdvenster van het programma op de knop ⚙.
2. Selecteer **Advanced Threat Protection** → **Anti-Cryptor** in het venster met de programma-instellingen.
3. Gebruik het selectievakje **Bescherming van gedeelde mappen tegen externe encryptie** om de detectie van activiteit die typisch is voor externe encryptie in of uit te schakelen.
4. Gebruik het selectievakje **Bescherming van gedeelde mappen tegen externe encryptie** om de detectie van activiteit die typisch is voor externe encryptie in of uit te schakelen.

5. Selecteer de relevante actie die het programma moet ondernemen wanneer er een poging wordt gedetecteerd om bestanden in gedeelde mappen te wijzigen:

   - **Verbinding blokkeren voor (min) N min**. Als Kaspersky Endpoint Security een poging tot wijziging van bestanden in gedeelde mappen detecteert wanneer deze optie is geselecteerd, blokkeert het toegang tot bestandswijziging voor de sessie die de kwaadaardige activiteit heeft gestart en maakt back-ups van de gewijzigde bestanden.

     Als het onderdeel Remediation Engine is ingeschakeld en de optie **Verbinding blokkeren voor (min) N min** is geselecteerd, worden gewijzigde bestanden teruggezet vanuit back-ups.

   - **Melden**. Als deze optie is geselecteerd, voegt Kaspersky Endpoint Security bij het detecteren van een poging om bestanden in gedeelde mappen te wijzigen, informatie over deze poging toe aan de lijst met actieve bedreigingen, voegt een item toe aan lokale programma-interface rapporten en stuurt informatie over de gedetecteerde kwaadaardige activiteit naar Kaspersky Security Center.

6. Indien nodig bewerk een beschermd bereik en definieer uitzonderingen.

7. Sla uw wijzigingen op.

De blokkeringsperiode van een niet-vertrouwde computer configureren

Een *niet-vertrouwde computer* is een computer op afstand die zich bezighoudt met kwaadaardige activiteiten of gegevensencryptie. Kaspersky Endpoint Security blokkeert standaard de sessie van de externe gebruiker gedurende één uur. Wanneer de blokkeerperiode afloopt, verwijdert Kaspersky Endpoint Security de computer van de blokkeerlijst en wordt de toegang tot de gedeelde map hersteld.

Hoe de blokkeringsperiode van een niet-vertrouwde computer configureren in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.

2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

3. Selecteer **Advanced Threat Protection** → **Anti-Cryptor** in het beleidsvenster.

4. In de **Actie bij detectie van een dreiging** blokkeren, selecteer **Blokkeer verbinding N min**.

5. Configureer de blokkeringsperiode van een niet-vertrouwde computer die zich bezighoudt met kwaadaardige activiteiten of gegevensencryptie.

6. Sla uw wijzigingen op.

Configureer de blokkeringsperiode van een niet-vertrouwde computer in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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 **Host Threat Protection** → **Behavior Analysis** → **Anti-Cryptor**.
5. Onder **Action on threat detection**, configureer de blokkeringsperiode van een niet-vertrouwde computer die zich bezighoudt met kwaadaardige activiteiten of gegevensencryptie.
6. Sla uw wijzigingen op.

Configureer de blokkeringsperiode van een niet-vertrouwde computer in de programma-interface

1. Klik in het hoofdvenster van het programma op de knop ⚙.
2. Selecteer **Advanced Threat Protection** → **Anti-Cryptor** in het venster met de programma-instellingen.
3. Selecteer in het blok **Actie bij detectie van een dreiging Verbinding blokkeren voor (min)**.
4. Configureer de blokkeringsperiode van een niet-vertrouwde computer die zich bezighoudt met kwaadaardige activiteiten of gegevensencryptie.
5. Sla uw wijzigingen op.

Als gevolg hiervan wordt de externe computer vergrendeld. Om de externe computer te ontgrendelen, kunt u Kaspersky Endpoint Security opnieuw opstarten.

beschermd bereik bewerken

Het *beschermd bereik* is een lijst met paden naar gedeelde mappen waarin Kaspersky Endpoint Security de bestandsactiviteit controleert. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de `*` en `?`-tekens bij het invoeren van een masker. Standaard identificeert het programma automatisch gedeelde mappen en controleert de bestandsactiviteit in alle mappen.

Het uitsluiten van een map van het beschermd bereik 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.

> U kunt ook computers uitsluiten waarvan externe encryptie-pogingen niet mogen worden afgehandeld.

Een beschermd bereik bewerken via de beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Advanced Threat Protection** → **Anti-Cryptor** in het beleidsvenster.
4. Selecteer in het blok **Beschermd bereik Alleen opgegeven gedeelde mappen**.
5. Klik in de lijst met mappen op **Toevoegen**.

6. Er wordt een venster geopend; in dat venster voert u het pad in naar de gedeelde map die u wilt opnemen in het beschermd bereik (bijvoorbeeld `C:\Share`).

   Gebruik een lokaal pad om een gedeelde map toe te voegen aan het beschermd bereik.

7. Klik op **OK**.

8. Definieer indien nodig uitzonderingen van de beschermd bereik:

   a. In het blok **Scanuitzonderingen**, klikt u op de knop **Op masker**.

   b. Klik in het venster op de knop **Toevoegen**.

   c. Geef in het weergegeven venster een bestandsextensie op in de indeling `*.<file extension>` of een mappad. Kaspersky Endpoint Security biedt geen ondersteuning voor de tekens `*` en `?` bij de invoer van een masker.

      Het programma ondersteunt sommige uitzonderingsextensies van bestanden niet. U kunt dus een uitzonderingen opgeven als `*.docx` or `**\Folder\**`.

   U kunt een object uitsluiten van scans zonder het te verwijderen uit de lijst met objecten in het beschermd bereik. Schakel hiervoor het selectievakje naast het object uit.

9. Sla uw wijzigingen op.

Een beschermd bereik bewerken via de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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 **Host Threat Protection** → **Behavior Analysis** → **Anti-Cryptor**.

5. Selecteer in het blok **Protection scope Only specified shared folders**.

6. Klik in de lijst met mappen op **Add**.

7. Er wordt een venster geopend; in dat venster voert u het pad in naar de gedeelde map die u wilt opnemen in het beschermd bereik (bijvoorbeeld `C:\Share`).

   Gebruik een lokaal pad om een gedeelde map toe te voegen aan het beschermd bereik.

8. Klik op **OK**.

9. Definieer indien nodig uitzonderingen van de beschermd bereik:

   a. Klik in het bovenste gedeelte van het venster op de link **Scan exclusions**.

   b. Klik in het venster op de knop **Add**.

c. Geef in het weergegeven venster een bestandsextensie op in de indeling `*.<file extension>` of een mappad. Kaspersky Endpoint Security biedt geen ondersteuning voor de tekens `*` en `?` bij de invoer van een masker.

Het programma ondersteunt sommige uitzonderingsextensies van bestanden niet. U kunt dus een uitzonderingen opgeven als `*.docx` or `**\Folder\**`.

U kunt een object uitsluiten van scans zonder het te verwijderen uit de lijst met objecten in het beschermd bereik. Schakel hiervoor het selectievakje naast het object uit.

10. Sla uw wijzigingen op.

Een scanbereik bewerken via de programma-interface

1. Klik in het hoofdvenster van het programma op de knop ⚙.
2. Selecteer **Advanced Threat Protection** → **Anti-Cryptor** in het venster met de programma-instellingen.
3. Selecteer in het blok **Beschermd bereik Alleen opgegeven gedeelde mappen**.
4. Klik in de lijst met mappen op **Toevoegen**.
5. Er wordt een venster geopend; in dat venster voert u het pad in naar de gedeelde map die u wilt opnemen in het beschermd bereik (bijvoorbeeld `C:\Share`).

> Gebruik een lokaal pad om een gedeelde map toe te voegen aan het beschermd bereik.

6. Klik op **OK**.
7. Definieer indien nodig uitzonderingen van de beschermd bereik:

a. Klik in het bovenste gedeelte van het venster op de link **Uitzonderingen door masker**.

b. Klik in het venster op de knop **Toevoegen**.

c. Geef in het weergegeven venster een bestandsextensie op in de indeling `*.<file extension>` of een mappad. Kaspersky Endpoint Security biedt geen ondersteuning voor de tekens `*` en `?` bij de invoer van een masker.

Het programma ondersteunt sommige uitzonderingsextensies van bestanden niet. U kunt dus een uitzonderingen opgeven als `*.docx` or `**\Folder\**`.

U kunt een object uitsluiten van scans zonder het te verwijderen uit de lijst met objecten in het beschermd bereik. Schakel hiervoor het selectievakje naast het object uit.

8. Sla uw wijzigingen op.

1. Klik in het hoofdvenster van het programma op de knop ⚙.
2. Selecteer **Algemene instellingen** → **Uitzonderingen en types van detectie van objecten** 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 verwijderen. 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:\Folder\**\*.txt` omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen bevinden genest in de `Folder`, uitgezonderd de `Folder` 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:\Folder\???.txt` omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam `Folder` bevinden, die een TXT-extensie hebben en die een naam met drie tekens hebben.

   U kunt maskers gebruiken aan het begin, in het midden of aan het einde van het bestandspad. Als u bijvoorbeeld een map voor alle gebruikers aan uitzonderingen wilt toevoegen, voert u het masker `?:\Users\*\Folder\` in.

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.

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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 het gedeelte **Trusted Zone**.

5. Klik in het venster op de link **Malware 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 exclusions** 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. En, wanneer dit selectievakje uitgeschakeld is, verbergt Kaspersky Endpoint Security de geconsolideerde lijst met scanuitzonderingen in de gebruikersinterface van het programma.

8. Klik **Add** en selecteer een actie:

   - **Category**. U kunt scanuitzonderingen groeperen in afzonderlijke categorieën. Om een nieuwe categorie te maken, voer de naam van de categorie in en voeg ten minste één scanuitzonderingen toe aan de categorie.
   - **New exclusion**. Kaspersky Endpoint Security voegt een nieuwe scanuitzondering toe aan de hoofdmap van de lijst.
   - **Select exclusion from list**. Om Kaspersky Endpoint Security snel te configureren op SQL-servers, Microsoft Exchange-servers en System Center Configuration Manager, bevat het programma: *vooraf gedefinieerde scanuitzonderingen*. Er zijn ook vooraf gedefinieerde scanuitzonderingen toegevoegd om de installatie van progromma's in virtuele Citrix- en VMware-omgevingen te ondersteunen. U moet vooraf gedefinieerde scanuitzonderingen selecteren, afhankelijk van het doel van de beveiligde server.

9. Selecteer hoe u de uitzondering wil toevoegen **Path to the file or folder**.

10. Voer het pad naar de gedeelde map in.

    U kunt het pad ook handmatig verwijderen. 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:\Folder\**\*.txt` omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen bevinden genest in de `Folder`, uitgezonderd de `Folder` 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:\Folder\???.txt` omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam `Folder` bevinden, die een TXT-extensie hebben en die een naam met drie tekens hebben.

    U kunt maskers gebruiken aan het begin, in het midden of aan het einde van het bestandspad. Als u bijvoorbeeld een map voor alle gebruikers aan uitzonderingen wilt toevoegen, voert u het masker `C:\Users\*\Folder\` in.

11. Selecteer in het blok **Apply exclusion to** het onderdeel **Behavior Detection**.

12. Typ indien nodig in het veld **Comment** een korte opmerking over de scanuitzondering die u maakt.

13. Selecteer de status **Add to exclusions** voor de uitzondering.

    U kunt de schakelaar gebruiken om een uitzondering op elk moment te stoppen.

14. Sla uw wijzigingen op.

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.

2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

3. Selecteer **Algemene instellingen** → **Uitzonderingen en objecttypen** in het beleidsvenster.

4. In het blok **Scanuitzonderingen en vertrouwde programma's** → **Scanuitzonderingen**, klikt u op de knop **Instellingen**.

   Met een klik op deze koppeling opent u een venster waarin u een lijst met uitzonderingen vindt.

5. Schakel het selectievakje **Waarden samenvoegen bij overname** 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.

6. Schakel het selectievakje **Gebruik van lokale uitzonderingen toestaan** 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. En, wanneer dit selectievakje uitgeschakeld is, verbergt Kaspersky Endpoint Security de geconsolideerde lijst met scanuitzonderingen in de gebruikersinterface van het programma.

7. Klik **Toevoegen** en selecteer een actie:

   - **Categorie**. U kunt scanuitzonderingen groeperen in afzonderlijke categorieën. Om een nieuwe categorie te maken, voer de naam van de categorie in en voeg ten minste één scanuitzonderingen toe aan de categorie.

   - **Nieuwe uitzondering**. Kaspersky Endpoint Security voegt een nieuwe scanuitzondering toe aan de hoofdmap van de lijst.

   - **Selecteer uitzonderingen uit lijst**. Om Kaspersky Endpoint Security snel te configureren op SQL-servers, Microsoft Exchange-servers en System Center Configuration Manager, bevat het programma: *vooraf gedefinieerde scanuitzonderingen*. Er zijn ook vooraf gedefinieerde scanuitzonderingen toegevoegd om de installatie van progromma's in virtuele Citrix- en VMware-omgevingen te ondersteunen. U moet vooraf gedefinieerde scanuitzonderingen selecteren, afhankelijk van het doel van de beveiligde server.

8. Klik op **Toevoegen**.

9. Schakel in het blok **Eigenschappen** het selectievakje **Bestand of map** in.

10. Klik op de link **Selecteer bestand of map** 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.

11. Klik op **Bladeren** en selecteer de gedeelde map.

U kunt het pad ook handmatig verwijderen. 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:\Folder\**\*.txt` omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen bevinden genest in de `Folder`, uitgezonderd de `Folder` 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:\Folder\???.txt` omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam `Folder` bevinden, die een TXT-extensie hebben en die een naam met drie tekens hebben.

U kunt maskers gebruiken aan het begin, in het midden of aan het einde van het bestandspad. Als u bijvoorbeeld een map voor alle gebruikers aan uitzonderingen wilt toevoegen, voert u het masker `?:\Users\*\Folder\` in.

12. Typ indien nodig in het veld **Opmerking** een korte opmerking over de scanuitzondering die u maakt.

13. Klik op de link in de **Beschrijving van scanuitzondering (klik op de onderstreepte items om ze te bewerken)** blok om de **Beschermingsonderdelen** venster te openen.

14. Schakel het selectievakje in naast de **Gedragsdetectie** onderdeel.

15. Sla uw wijzigingen op.

Vertrouwde computers toevoegen voor externe gegevensencryptie

Als uw organisatie externe gegevensencryptie gebruikt in de workflow bestandsuitwisseling, moet u een lijst met vertrouwde computers maken. Kaspersky Endpoint Security houdt geen toezicht op gegevensencryptie door vertrouwde computers.

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.

Het wijzigen van de lijst met vertrouwde computers wordt mogelijk geblokkeerd door de eigenschappen van het bovenliggende beleid. Om de lijst te wijzigen, moet u toestaan dat de instellingen van vertrouwde zone in de Webconsole (het "hangslot" moet ontgrendeld zijn).

Vertrouwde zones zijn verschillend gegroepeerd in de Beheerconsole (MMC) en de Webconsole. Ook de manier waarop wijziging in de parameters voor de vertrouwde zone worden voorkomen, verschilt (verschillende "hangsloten"). We raden aan dat u alleen de Webconsole gebruikt om het programma te beheren. Als u de vertrouwde zone in verschillende consoles configureert, kan de beheerplug-in het "hangslot" terugzetten naar de standaardstatus.

Een vertrouwde computer toevoegen voor externe gegevensencryptie in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Advanced Threat Protection** → **Anti-Cryptor** in het beleidsvenster.
4. In het blok **Scanuitzonderingen**, klikt u op de knop **Op naam of IP-adres**.
5. Klik in het venster op de knop **Op naam of IP-adres**.
6. Voer IP-adressen, IP-adresbereiken of namen van computers in waarvan externe encryptie-pogingen niet mogen worden verwerkt.

   Voorbeelden:

   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`

- `192.168.2-3.0-128`
- `2001:db8:fd0c::/64`
- `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`

7. Sla uw wijzigingen op.

Voeg een vertrouwde computer toe voor externe gegevensencryptie in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Host Threat Protection** → **Behavior Analysis** → **Anti-Cryptor**.
5. Klik in het bovenste gedeelte van het venster op de link **Exclusions by name or IP address**.
6. Klik in het venster op de knop **Add**.
7. Voer IP-adressen, IP-adresbereiken of namen van computers in waarvan externe encryptie-pogingen niet mogen worden verwerkt.

   Voorbeelden:

   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`

8. Sla uw wijzigingen op.

Een vertrouwde computer toevoegen voor externe gegevensencryptie in de interface van het programma

1. Klik in het hoofdvenster van het programma op de knop ⚙.
2. Selecteer **Advanced Threat Protection** → **Anti-Cryptor** in het venster met de programma-instellingen.
3. Klik in het bovenste gedeelte van het venster op de link **Uitzonderingen op naam of IP-adres**.
4. Klik in het venster op de knop **Toevoegen**.
5. Voer IP-adressen, IP-adresbereiken of namen van computers in waarvan externe encryptie-pogingen niet mogen worden verwerkt.

Voorbeelden:

- `192.168.0.0 - 192.168.255.255`
- `192.168.0.0/24`
- `192.168.2-3.0-128`
- `2001:db8:fd0c::/64`
- `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`

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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Advanced Threat Protection** → **Anti-Cryptor** in het beleidsvenster.
4. In het blok **Scanuitzonderingen**, klikt u op de knop **Op naam of IP-adres**.
5. 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 knop → **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.
6. De lijst met uitzonderingen importeren:
   a. Klik op de knop → **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.

7. Sla uw wijzigingen op.

Een lijst met uitzonderingen exporteren en importeren in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Host Threat Protection** → **Behavior Analysis** → **Anti-Cryptor**.
5. Klik op de koppeling **Exclusions by name or IP address**.
6. De lijst met regels exporteren:

   a. Selecteer de uitzonderingen die u wilt exporteren.

   b. Klik op de knop → **Export**.

   Kaspersky Endpoint Security exporteert de lijst met uitzonderingen naar een JSON-bestand in de standaard downloadmap.
7. De lijst met uitzonderingen importeren:

   a. Klik op de knop → **Import**.

   Selecteer in het geopende venster het JSON-bestand waaruit u de lijst met uitzonderingen wil importeren.

   b. 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 JSON-bestand.
8. Sla uw wijzigingen op.

Remediation Engine

Via het onderdeel 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 geïnfiltreerd.
- 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 malwarescan.

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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Advanced Threat Protection** → **Remediation Engine** in het beleidsvenster.
4. Gebruik het selectievakje **Remediation Engine** om het onderdeel in of uit te schakelen.
5. Sla uw wijzigingen op.

Het onderdeel Remediation Engine in- of uitschakelen in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Host Threat Protection** → **Behavior Analysis** → **Remediation Engine**.
5. Gebruik de schakelaar **Remediation Engine ENABLED** 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.

KSN-functionaliteit is mogelijk niet beschikbaar in het programma in de Verenigde Staten.

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 het Kaspersky Security Network, voorzien de KSN-services Kaspersky Endpoint Security van informatie over de reputatie van gescande webadressen, evenals informatie over de categorie en reputatie van gescande bestanden. Voor meer informatie over het configureren van de toegang tot KSN raadpleeg de Help van Kaspersky Security Center.

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.

De infrastructuur van Kaspersky-reputatiedatabases

Kaspersky Endpoint Security ondersteunt de volgende infrastructuuroplossingen voor het werken met Kaspersky-reputatiedatabases:

- *Kaspersky Security Network (KSN)* is de oplossing die door de meeste Kaspersky-programma's wordt gebruikt. Deelnemers aan KSN ontvangen informatie van Kaspersky 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-databases die reputatie-informatie en statistische gegevens bevatten.
- *Kaspersky Private Security Network (KPSN)* is een oplossing waarmee gebruikers van computers waarop Kaspersky Endpoint Security of andere Kaspersky-programma's worden gehost toegang krijgen tot reputatiedatabases van Kaspersky en tot andere statistische gegevens zonder gegevens naar Kaspersky te versturen vanaf hun eigen computers. KPSN 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.

Het gebruik van Kaspersky Security Network inschakelen en uitschakelen

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.

KSN-gebruik in- of uitschakelen in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Advanced Threat Protection** → **Kaspersky Security Network** in het beleidsvenster.
4. 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.
5. Schakel indien nodig het selectievakje **Uitgebreide KSN-modus inschakelen** uit. De uitgebreide KSN-modus is standaard ingeschakeld.
6. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

KSN-gebruik in- of uitschakelen in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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** → **Kaspersky Security Network**.
5. Gebruik de schakelaar **Use of Kaspersky Security Network (KSN) ENABLED** 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.
6. Zet indien nodig de schakelaar **Use extended KSN mode** uit. De uitgebreide KSN-modus is standaard ingeschakeld.
7. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

KSN-gebruik in- of uitschakelen in de programma-interface

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.
4. Zet indien nodig de schakelaar **Uitgebreide KSN-modus inschakelen** uit. De uitgebreide KSN-modus is standaard ingeschakeld.
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 Kaspersky Private Security Network

Kaspersky Private Security Network (KPSN) is een oplossing waarmee gebruikers van computers waarop Kaspersky Endpoint Security of andere Kaspersky-programma's worden gehost toegang krijgen tot reputatiedatabases van Kaspersky en tot andere statistische gegevens zonder gegevens naar Kaspersky te versturen vanaf hun eigen computers. Met Kaspersky Private Security Network 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 werklast. De lijst met relevante indelingen en groottelimieten 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.

- Kaspersky Endpoint Security in de Light Agent-modus communiceert met KSN-servers via een KSN-proxyserver. Directe communicatie met KSN wordt niet ondersteund.

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.

Als het programma in Light Agent-modus werkt, is de Cloud-modus niet beschikbaar.

Het onderdeel cloudmodus voor beschermingsonderdelen in- of uitschakelen in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.

2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

3. Selecteer **Advanced Threat Protection** → **Kaspersky Security Network** in het beleidsvenster.

4. Gebruik het selectievakje **Cloudmodus inschakelen** om het onderdeel in of uit te schakelen.
5. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Het onderdeel cloudmodus voor beschermingsonderdelen in- of uitschakelen in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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** → **Kaspersky Security Network**.
5. Gebruik de schakelaar **Use cloud mode** om de component in of uit te schakelen.
6. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Het onderdeel cloudmodus voor beschermingsonderdelen in de programma-interface 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 **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 rechtstreeks of via de service KSN Proxy met KSN communiceren.

Als het programma in Light Agent-modus draait, wordt directe communicatie met KSN niet ondersteund. Kaspersky Endpoint Security communiceert met KSN-servers via een KSN proxyserver.

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 raadpleeg de Help van Kaspersky Security Center. U kunt KSN Proxy ook in- of uitschakelen voor individuele computers in het Kaspersky Endpoint Security-beleid.

KSN Proxy inschakelen of uitschakelen in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Advanced Threat Protection** → **Kaspersky Security Network** in het beleidsvenster.
4. Gebruik in het blok **Instellingen voor KSN-proxy** het selectievakje **Gebruik Administration Server als een KSN-proxyserver** om KSN Proxy in of uit te schakelen.
5. Schakel indien nodig het selectievakje **Gebruik Kaspersky Security Network-servers als de KSN-proxyserver niet beschikbaar is** in.

   Als het selectievakje is ingeschakeld, gebruikt Kaspersky Endpoint Security KSN-servers wanneer de KSN Proxy service niet beschikbaar is. KSN-servers kunnen zowel van Kaspersky als van derden (wanneer privaat KSN wordt gebruikt) zijn.
6. Sla uw wijzigingen op.

KSN-proxy inschakelen of uitschakelen in de webconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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** → **Kaspersky Security Network**.
5. Gebruik het selectievakje **Use Administration Server as a KSN proxy server** om het KSN Proxy in of uit te schakelen.

6. Schakel indien nodig het selectievakje **Use Kaspersky Security Network servers if the KSN proxy server is unavailable** in.

   Als het selectievakje is ingeschakeld, gebruikt Kaspersky Endpoint Security KSN-servers wanneer de KSN Proxy service niet beschikbaar is. KSN-servers kunnen zowel van Kaspersky als van derden (wanneer privaat KSN wordt gebruikt) zijn. Het selectievakje is standaard uitgeschakeld.

7. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en 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 Proxy adres handmatig bijwerken.

Het KSN Proxy-adres configureren:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de consolestructuur de map **Advanced** → **Remote installation** → **Installation packages**.
3. Selecteer in het contextmenu van het de map met het **Properties** de optie **Installation packages**.
4. Op het tabblad **General** in het geopende venster, specificeert u het nieuwe adres van de KSN-proxyserver.
5. 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 toepassing beschouwt een bestand als vertrouwd als aan een of meer van de volgende voorwaarden wordt voldaan:

- het bestand is digitaal ondertekend door een vertrouwde leverancier;
- het bestand heeft een vertrouwde reputatie in Kaspersky Security Network;
- de gebruiker heeft het bestand in de groep 'Vertrouwd' geplaatst.

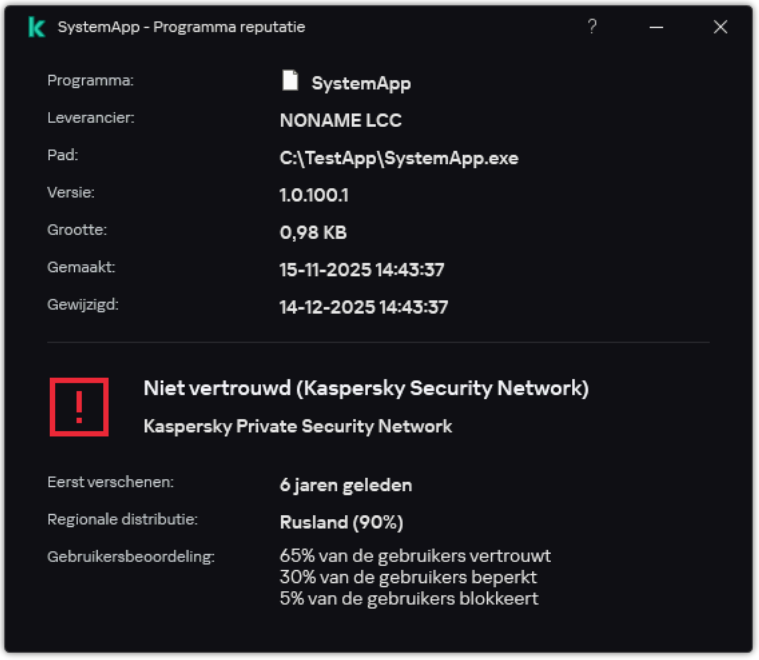
Legitieme software die hackers kunnen gebruiken om de computer of persoonlijke gegevens te beschadigen. Hoewel ze geen kwaadaardige functies hebben, kunnen dit soort programma's door indringers worden gebruikt als een hulpmiddel. Voor informatie over legitieme software die criminelen kunnen gebruiken 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.

Niet 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: *Kaspersky Security Network* of *Kaspersky Private Security Network*.

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, Web Threat Protection, Gedragsdetectie en Exploit-preventie 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

Standaard scant Kaspersky Endpoint Security niet altijd versleutelde verbindingen, maar alleen wanneer de beschermingsonderdelen daarom vragen.

Versleutelde verbindingen scannen inschakelen in de Beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de beheerconsole **Policies**.
3. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
4. Selecteer **Algemene instellingen** → **Netwerkinstellingen** in het beleidsvenster.
5. Selecteer in het blok **Scan van geëncrypte verbindingen** de modus voor het scannen van versleutelde verbindingen:
   - **Geëncrypte verbindingen scannen**. Kaspersky Endpoint Security heeft geen toegang tot de inhoud van websites waarvan het adres begint met `https://`.
   - **Geëncrypte verbindingen scannen op verzoek van beschermingsonderdelen**. Kaspersky Endpoint Security scant versleuteld verkeer alleen wanneer daarom wordt gevraagd door de onderdelen Web Threat Protection, Mail Threat Protection en Web Control.
   - **Geëncrypte 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.

6. Voeg indien nodig scanuitzonderingen toe: vertrouwde adressen en programma's.
7. Configureer de instellingen voor het scannen van versleutelde verbindingen (zie onderstaande tabel).
8. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Versleutelde verbindingen scannen inschakelen in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de Webconsole het tabblad **Asset management** → **Policies**.
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** → **Network Settings**.
5. Schakel onder **Encrypted Connections Scan** de schakelaar **Encrypted Connections Scan ENABLED** aan.

   Als de schakelknop is uitgeschakeld, heeft Kaspersky Endpoint Security geen toegang tot de inhoud van websites waarvan het adres begint met `https://`.
6. Klik op **Settings** en selecteer de modus voor het scannen van versleutelde verbindingen:

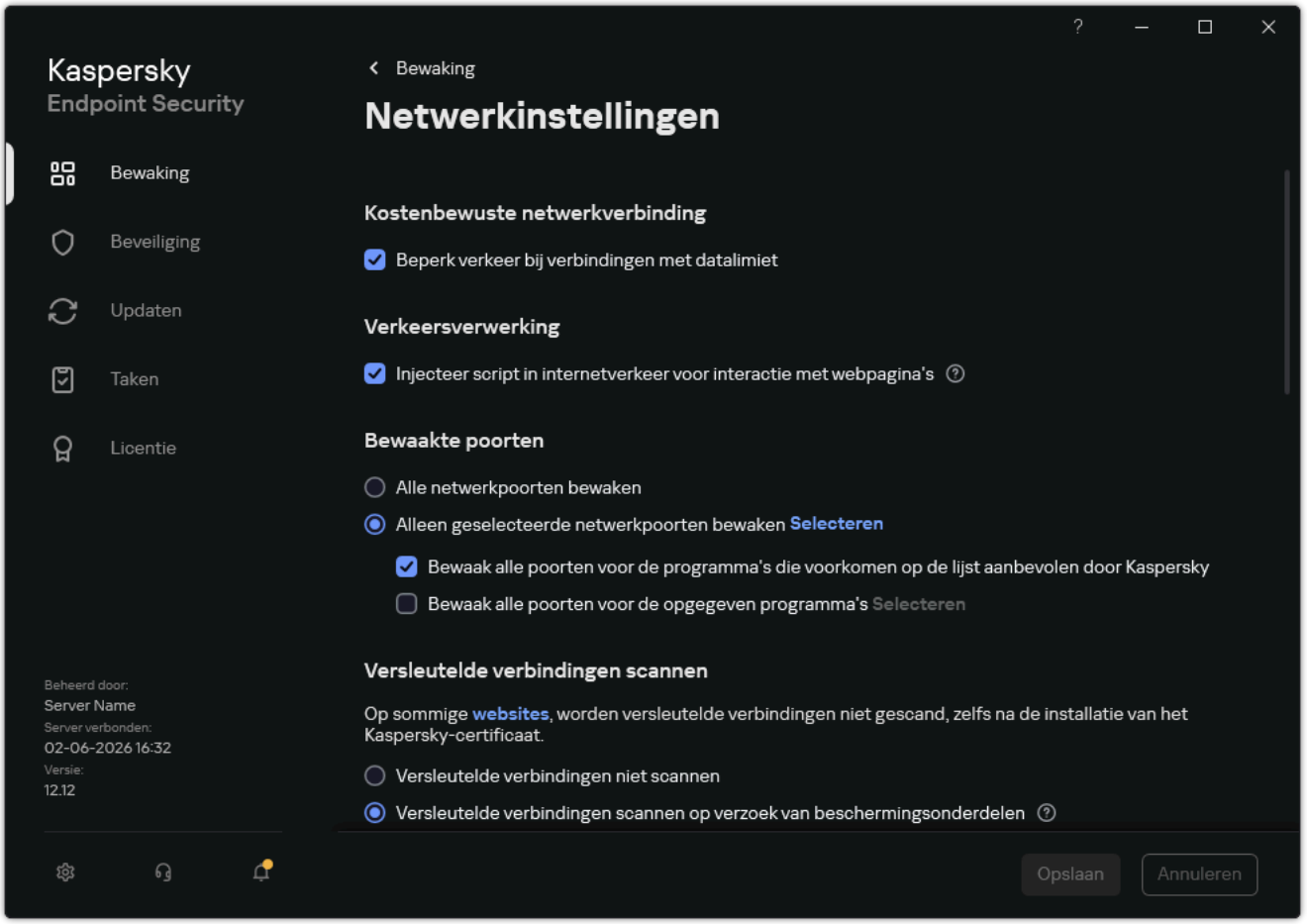
   - **Scan encrypted connections upon request from protection components**. Kaspersky Endpoint Security scant versleuteld verkeer alleen wanneer daarom wordt gevraagd door de onderdelen Web Threat Protection, Mail Threat Protection en Web Control.
   - **Always scan encrypted connections**. Kaspersky Endpoint 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.

7. Voeg indien nodig scanuitzonderingen toe: vertrouwde adressen en programma's.
8. Configureer de instellingen voor het scannen van versleutelde verbindingen (zie onderstaande tabel).
9. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Versleutelde verbindingen scannen inschakelen 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.



Instellingen voor het scannen van versleutelde verbindingen

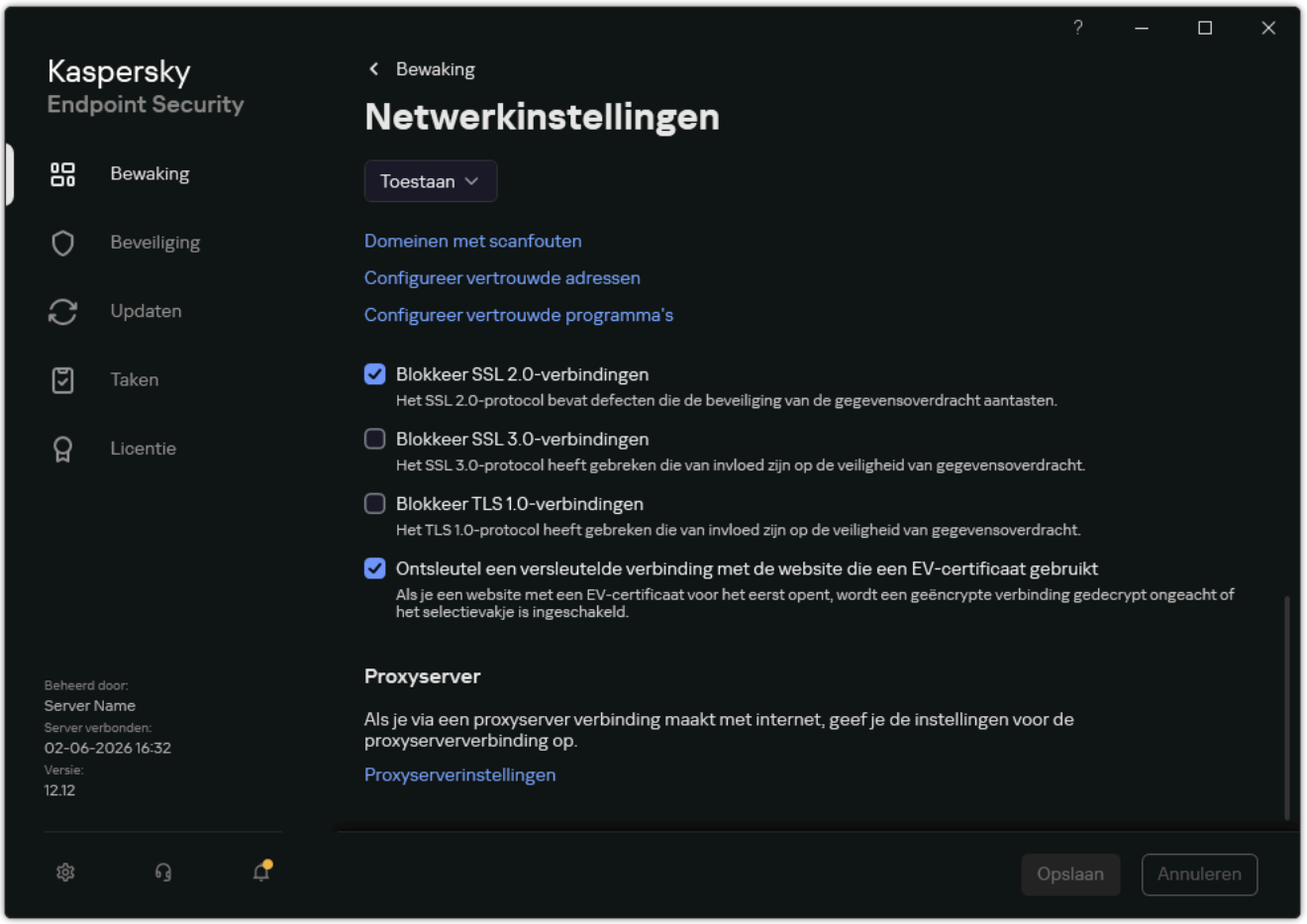
3. Selecteer in het blok **Versleutelde verbindingen scannen** de modus voor het scannen van versleutelde verbindingen:

   - **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 Web 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 scanuitzonderingen toe: vertrouwde adressen en programma's.

5. Configureer de instellingen voor het scannen van versleutelde verbindingen (zie onderstaande tabel).



Aanvullende instellingen voor het scannen van versleutelde verbindingen

6. Sla uw wijzigingen op.

Parameter	Beschrijving
Vertrouwde basiscertificaten	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 verbindingsfout krijgen vanwege een certificaatprobleem. Als u wilt toevoegen aan het systeemcertificaatarchief, kunt u het groepsbeleid van Active Directory gebruiken.
Een domein bezoeken met een niet-vertrouwd certificaat	• **Toestaan**. 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 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 *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. • **Blokkeren**. 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.
Een domein bezoeken met een scanfout met geëncrypte verbindingen	• **Blokkeren**. Als een fout tijdens het scannen van een beveiligde verbinding optreedt, blokkeert Kaspersky Endpoint Security de netwerkverbinding. • **Toestaan en domein toevoegen aan uitzonderingen**. Als 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 **Blokkeren** selecteren. Kaspersky Endpoint Security genereert ook een gebeurtenis voor de fout bij het scannen van de versleutelde verbinding.
Blokkeer SSL 2.0-verbindingen	Als het selectievakje is ingeschakeld, bewaakt en blokkeert het programma netwerkverbindingen die via het SSL 2.0-protocol tot stand zijn gebracht. Als het selectievakje is uitgeschakeld, bewaakt of blokkeert het programma netwerkverbindingen die via het SSL 2.0-protocol tot stand zijn gebracht. Het programma bewaakt echter geen netwerkverkeer via dit protocol.
Blokkeer SSL 3.0-verbindingen	Als het selectievakje is ingeschakeld, blokkeert het programma netwerkverbindingen die via het SSL 3.0-protocol tot stand zijn gebracht. Als het selectievakje is uitgeschakeld, bewaakt of blokkeert het programma netwerkverbindingen die via het SSL 3.0-protocol tot stand zijn gebracht. Het programma bewaakt het netwerkverkeer via dit protocol. Alle onderdelen van het programma werken zonder beperkingen.
Blokkeer TLS 1.0-verbindingen	Als het selectievakje is ingeschakeld, blokkeert het programma netwerkverbindingen die via het TLS 1.0-protocol tot stand zijn gebracht. Als het selectievakje is uitgeschakeld, bewaakt of blokkeert het programma netwerkverbindingen die via het TLS 1.0-protocol tot stand zijn gebracht. Het programma bewaakt het netwerkverkeer via dit protocol. Alle onderdelen van het programma werken zonder beperkingen.
Ontsleutel een versleutelde verbinding met de website die een EV-certificaat gebruikt	EV-certificaten (Extended Validation Certificate) 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. Als het selectievakje is ingeschakeld, decrypt en bewaakt het programma geëncrypte verbindingen met websites die een EV-certificaat gebruiken. Als het selectievakje is uitgeschakeld, heeft het programma geen toegang tot de inhoud van HTTPS-verkeer. Om deze reden bewaakt het programma HTTPS-verkeer alleen op basis van het webadres, zoals `https://bing.com`. Als u een website met een EV-certificaat voor het eerst opent, wordt de beveiligde verbinding gedecrypt ongeacht of het selectievakje is ingeschakeld.

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 verbindingsfout krijgen vanwege een certificaatprobleem. Als u wilt toevoegen aan het systeemcertificaatarchief, kunt u het groepsbeleid van Active Directory gebruiken.

Het wijzigen van de lijst met vertrouwde basiscertificaten wordt mogelijk geblokkeerd door de eigenschappen van het bovenliggende beleid. Om de lijst te wijzigen, moet u toestaan dat de instellingen van vertrouwde zone in de Webconsole (het "hangslot" moet ontgrendeld zijn).

Vertrouwde zones zijn verschillend gegroepeerd in de Beheerconsole (MMC) en de Webconsole. Ook de manier waarop wijziging in de parameters voor de vertrouwde zone worden voorkomen, verschilt (verschillende "hangsloten"). We raden aan dat u alleen de Webconsole gebruikt om het programma te beheren. Als u de vertrouwde zone in verschillende consoles configureert, kan de beheerplug-in het "hangslot" terugzetten naar de standaardstatus.

Hoe installeer ik vertrouwde rootcertificaten in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Algemene instellingen** → **Netwerkinstellingen** in het beleidsvenster.
4. In het blok **Vertrouwde basiscertificaten**, klikt u op de knop **Toevoegen**.
5. Dit opent een venster; selecteer in dat venster een vertrouwd rootcertificaat.

   Kaspersky Endpoint Security ondersteunt certificaten met PEM-, der- en CRT-extensies.
6. Sla uw wijzigingen op.

Vertrouwde rootcertificaten installeren in Webconsole en Cloud Console

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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** → **Network Settings**.
5. Klik op de koppeling **Trusted root certificates**.

6. Dit opent een venster, klik in dat venster op **Add** 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. In het blok **Versleutelde verbindingen scannen**, klikt u op de knop **Certificaten tonen**.
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-waarschuwingspagina 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.

  In sommige gevallen kan Kaspersky Endpoint Security technisch gezien geen HTML-pagina met een waarschuwing weergeven in de browser (zie onderstaande afbeelding). Bijvoorbeeld als een webbron een verouderde versie van een netwerkprotocol en een niet-standaard poort gebruikt. In deze gevallen blokkeert Kaspersky Endpoint Security de toegang tot dit domein en toont de browser het standaardvenster `ERR_CONNECTION_RESET`. Om toegang te krijgen tot een webbron, kunt u domein toevoegen aan uitsluitingen of een vertrouwd certificaat gebruiken.

- 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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Algemene instellingen** → **Netwerkinstellingen** in het beleidsvenster.
4. In het blok **Scan van geëncrypte verbindingen**, klikt u op de knop **Geavanceerde instellingen**.
5. Selecteer in het venster dat opent de uitvoermodus van het programma wanneer u een domein bezoekt met een niet-vertrouwd certificaat: **Toestaan** of **Blokkeren**.
6. Sla uw wijzigingen op.

Het scannen van versleutelde verbindingen configureren met een niet-vertrouwd certificaat in Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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** → **Network Settings**.
5. Klik in het blok **Encrypted Connections Scan** op de koppeling **Settings**.
6. Selecteer in het venster dat opent de uitvoermodus van het programma wanneer u een domein bezoekt met een niet-vertrouwd certificaat: **Allow connection** of **Block connection**.
7. 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 in het blok **Versleutelde verbindingen scannen** de uitvoermodus van het programma wanneer u een domein bezoekt met een niet-vertrouwd certificaat: **Toestaan** of **Blokkeren**.
4. Sla uw wijzigingen op.



Waarschuwing over een bezoek aan een domein met een niet-vertrouwd certificaat

Kaspersky-certificaat toevoegen aan het eigen certificatenarchief

Browsers en e-mailprogramma's gebruiken het certificaat om de veiligheid en authenticiteit van webbronnen te verifiëren. Het certificaat biedt ook gegevensversleuteling tussen webbronnen en de gebruiker. De meeste browsers en e-mailprogramma's gebruiken het vertrouwde certificatenarchief (Windows certificate store). Bijvoorbeeld Google Chrome. Sommige browsers en e-mailprogramma's gebruiken standaard hun eigen certificatenarchief in plaats van het certificatenarchief van Windows. Bijvoorbeeld Firefox enThunderbird.

Na installatie voegt Kaspersky Endpoint Security een Kaspersky-certificaat toe aan de systeemopslag voor vertrouwde certificaten (Windows-certificaatarchief). Als Kaspersky Security Center is geïmplementeerd in uw organisatie en er wordt een beleid toegepast op een computer, maakt Kaspersky Endpoint Security automatisch het gebruik van het Windows-certificaatarchief 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 het certificaatarchief kiezen dat wordt gebruikt door browsers e-mailprogramma's. Als u het eigen certificaatarchief hebt geselecteerd, voegt u het Kaspersky-certificaat handmatig toe aan het archief. 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 het programma geen versleuteld verkeer in de Mozilla Firefox-browser en Thunderbird-mailclient. Het scannen van versleutelde verbindingen moet ook worden ingeschakeld om verkeer in MyOffice Mail en R7-Office Organizer e-mailprogramma's te scannen.

Voordat u een certificaat toevoegt aan het eigen certificaatarchief van de browser of de e-mailagent, moet u het Kaspersky-certificaat exporteren vanuit het Configuratiescherm van Windows (Interneteigenschappen). U kunt meer te weten komen over het toevoegen van een certificaat aan het archief, bijvoorbeeld op de Mozilla-website voor technische ondersteuning.

U kunt de certificaatopslag alleen in de lokale interface van het programma kiezen.

Een certificatenarchief 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 **Versleutelde verbindingen scannen** het selectievakje **Om geëncrypte verbindingen te scannen in programma's met hun eigen certificaatopslag, gebruik** in.
4. Selecteer een certificaatarchief:
   - **Windows-certificaatarchief (aanbevolen)**. Het Kaspersky-rootcertificaat wordt aan deze opslag toegevoegd tijdens de installatie van Kaspersky Endpoint Security.
   - **Eigen certificaatopslag**. 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.

     MyOffice Mail en R7-Office Organizer mailprogramma's gebruiken ook hun eigen certificatenarchief.
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. In dit geval scant Kaspersky Endpoint Security geen HTTPS-verkeer van vertrouwde webadressen wanneer de onderdelen Web Threat Protection, Mail Threat Protection en Webcontrole hun werk doen.

Als een vertrouwde toepassing een versleutelde verbinding gebruikt, kunt 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.

Het wijzigen van de lijst met vertrouwde adressen wordt mogelijk geblokkeerd door de eigenschappen van het bovenliggende beleid. Om de lijst te wijzigen, moet u toestaan dat de instellingen van vertrouwde zone in de Webconsole (het "hangslot" moet ontgrendeld zijn).

Vertrouwde zones zijn verschillend gegroepeerd in de Beheerconsole (MMC) en de Webconsole. Ook de manier waarop wijziging in de parameters voor de vertrouwde zone worden voorkomen, verschilt (verschillende "hangsloten"). We raden aan dat u alleen de Webconsole gebruikt om het programma te beheren. Als u de vertrouwde zone in verschillende consoles configureert, kan de beheerplug-in het "hangslot" terugzetten naar de standaardstatus.

Een webadres uitsluiten van de scan van versleutelde verbindingen in de beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Algemene instellingen** → **Netwerkinstellingen** in het beleidsvenster.
4. In het blok **Scan van geëncrypte verbindingen**, klikt u op de knop **Configureer vertrouwde adressen**.
5. Klik op **Toevoegen**.
6. 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 niet het symbool `*` voor IP-adressen. U kunt een bereik van IP-adressen selecteren door een subnet masker te gebruiken (bijvoorbeeld 198.51.100.0/24).

   Voorbeelden:

   - `domain.com` – de record bevat de volgende adressen: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. De record bevat geen subdomeinen (bijvoorbeeld `subdomain.domain.com`).
   - `subdomain.domain.com` – de record bevat de volgende adressen: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. De record bevat niet het domein `domain.com`.
   - `*.domain.com` – de record bevat de volgende adressen: `https://movies.domain.com`, `https://images.domain.com/page123`. De record bevat niet het domein `domain.com`.
7. Sla uw wijzigingen op.

Een webadres uitsluiten van de scan van versleutelde verbindingen in webconsole en Cloud Console.

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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** → **Network Settings**.
5. In het blok **Encrypted Connections Scan**, klikt u op de knop **Trusted domains**.
6. Klik op **Add**.
7. 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.

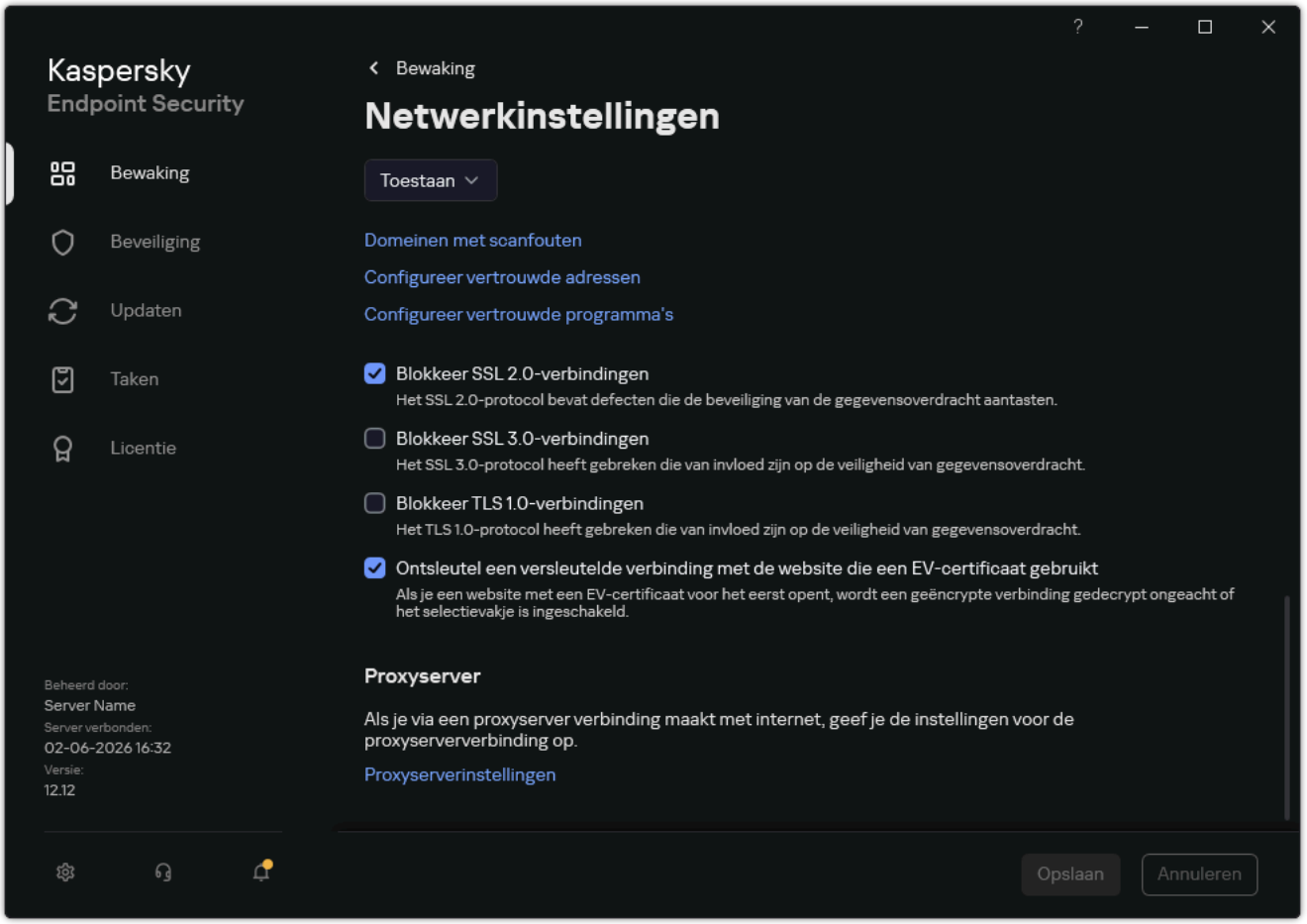
   > Kaspersky Endpoint Security ondersteunt niet het symbool `*` voor IP-adressen. U kunt een bereik van IP-adressen selecteren door een subnet masker te gebruiken (bijvoorbeeld 198.51.100.0/24).

   Voorbeelden:

   - `domain.com` – de record bevat de volgende adressen: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. De record bevat geen subdomeinen (bijvoorbeeld `subdomain.domain.com`).
   - `subdomain.domain.com` – de record bevat de volgende adressen: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. De record bevat niet het domein `domain.com`.
   - `*.domain.com` – de record bevat de volgende adressen: `https://movies.domain.com`, `https://images.domain.com/page123`. De record bevat niet het domein `domain.com`.
8. Sla uw wijzigingen op.

Een webadres uitsluiten van de scan van versleutelde verbindingen 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.



Netwerkinstellingen programma

3. In het blok **Versleutelde verbindingen scannen**, klikt u op de knop **Configureer 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 niet het symbool `*` voor IP-adressen. U kunt een bereik van IP-adressen selecteren door een subnet masker te gebruiken (bijvoorbeeld 198.51.100.0/24).

Voorbeelden:

- `domain.com` – de record bevat de volgende adressen: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. De record bevat geen subdomeinen (bijvoorbeeld `subdomain.domain.com`).
- `subdomain.domain.com` – de record bevat de volgende adressen: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. De record bevat niet het domein `domain.com`.
- `*.domain.com` – de record bevat de volgende adressen: `https://movies.domain.com`, `https://images.domain.com/page123`. De record bevat niet het domein `domain.com`.

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 geëncrypt 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 **Tasks**.

   De lijst met taken wordt geopend.

2. Klik op **Add**.

   De wizard Taak wordt gestart.

3. Configureer de taakinstellingen:

   a. Selecteer in de vervolgkeuzelijst **Application** de optie **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. Selecteer in de vervolgkeuzelijst **Task type** de optie **Wipe data**.

   c. Typ in het veld **Task name** een korte omschrijving, zoals *Gegevens wissen (Anti-Diefstal)*.

   d. Selecteer in het gedeelte **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. 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 **Wipe data** van 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 overschrijdt 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.

Houd er rekening mee bij het configureren van uitgestelde verwijdering van gegevens dat werknemers mogelijk verschillende werkschema's hebben. 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 de computer is uitgeschakeld en de verbinding is langer dan de geconfigureerde duur afwezig geweest, verwijdert Kaspersky Endpoint Security de gegevens niet onmiddellijk nadat de computer is ingeschakeld. Het programma wacht één uur op de synchronisatie met Kaspersky Security Center. Dit is nodig om te voorkomen dat onbevoegde gegevens worden verwijderd op computers van gebruikers die hun computer hebben uitgeschakeld, bijvoorbeeld voordat ze op vakantie gaan.

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:
  - **Documents**. 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).
  - **Desktop**. 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.
  - **Temporary files**. 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 files**. 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 **Start**.

    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).

Om Webcontrole te kunnen gebruiken, moet u de initiële configuratie van het programma voltooien:

- Voor de bewaking van HTTPS-verkeer, schakel het scannen van versleutelde verbindingen in (standaard ingeschakeld).
- Selecteer de poorten die: Kaspersky Endpoint Security moet monitoren (standaard bewaakt het programma alle poorten).
- Selecteer het programma waarvan u wilt dat Kaspersky Endpoint Security het verkeer bewaakt. De meeste browsers staan al in de lijst met door Kaspersky aanbevolen programma's. Als uw browser niet in de lijst staat, kunt u deze handmatig toevoegen.
- Wij adviseren om een script voor webpagina-interactie in het webverkeer te injecteren (scriptinjectie is standaard uitgeschakeld). Met dit script kunnen Webcontrole-gebeurtenissen voor het programmagebeurtenislogboek, het OS-gebeurtenislogboek en rapporten worden geregistreerd.

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 *Afbeeldingen*.

- **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-programmabestanden* 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.





Berichten van Webcontrole

Een toegangsregel voor webbronnen toevoegen

Een *toegangsregel voor webbronnen* is een reeks filters en acties die Kaspersky Endpoint Security toepast wanneer gebruikers webbronnen bezoeken. Toegangsregels kunnen een regelplanning bevatten.

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. De *Standaardregel* is vooraf ingesteld. 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.

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.

Een toegangsregel voor webbronnen toevoegen in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Security Controls** → **Webcontrole** in het beleidsvenster.
4. Selecteer het selectievakje **Webcontrole**.
5. In het blok **Instellingen van Webcontrole**, klikt u op de knop **Toevoegen**.

   Het venster **Regel voor toegang tot webbronnen** wordt geopend.
6. Configureer de toegangsregel voor webbronnen: (zie onderstaande tabel).
7. Als u wilt dat Webcontrole de verbinding met de verboden webbron verbreekt onmiddellijk nadat het beleid is toegepast, selecteer het **Beëindig actieve browsersessies van gebruikers nadat de regel is toegepast** selectievakje.

   > Met Webcontrole kunt u alleen in webbrowsers de verbinding met webbronnen onmiddellijk verbreken. Voor andere programma's beperkt Webcontrole alleen nieuwe verbindingen.

   Als het selectievakje is uitgeschakeld, beperkt Webcontrole alleen nieuwe verbindingen met verboden webbronnen. Webcontrole beëindigt geen actieve verbindingen.
8. Sla uw wijzigingen op.

Een toegangsregel voor webbronnen toevoegen in Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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**.

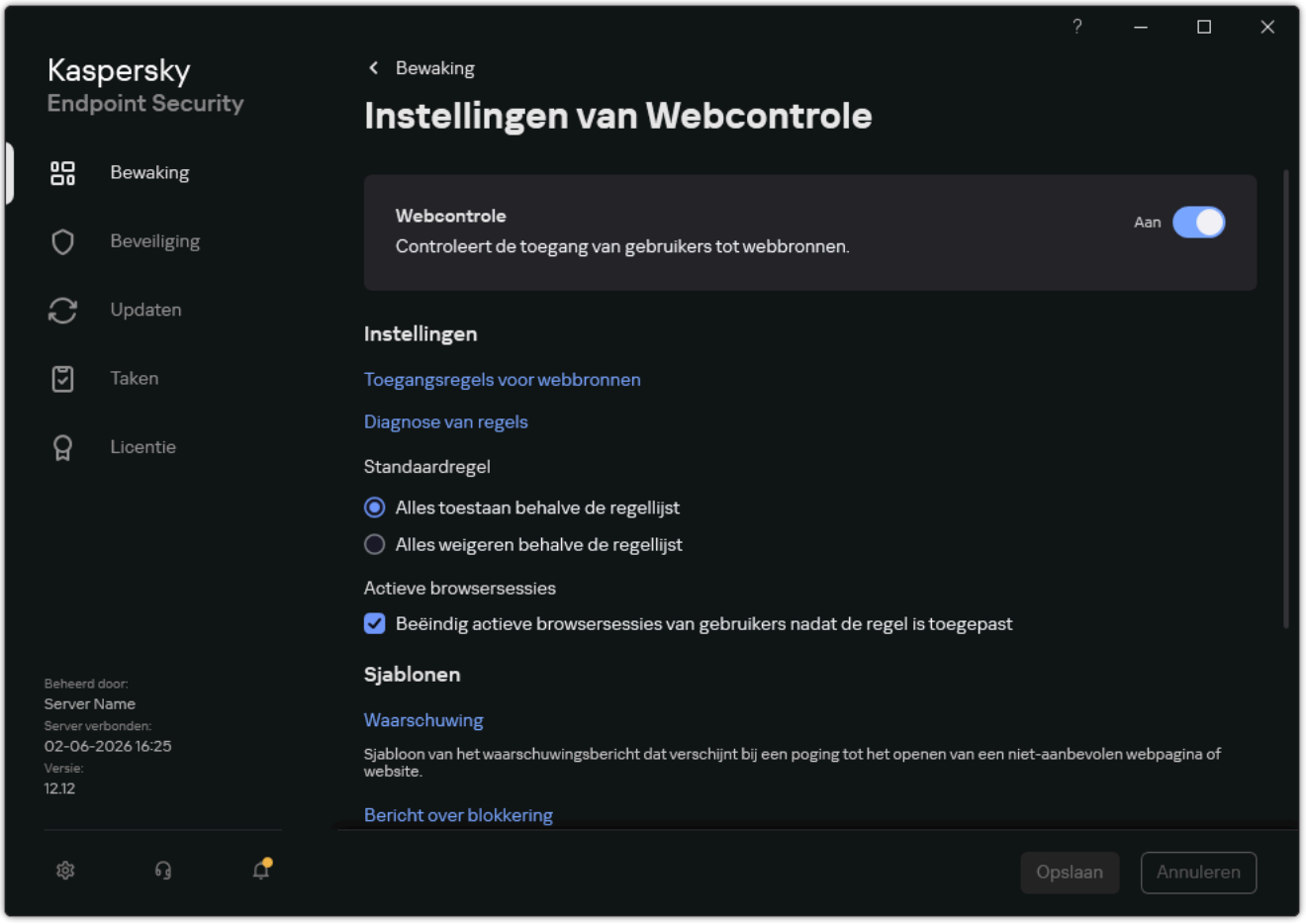
4. Ga naar **Security Controls** → **Web Control**.
5. Zet de schakelaar **Web Control ENABLED** aan.
6. In het blok **Rules list**, klikt u op de knop **Add**.
7. Configureer de toegangsregel voor webbronnen: (zie onderstaande tabel).
8. Als u wilt dat Webcontrole de verbinding met de verboden webbron verbreekt onmiddellijk nadat het beleid is toegepast, selecteer het **Terminate active user browser sessions after the rule is applied** selectievakje.

   > Met Webcontrole kunt u alleen in webbrowsers de verbinding met webbronnen onmiddellijk verbreken. Voor andere programma's beperkt Webcontrole alleen nieuwe verbindingen.

   Als het selectievakje is uitgeschakeld, beperkt Webcontrole alleen nieuwe verbindingen met verboden webbronnen. Webcontrole beëindigt geen actieve verbindingen.
9. Sla uw wijzigingen op.

Een toegangsregel voor webbronnen toevoegen in de programma-interface

1. Klik in het hoofdvenster van het programma op de knop ⚙.
2. Selecteer **Security Controls** → **Webcontrole** in het venster met de programma-instellingen.



Webcontrole Instellingen

3. Zet de schakelaar **Webcontrole** aan.
4. In het blok **Instellingen**, klikt u op de knop **Toegangsregels voor webbronnen**.

5. Klik in het venster op de knop **Toevoegen**.

   Het venster **Regel voor toegang tot webbronnen** wordt geopend.

6. Configureer de toegangsregel voor webbronnen: (zie onderstaande tabel).

7. Als u wilt dat Webcontrole de verbinding met de verboden webbron verbreekt onmiddellijk nadat het beleid is toegepast, selecteer het **Beëindig actieve browsersessies van gebruikers nadat de regel is toegepast** selectievakje.

   > Met Webcontrole kunt u alleen in webbrowsers de verbinding met webbronnen onmiddellijk verbreken. Voor andere programma's beperkt Webcontrole alleen nieuwe verbindingen.

   Als het selectievakje is uitgeschakeld, beperkt Webcontrole alleen nieuwe verbindingen met verboden webbronnen. Webcontrole beëindigt geen actieve verbindingen.

8. Sla uw wijzigingen op.

Als resultaat wordt de nieuwe Webcontrole-regel aan de lijst toegevoegd. Indien nodig, wijzig de prioriteit van de Webcontrole-regel. U kunt ook op elk gewenst moment de schakelaar gebruiken om de toegangsregel voor webbronnen uit te schakelen zonder deze uit de lijst te verwijderen.

Parameters voor Webcontrole-regel

Parameter	Beschrijving
Regelnaam	Naam van de Webcontrole-regel.
Status	• **Aan**. • **Uit**. U kunt de schakelaar gebruiken om de toegangsregel voor webbronnen op elk gewenst moment uit te schakelen.
Actie	• **Toestaan**. Webcontrole biedt toegang tot webbronnen die overeenkomen met de parameters van de regel. • **Blokkeren**. Webcontrole blokkeert de toegang tot webbronnen die overeenkomen met de parameters van de regel en geeft een bericht weer dat toegang tot de website is geweigerd. • **Waarschuwen**. Als de gebruiker toegang probeert te krijgen tot een webbron die overeenkomt met de regel, geeft Webcontrole een waarschuwing weer dat het bezoeken van de webbron af te raden is. Met de koppelingen in het waarschuwingsbericht kan de gebruiker toegang tot de opgevraagde webbron krijgen.
Inhoud van de filter	• **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 *Afbeeldingen*).
Adressen	• **Op alle adressen**. Webcontrole filtert webbronnen niet op adres. • **Op individuele adressen**. Webcontrole filtert alleen adressen van webbronnen uit de lijst. U kunt een webadres invoeren of maskers gebruiken. U kunt ook een lijst met webbronadressen exporteren vanuit een TXT-bestand. U kunt gebruikers selecteren in Active Directory, in de lijst van accounts in Kaspersky Security Center, of door handmatig een lokale gebruikersnaam in te voeren. Kaspersky raadt aan om locale gebruikersaccounts alleen in speciale gevallen te gebruiken, wanneer het niet mogelijk is om domeingebruikersaccounts te gebruiken. Als de Scan van versleutelde verbindingen is uitgeschakeld, kunt u voor het HTTPS-protocol alleen op servernaam filteren.
Gebruikers	• **Op alle gebruikers**. Webcontrole filtert geen webbronnen voor specifieke gebruikers. • **Op individuele gebruikers en/of groepen**. Webcontrole filtert webbronnen alleen voor specifieke gebruikers. U kunt gebruikers selecteren in Active Directory, in de lijst van accounts in Kaspersky Security Center, of door handmatig een lokale gebruikersnaam in te voeren. Kaspersky raadt aan om locale gebruikersaccounts alleen in speciale gevallen te gebruiken, wanneer het niet mogelijk is om domeingebruikersaccounts te gebruiken.
Regelplanning	De regelplanning bepaalt de periode wanneer Kaspersky Endpoint Security de toegang tot de opgegeven webbronnen in de regel monitort. U kunt bijvoorbeeld de internettoegang via een browser tijdens de werkuren beperken.

Filteren op adressen van webbronnen

Om de toegang tot individuele webbronnen te beheren, moet u een Webcontrole-regel maken, een lijst met webadressen maken en een Webcontrole-actie selecteren. Bij het maken van een webadressenlijst kunt u URL-adressen invoeren of maskers gebruiken.

Regels kunnen een regelplanning en een lijst met gebruikers bevatten waarop de regel van toepassing is. Bijvoorbeeld, u kunt de toegang tot websites alleen tijdens werkuren beperken of het bezoeken van websites toestaan aan gebruikers in bepaalde groepen.

Schakel een adresfilter in voor webbronnen in de beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Security Controls** → **Webcontrole** in het beleidsvenster.
4. Selecteer het selectievakje **Webcontrole**.
5. In het blok **Instellingen van Webcontrole**, klikt u op de knop **Toevoegen**.
   Het venster **Regel voor toegang tot webbronnen** wordt geopend.
6. Configureer de toegangsregel voor webbronnen:
   a. Typ in het veld **Naam** de naam van de regel.
   b. Selecteer in de vervolgkeuzelijst **Pas toe op adressen** de optie **Op individuele adressen**.
   c. Maak een lijst met vertrouwde adressen van webbronnen. U kunt een webadres invoeren of maskers gebruiken. U kunt ook een lijst met webbronadressen exporteren vanuit een TXT-bestand.

      Als de Scan van versleutelde verbindingen is uitgeschakeld, kunt u voor het HTTPS-protocol alleen op servernaam filteren.

   d. In de **Pas toe op gebruikers** vervolgkeuzelijst, selecteer de relevante filter voor gebruikers:

      - **Op alle gebruikers**. Webcontrole filtert webbronnen niet op adres.
      - **Op individuele gebruikers of groepen**. Webcontrole filtert alleen adressen van webbronnen uit de lijst. U kunt een webadres invoeren of maskers gebruiken. U kunt ook een lijst met webbronadressen exporteren vanuit een TXT-bestand. U kunt gebruikers selecteren in Active Directory, in de lijst van accounts in Kaspersky Security Center, of door handmatig een lokale gebruikersnaam in te voeren. Kaspersky raadt aan om locale gebruikersaccounts alleen in speciale gevallen te gebruiken, wanneer het niet mogelijk is om domeingebruikersaccounts te gebruiken.

e. In de **Actie** vervolgkeuzelijst, selecteer een optie:

- **Toestaan**. Webcontrole biedt toegang tot webbronnen die overeenkomen met de parameters van de regel.
- **Blokkeren**. Webcontrole blokkeert de toegang tot webbronnen die overeenkomen met de parameters van de regel en geeft een bericht weer dat toegang tot de website is geweigerd.
- **Waarschuwen**. Als de gebruiker toegang probeert te krijgen tot een webbron die overeenkomt met de regel, geeft Webcontrole een waarschuwing weer dat het bezoeken van de webbron af te raden is. Met de koppelingen in het waarschuwingsbericht kan de gebruiker toegang tot de opgevraagde webbron krijgen.

f. In de **Regelplanning** vervolgkeuzelijst, selecteer een schema of maak een nieuw schema.

7. Als u wilt dat Webcontrole de verbinding met de verboden webbron verbreekt onmiddellijk nadat het beleid is toegepast, selecteer het **Beëindig actieve browsersessies van gebruikers nadat de regel is toegepast** selectievakje.

   Met Webcontrole kunt u alleen in webbrowsers de verbinding met webbronnen onmiddellijk verbreken. Voor andere programma's beperkt Webcontrole alleen nieuwe verbindingen.

   Als het selectievakje is uitgeschakeld, beperkt Webcontrole alleen nieuwe verbindingen met verboden webbronnen. Webcontrole beëindigt geen actieve verbindingen.

8. Sla uw wijzigingen op.

Schakel een adresfilter in voor webbronnen in Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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** → **Web Control**.
5. Zet de schakelaar **Web Control ENABLED** aan.
6. In het blok **Rules list**, klikt u op de knop **Add**.
7. Configureer de toegangsregel voor webbronnen:

   a. Typ in het veld **Rule name** de naam van de regel.

   b. Selecteer de status **Enabled** voor de toegangsregel voor webbronnen.

   U kunt de schakelaar gebruiken om de toegangsregel voor webbronnen op elk gewenst moment uit te schakelen zonder deze uit de lijst te verwijderen.

c. Selecteer in het blok **Action** de relevante optie:

- **Allow**. Webcontrole biedt toegang tot webbronnen die overeenkomen met de parameters van de regel.
- **Block**. Webcontrole blokkeert de toegang tot webbronnen die overeenkomen met de parameters van de regel en geeft een bericht weer dat toegang tot de website is geweigerd.
- **Inform**. Als de gebruiker toegang probeert te krijgen tot een webbron die overeenkomt met de regel, geeft Webcontrole een waarschuwing weer dat het bezoeken van de webbron af te raden is. Met de koppelingen in het waarschuwingsbericht kan de gebruiker toegang tot de opgevraagde webbron krijgen.

d. Onder **Scope**, selecteer **Individual websites**.

e. Inhoudsfilter configureren:

- **Individual address**. Maak een lijst met vertrouwde adressen van webbronnen. U kunt een webadres invoeren of maskers gebruiken. U kunt ook een lijst met webbronadressen exporteren vanuit een TXT-bestand.

  > Als de Scan van versleutelde verbindingen is uitgeschakeld, kunt u voor het HTTPS-protocol alleen op servernaam filteren.

- **Data type**. U kunt de gebruikerstoegang tot webbronnen beheren op basis van het specifieke gegevenstype van de gepubliceerde gegevens (bijvoorbeeld *Afbeeldingen*).

f. Onder **User or group**, selecteer gebruikers op wie u wilt dat Webcontrole de regel toepast.

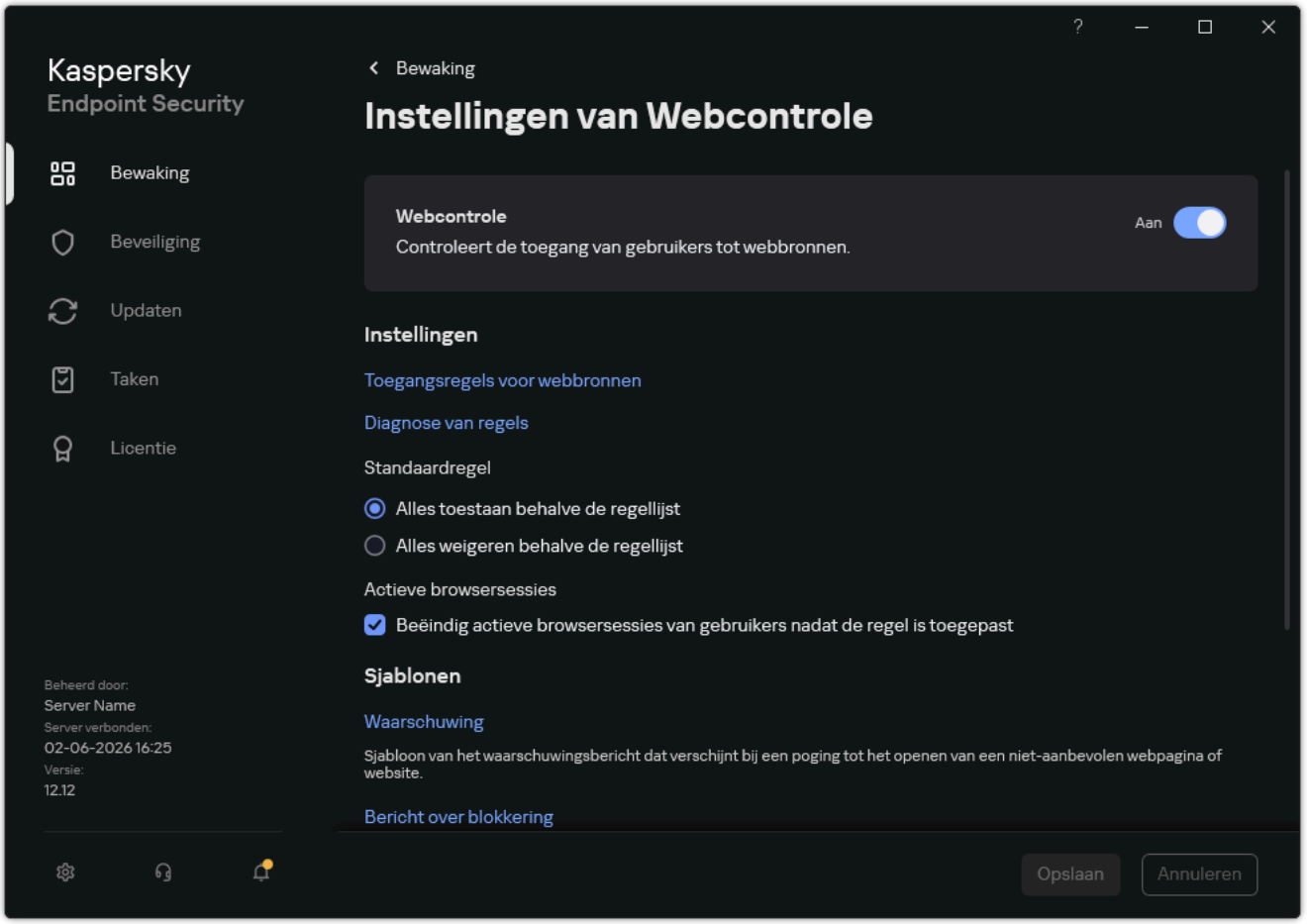
Webcontrole filtert alleen adressen van webbronnen uit de lijst. U kunt een webadres invoeren of maskers gebruiken. U kunt ook een lijst met webbronadressen exporteren vanuit een TXT-bestand. U kunt gebruikers selecteren in Active Directory, in de lijst van accounts in Kaspersky Security Center, of door handmatig een lokale gebruikersnaam in te voeren. Kaspersky raadt aan om locale gebruikersaccounts alleen in speciale gevallen te gebruiken, wanneer het niet mogelijk is om domeingebruikersaccounts te gebruiken.

g. In het **Access schedule** blok, selecteer een schema of maak een nieuw schema.

8. Sla uw wijzigingen op.

Schakel een adresfilter in voor webbronnen in de programma-interface

1. Klik in het hoofdvenster van het programma op de knop ⚙.
2. Selecteer **Security Controls** → **Webcontrole** in het venster met de programma-instellingen.



Webcontrole 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**. Webcontrole biedt toegang tot webbronnen die overeenkomen met de parameters van de regel.
   - **Blokkeren**. Webcontrole blokkeert de toegang tot webbronnen die overeenkomen met de parameters van de regel en geeft een bericht weer dat toegang tot de website is geweigerd.
   - **Waarschuwen**. Als de gebruiker toegang probeert te krijgen tot een webbron die overeenkomt met de regel, geeft Webcontrole een waarschuwing weer dat het bezoeken van de webbron af te raden is. Met de koppelingen in het waarschuwingsbericht kan de gebruiker toegang tot de opgevraagde webbron krijgen.

8. Onder **Adressen**, selecteer **Op individuele adressen**.

   Maak een lijst met vertrouwde adressen van webbronnen. U kunt een webadres invoeren of maskers gebruiken. U kunt ook een lijst met webbronadressen exporteren vanuit een TXT-bestand.

   > Als de Scan van versleutelde verbindingen is uitgeschakeld, kunt u voor het HTTPS-protocol alleen op servernaam filteren.

9. 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 alleen adressen van webbronnen uit de lijst. U kunt een webadres invoeren of maskers gebruiken. U kunt ook een lijst met webbronadressen exporteren vanuit een TXT-bestand. U kunt gebruikers selecteren in Active Directory, in de lijst van accounts in Kaspersky Security Center, of door handmatig een lokale gebruikersnaam in te voeren. Kaspersky raadt aan om locale gebruikersaccounts alleen in speciale gevallen te gebruiken, wanneer het niet mogelijk is om domeingebruikersaccounts te gebruiken.

10. In de **Regelplanning** vervolgkeuzelijst, selecteer een schema of maak een nieuw schema.

11. Als u wilt dat Webcontrole de verbinding met de verboden webbron verbreekt onmiddellijk nadat het beleid is toegepast, selecteer het **Beëindig actieve browsersessies van gebruikers nadat de regel is toegepast** selectievakje.

    > Met Webcontrole kunt u alleen in webbrowsers de verbinding met webbronnen onmiddellijk verbreken. Voor andere programma's beperkt Webcontrole alleen nieuwe verbindingen.

    Als het selectievakje is uitgeschakeld, beperkt Webcontrole alleen nieuwe verbindingen met verboden webbronnen. Webcontrole beëindigt geen actieve verbindingen.

12. Sla uw wijzigingen op.

Als resultaat wordt de nieuwe Webcontrole-regel aan de lijst toegevoegd. Indien nodig, wijzig de prioriteit van de Webcontrole-regel. U kunt ook op elk gewenst moment de schakelaar gebruiken om de toegangsregel voor webbronnen uit te schakelen zonder deze uit de lijst te verwijderen.

Filteren op inhoud van webbronnen

Om de toegang via de inhoud van webbronnen te controleren, biedt Webcontrole een categoriefilter en een gegevenstypefilter.

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.

U kunt de gebruikerstoegang tot een website beperken op basis van het gegevenstype, bijvoorbeeld om afbeeldingen te verbergen. Kaspersky Endpoint Security bepaalt het gegevenstype op basis van de bestandsindeling en niet op basis van de extensie. Webcontrole onderscheidt de volgende gegevenstypen:

- Video
- Geluid
- Office-programmabestanden
- Uitvoerbare bestanden
- Archieven
- Afbeeldingen
- Scripts

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 *Afbeeldingen*.

Regels kunnen een regelplanning en een lijst met gebruikers bevatten waarop de regel van toepassing is. Bijvoorbeeld, u kunt de toegang tot websites alleen tijdens werkuren beperken of het bezoeken van websites toestaan aan gebruikers in bepaalde groepen.

Een inhoudsfilter voor webbronnen inschakelen in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Security Controls** → **Webcontrole** in het beleidsvenster.
4. Selecteer het selectievakje **Webcontrole**.
5. In het blok **Instellingen van Webcontrole**, klikt u op de knop **Toevoegen**.
   Het venster **Regel voor toegang tot webbronnen** wordt geopend.
6. Configureer de toegangsregel voor webbronnen:
   a. Typ in het veld **Naam** de naam van de regel.
   b. In de **Filter inhoud** vervolgkeuzelijst, selecteert de relevante inhoudsfilter:
      - **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 *Afbeeldingen*).
      - **Op inhoudscategorieën en gegevenstypen**. Filters op inhoudscategorieën en gegevenstypen zijn ingeschakeld.

   Nadat de filters zijn geselecteerd, configureer de filterparameters.

c. In de **Pas toe op gebruikers** vervolgkeuzelijst, selecteer de relevante filter voor gebruikers:

- **Op alle gebruikers**. Webcontrole filtert webbronnen niet op adres.
- **Op individuele gebruikers of groepen**. Webcontrole filtert alleen adressen van webbronnen uit de lijst. U kunt een webadres invoeren of maskers gebruiken. U kunt ook een lijst met webbronadressen exporteren vanuit een TXT-bestand. U kunt gebruikers selecteren in Active Directory, in de lijst van accounts in Kaspersky Security Center, of door handmatig een lokale gebruikersnaam in te voeren. Kaspersky raadt aan om locale gebruikersaccounts alleen in speciale gevallen te gebruiken, wanneer het niet mogelijk is om domeingebruikersaccounts te gebruiken.

d. In de **Actie** vervolgkeuzelijst, selecteer een optie:

- **Toestaan**. Webcontrole biedt toegang tot webbronnen die overeenkomen met de parameters van de regel.
- **Blokkeren**. Webcontrole blokkeert de toegang tot webbronnen die overeenkomen met de parameters van de regel en geeft een bericht weer dat toegang tot de website is geweigerd.
- **Waarschuwen**. Als de gebruiker toegang probeert te krijgen tot een webbron die overeenkomt met de regel, geeft Webcontrole een waarschuwing weer dat het bezoeken van de webbron af te raden is. Met de koppelingen in het waarschuwingsbericht kan de gebruiker toegang tot de opgevraagde webbron krijgen.

e. In de **Regelplanning** vervolgkeuzelijst, selecteer een schema of maak een nieuw schema.

7. Als u wilt dat Webcontrole de verbinding met de verboden webbron verbreekt onmiddellijk nadat het beleid is toegepast, selecteer het **Beëindig actieve browsersessies van gebruikers nadat de regel is toegepast** selectievakje.

   Met Webcontrole kunt u alleen in webbrowsers de verbinding met webbronnen onmiddellijk verbreken. Voor andere programma's beperkt Webcontrole alleen nieuwe verbindingen.

   Als het selectievakje is uitgeschakeld, beperkt Webcontrole alleen nieuwe verbindingen met verboden webbronnen. Webcontrole beëindigt geen actieve verbindingen.

8. Sla uw wijzigingen op.

Schakel een inhoudsfilter in voor webbronnen in Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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** → **Web Control**.
5. Zet de schakelaar **Web Control ENABLED** aan.
6. In het blok **Rules list**, klikt u op de knop **Add**.

7. Configureer de toegangsregel voor webbronnen:

   a. Typ in het veld **Rule name** de naam van de regel.

   b. Selecteer de status **Enabled** voor de toegangsregel voor webbronnen.

      U kunt de schakelaar gebruiken om de toegangsregel voor webbronnen op elk gewenst moment uit te schakelen.

   c. Selecteer in het blok **Action** de relevante optie:

      - **Allow**. Webcontrole biedt toegang tot webbronnen die overeenkomen met de parameters van de regel.
      - **Block**. Webcontrole blokkeert de toegang tot webbronnen die overeenkomen met de parameters van de regel en geeft een bericht weer dat toegang tot de website is geweigerd.
      - **Inform**. Als de gebruiker toegang probeert te krijgen tot een webbron die overeenkomt met de regel, geeft Webcontrole een waarschuwing weer dat het bezoeken van de webbron af te raden is. Met de koppelingen in het waarschuwingsbericht kan de gebruiker toegang tot de opgevraagde webbron krijgen.

   d. Onder **Scope**, selecteer **Content category**.

   e. Inhoudsfilter configureren:

      - **Content category**. U kunt gebruikerstoegang tot webbronnen per categorie beheren (bijvoorbeeld de categorie *Sociale netwerken*).
      - **Data type**. U kunt de gebruikerstoegang tot webbronnen beheren op basis van het specifieke gegevenstype van de gepubliceerde gegevens (bijvoorbeeld *Afbeeldingen*).

   f. Onder **User or group**, selecteer gebruikers op wie u wilt dat Webcontrole de regel toepast.

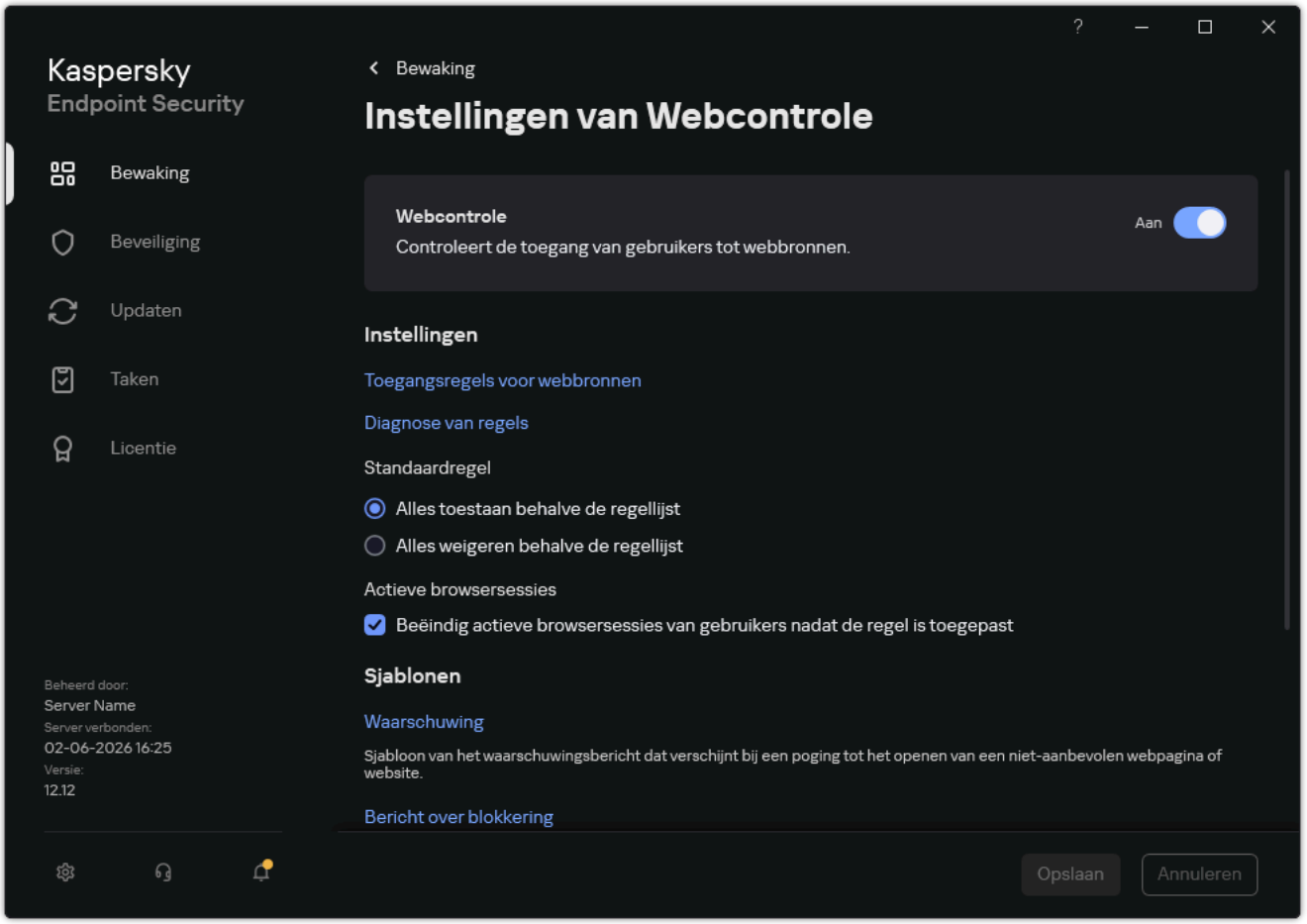
      Webcontrole filtert alleen adressen van webbronnen uit de lijst. U kunt een webadres invoeren of maskers gebruiken. U kunt ook een lijst met webbronadressen exporteren vanuit een TXT-bestand. U kunt gebruikers selecteren in Active Directory, in de lijst van accounts in Kaspersky Security Center, of door handmatig een lokale gebruikersnaam in te voeren. Kaspersky raadt aan om locale gebruikersaccounts alleen in speciale gevallen te gebruiken, wanneer het niet mogelijk is om domeingebruikersaccounts te gebruiken.

   g. In het **Access schedule** blok, selecteer een schema of maak een nieuw schema.

8. Sla uw wijzigingen op.

Een inhoudsfilter voor webbronnen inschakelen in de programma-interface

1. Klik in het hoofdvenster van het programma op de knop ⚙.
2. Selecteer **Security Controls** → **Webcontrole** in het venster met de programma-instellingen.



Webcontrole 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**. Webcontrole biedt toegang tot webbronnen die overeenkomen met de parameters van de regel.
   - **Blokkeren**. Webcontrole blokkeert de toegang tot webbronnen die overeenkomen met de parameters van de regel en geeft een bericht weer dat toegang tot de website is geweigerd.
   - **Waarschuwen**. Als de gebruiker toegang probeert te krijgen tot een webbron die overeenkomt met de regel, geeft Webcontrole een waarschuwing weer dat het bezoeken van de webbron af te raden is. 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 *Afbeeldingen*).

   Het inhoudsfilter configureren:

   a. Klik op de koppeling **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 **Gebruikers** het relevante filter voor gebruikers:

   - **Op alle gebruikers**. Webcontrole filtert webbronnen niet op adres.

   - **Op individuele gebruikers en/of groepen**. Webcontrole filtert alleen adressen van webbronnen uit de lijst. U kunt een webadres invoeren of maskers gebruiken. U kunt ook een lijst met webbronadressen exporteren vanuit een TXT-bestand. U kunt gebruikers selecteren in Active Directory, in de lijst van accounts in Kaspersky Security Center, of door handmatig een lokale gebruikersnaam in te voeren. Kaspersky raadt aan om locale gebruikersaccounts alleen in speciale gevallen te gebruiken, wanneer het niet mogelijk is om domeingebruikersaccounts te gebruiken. 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 groepen gebruikers waarop u de toegangsregel voor webbronnen wilt toepassen.

     c. Keer terug naar het venster voor het configureren van de toegangsregel voor webbronnen.

10. 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 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.

11. Als u wilt dat Webcontrole de verbinding met de verboden webbron verbreekt onmiddellijk nadat het beleid is toegepast, selecteer het **Beëindig actieve browsersessies van gebruikers nadat de regel is toegepast** selectievakje.

Met Webcontrole kunt u alleen in webbrowsers de verbinding met webbronnen onmiddellijk verbreken. Voor andere programma's beperkt Webcontrole alleen nieuwe verbindingen.

Als het selectievakje is uitgeschakeld, beperkt Webcontrole alleen nieuwe verbindingen met verboden webbronnen. Webcontrole beëindigt geen actieve verbindingen.

12. Sla uw wijzigingen op.

Als resultaat wordt de nieuwe Webcontrole-regel aan de lijst toegevoegd. Indien nodig, wijzig de prioriteit van de Webcontrole-regel. U kunt ook op elk gewenst moment de schakelaar gebruiken om de toegangsregel voor webbronnen uit te schakelen zonder deze uit de lijst te verwijderen.

Toegangsregels voor webbronnen testen

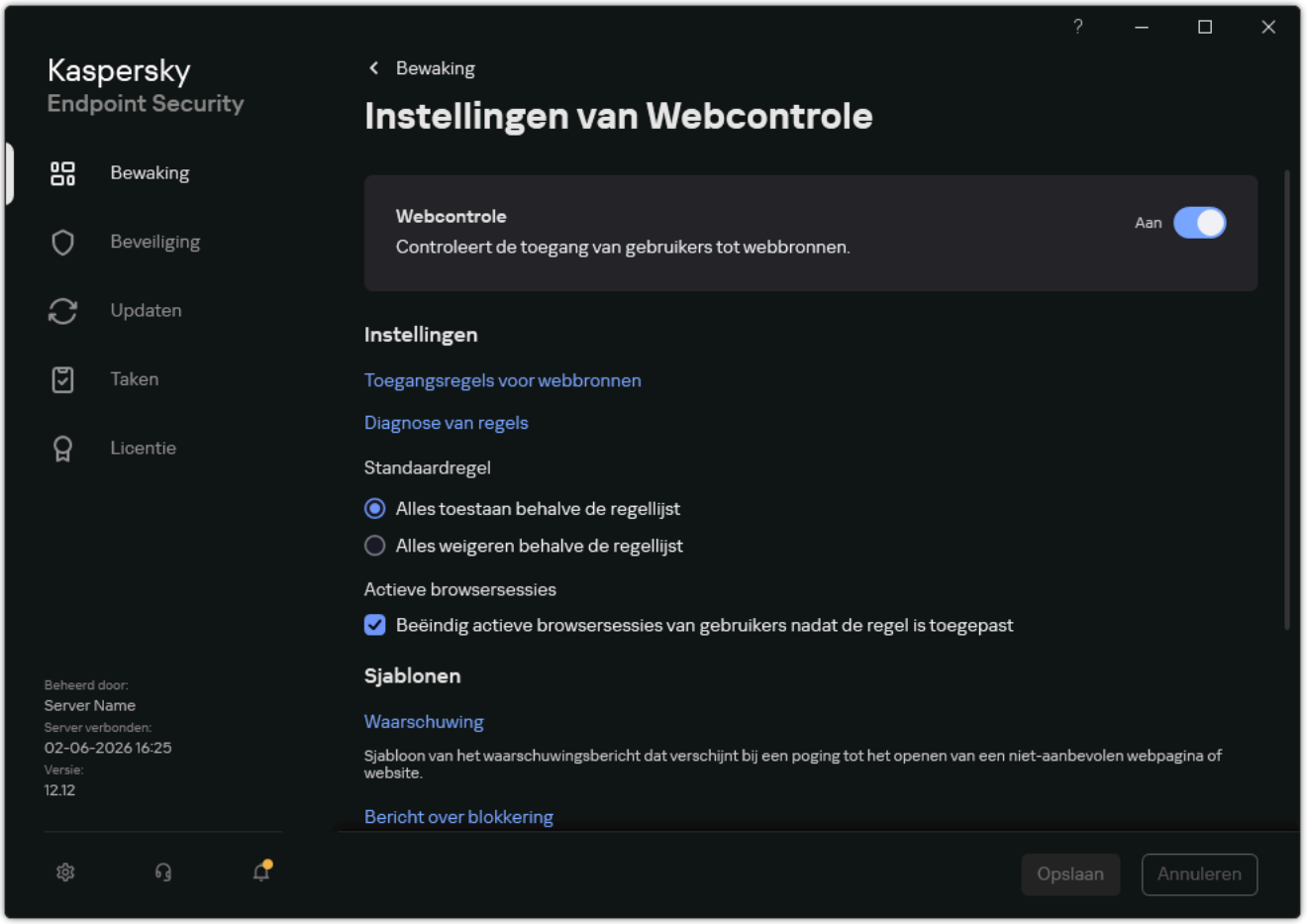
Wanneer u Webcontrole configureert, blokkeert u mogelijk onbedoeld de toegang tot webbronnen die gebruikers nodig hebben voor hun werk. Als u wilt weten welke regel voor Webcontrole de toegang tot webbronnen blokkeert, kunt u de tool *diagnostische Webcontrole-regels* gebruiken. Diagnostische Webcontrole-regels is alleen beschikbaar in de interface van Kaspersky Endpoint Security. In de Kaspersky Security Center console kunt u niet achterhalen welke Webcontrole-regel een bepaalde bron bevat.

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.

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.



Webcontrole 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 onderstaande veld in.

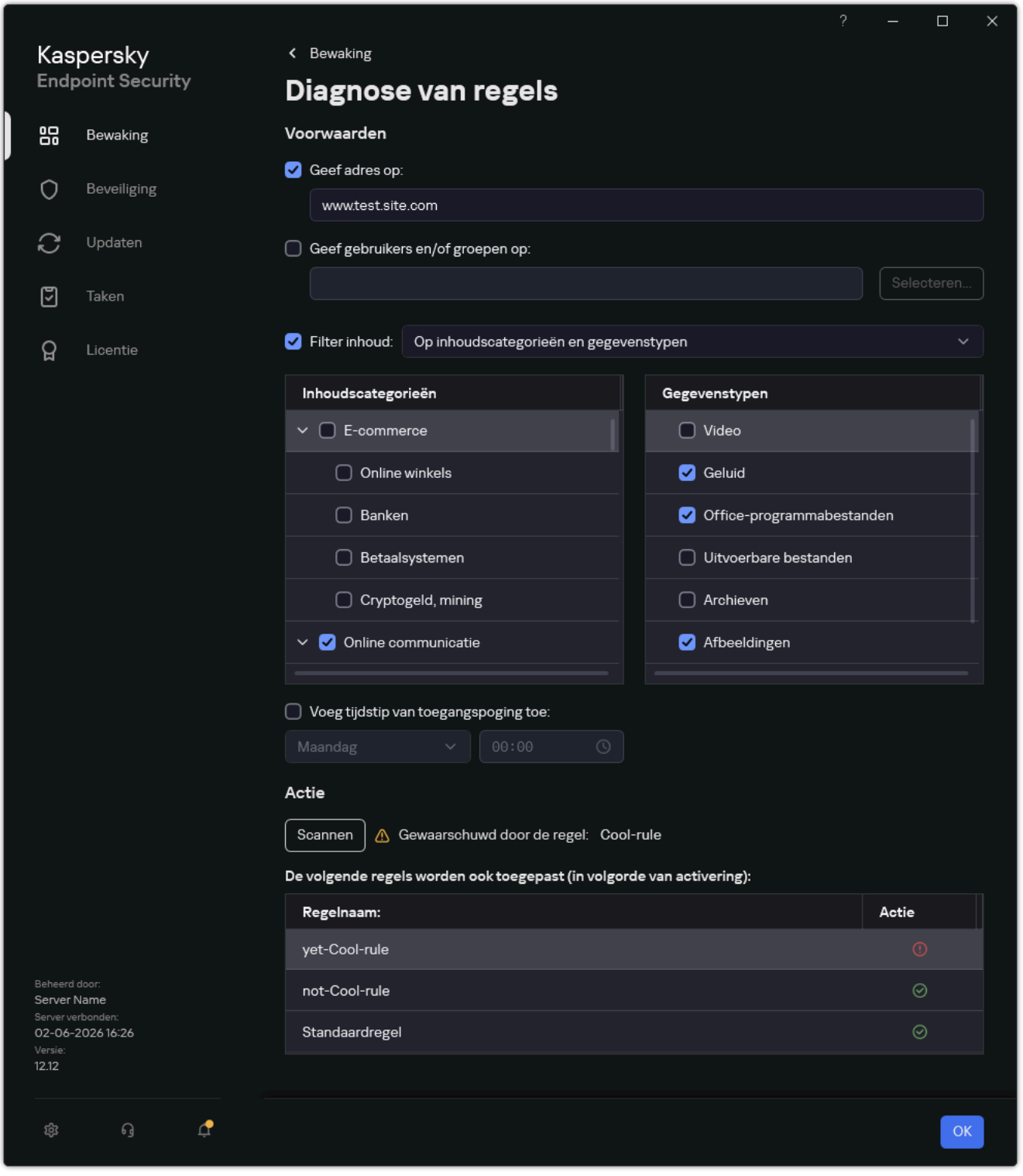
5. Als u de regels wilt testen die Kaspersky Endpoint Security gebruikt om de toegang tot webbronnen te controleren voor opgegeven gebruikers en/of groepen gebruikers, geeft u een lijst met gebruikers en/of groepen gebruikers op.

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.



Regels voor webcontrole exporteren en importeren

U kunt de lijst met regels van Webcontrole exporteren naar een XML-bestand of JSON-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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Security Controls** → **Webcontrole** in het beleidsvenster.
4. 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 koppeling **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.
5. Zo importeert u de lijst met regels van Webcontrole:
   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.
6. Sla uw wijzigingen op.

Een lijst met regels van Webconsole exporteren en importeren via de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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** → **Web Control**.

5. U exporteert de lijst met regels door het volgende te doen in het blok **Rules list**:

   a. Selecteer de regels die u wilt exporteren.

   b. Klik op de knop → **Export**.

      Kaspersky Endpoint Security exporteert de lijst met regels naar een JSON-bestand in de standaard downloadmap.

6. U importeert de lijst met regels door het volgende te doen in het blok **Rules list**:

   a. Klik op de knop → **Import**.

      Selecteer in het geopende venster het JSON-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 JSON-bestand.

7. Sla uw wijzigingen op.

Adressen van webbronnen van de webcontrole-regel exporteren en importeren

Als u een lijst met webbronadressen in een toegangsregel voor webbronnen hebt gemaakt, kunt u die naar een TXT-bestand exporteren.

- In TXT-indeling in de Beheerconsole (MMC)
- In CSV-indeling in de programma-interface

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.

U kunt ook alle Webcontrole-regels exporteren/importeren, niet alleen de adressen van een webbron van een afzonderlijke regel.

> U kunt geen adressen van een webbron van een Webcontrole-regel exporteren/importeren in Webconsole of Cloudconsole.

Export-/import adressen van webbronnen van de Webcontrole-regel in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Security Controls** → **Webcontrole** in het beleidsvenster.

4. In de **Instellingen van Webcontrole** blok, selecteer de regel waarvan u de lijst met adressen van webbronnen wilt exporteren of importeren.

   Eigenschappen voor Webcontrole-regels worden weergegeven.

5. Om de lijst met webbronnen te exporteren, doe het volgende in de adreslijst:

   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 de knop .

   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, doe het volgende in de adreslijst:

   a. Klik op de knop .

      Selecteer in het geopende venster het TXT-bestand waaruit u de lijst met webbronnen wilt importeren.

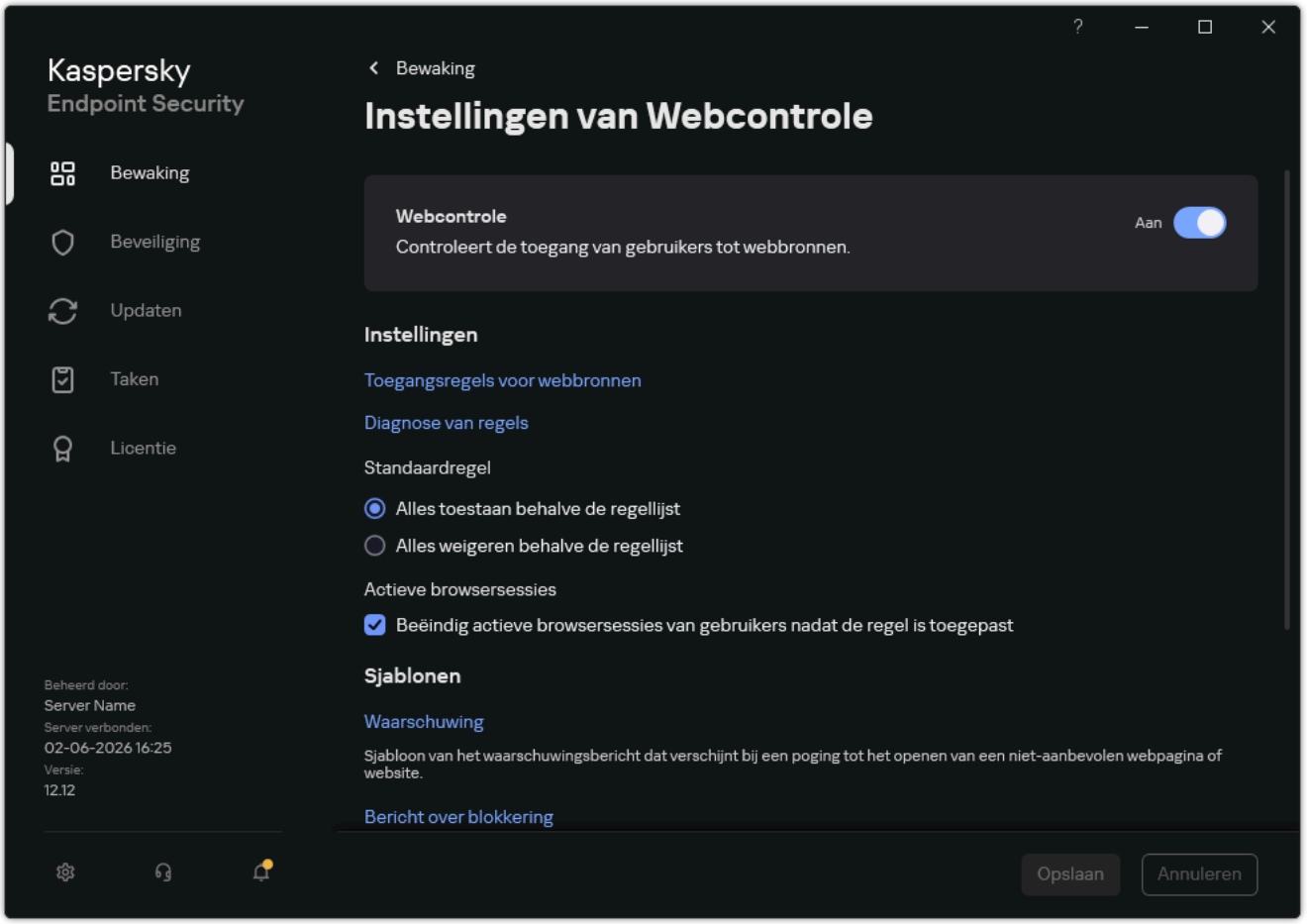
   b. Open het bestand.

      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.

Export-/import adressen van webbronnen van de Webcontrole-regel in de programma-interface

1. Klik in het hoofdvenster van het programma op de knop ⚙.
2. Selecteer **Security Controls** → **Webcontrole** in het venster met de programma-instellingen.



Webcontrole 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 CSV-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 CSV-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 CSV-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 CSV-bestand.

7. Sla uw wijzigingen op.

Activiteit van gebruikers op internet bewaken

Met Kaspersky Endpoint Security kunt u gegevens registeren over bezoeken aan websites, waaronder toegestane websites. Op deze manier krijgt u een compleet overzicht van de browseractiviteit. Kaspersky Endpoint Security verstuurt 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. Het monitoren van gebruikersactiviteit werkt niet in andere browsers.

Kaspersky Endpoint Security maakt de volgende gebeurtenissen over de activiteit van gebruikers op internet:

- Blokkeer de website (*Critical* status).
- Bezoek aan een niet-aanbevolen website (status *Warning*).
- Bezoek aan een toegestane website (status *Info*).

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 webpagina-interactiescript injecteren

Hoe een webpagina-interactiescript in het webverkeer te injecteren in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Algemene instellingen** → **Netwerkinstellingen** in het beleidsvenster.
4. Schakel in het blok **Scan van geëncrypte verbindingen** het selectievakje **Script injecteren in internetverkeer voor interactie met webpagina's** in.
5. Sla uw wijzigingen op.

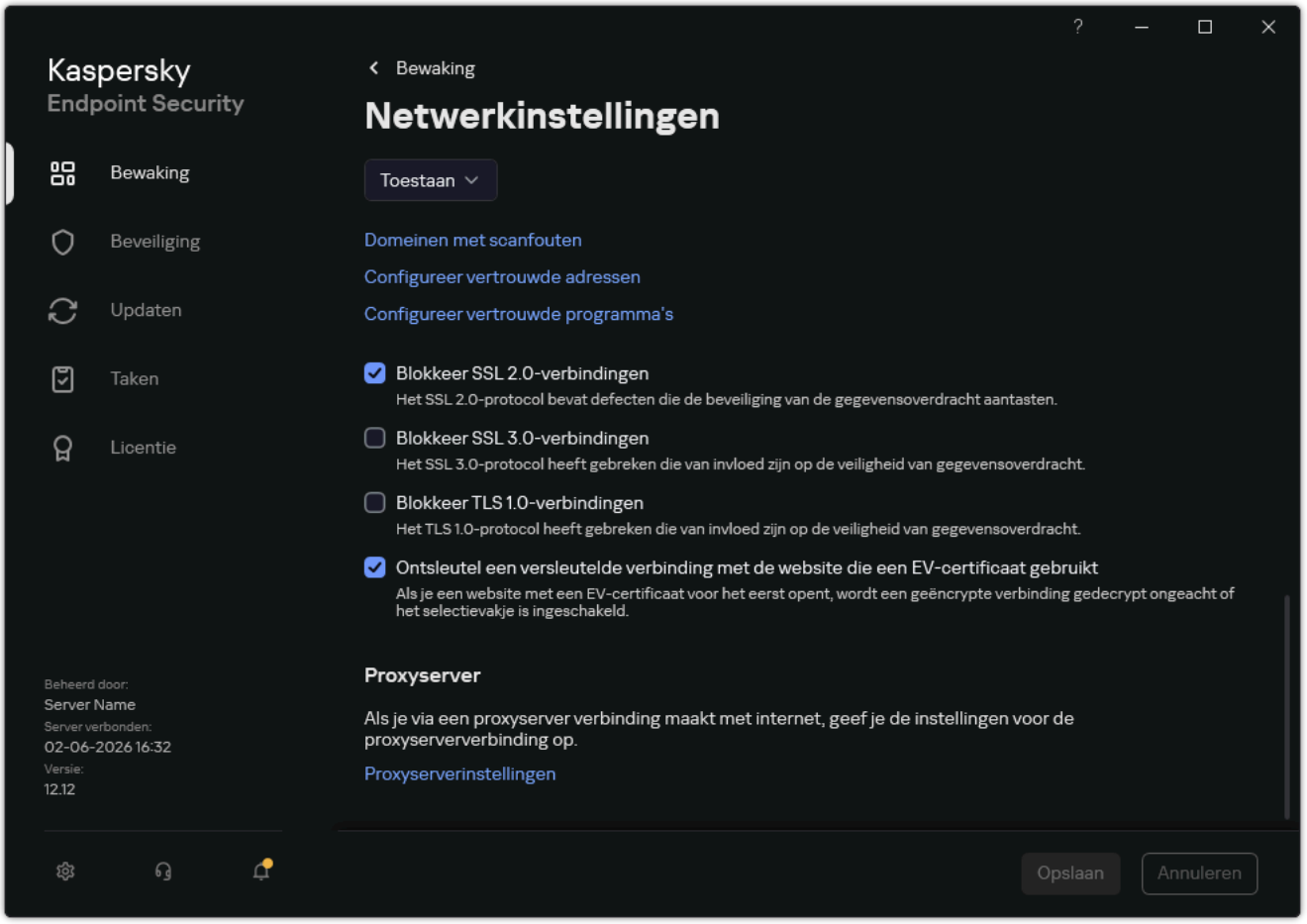
Hoe een webpagina-interactiescript in het webverkeer te injecteren in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **General Settings** → **Network Settings** in het beleidsvenster.
5. Schakel onder **Monitoring of internet connections** de schakelaar **Monitoring of internet connections ENABLED** aan.
6. Sla uw wijzigingen op.

Hoe een webpagina-interactiescript in het webverkeer te injecteren 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.



Netwerkinstellingen programma

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 programmagebeurtenislogboek, het OS-gebeurtenislogboek en rapporten worden geregistreerd.

Registratie van webcontrole-gebeurtenissen instellen

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 **Meldingen configureren**.
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:

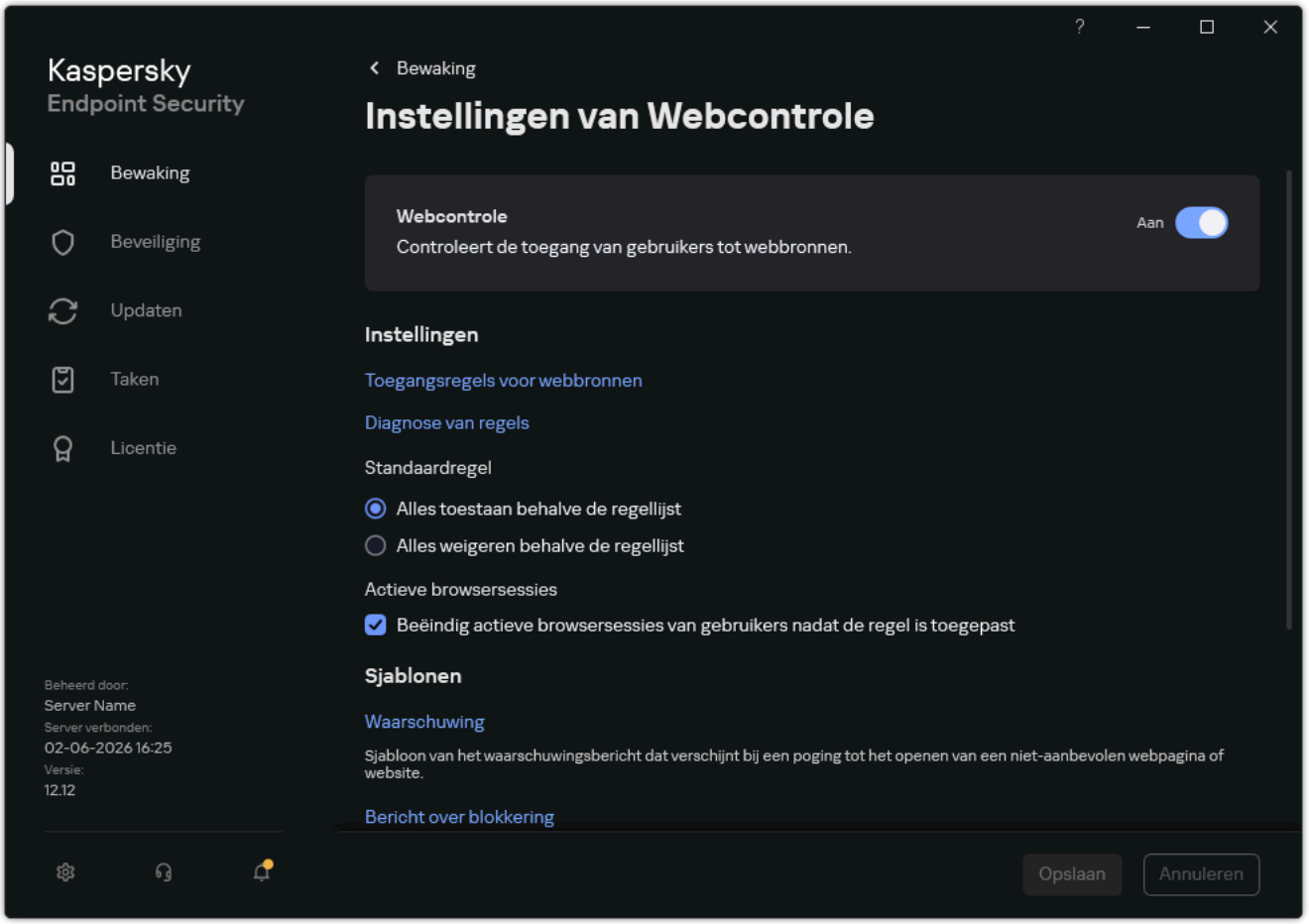
- Als u Kaspersky Security Center gebruikt, verzendt Webcontrole gebeurtenissen voor alle objecten waaruit de webpagina bestaat. Daarom kunnen meerdere gebeurtenissen worden aangemaakt wanneer een webpagina wordt geblokkeerd. Voorbeeld: bij de blokkering van de webpagina http://www.example.com, zal Kaspersky Endpoint Security gebeurtenissen voor de volgende objecten vastleggen: http://www.example.com, http://www.example.com/icon.ico, http://www.example.com/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.

Gebeurtenissen registreren bij het bezoeken van toegestane websites

Zo schakelt u de registratie van gebeurtenissen bij het bezoeken van toegestane websites in:

1. Klik in het hoofdvenster van het programma op de knop ⚙.

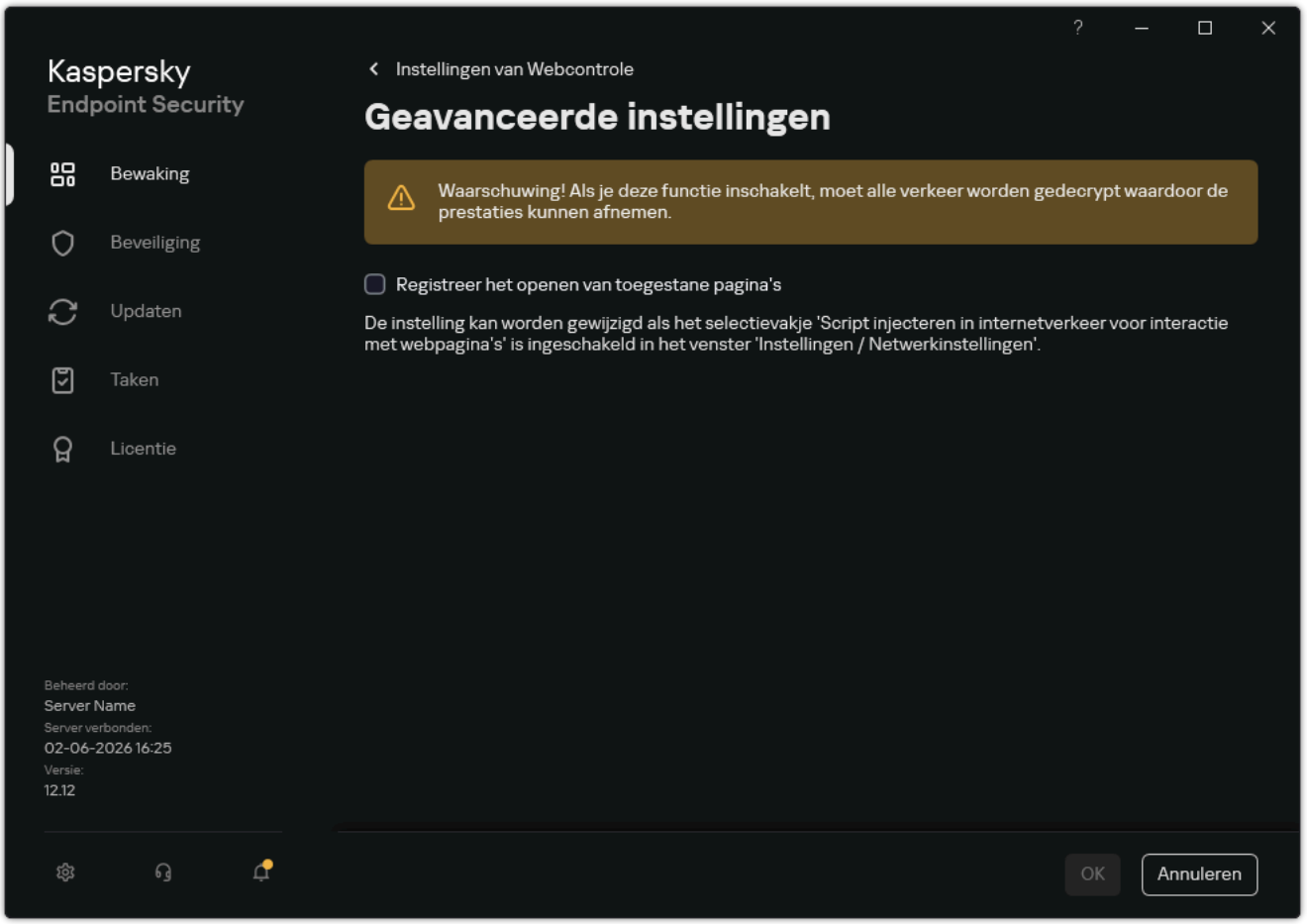
2. Selecteer **Security Controls** → **Webcontrole** in het venster met de programma-instellingen.



Webcontrole 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**.



Webcontrole geavanceerde instellingen

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):

- Waarschuwingsbericht. Dit bericht waarschuwt de gebruiker dat een bezoek aan de webbron wordt afgeraden en/of het beveiligingsbeleid van het bedrijf schendt. Kaspersky Endpoint Security toont een waarschuwingsbericht als de optie **Waarschuwen** is geselecteerd in de 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 (zie onderstaande afbeelding) 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.



Bericht over blokkering van webbronnen

Voor het waarschuwingsbericht, het bericht met de melding dat een webbron is geblokkeerd en het bericht dat naar de netwerkbeheerder wordt verstuurd zijn speciale sjablonen voorzien. Er zijn speciale variabelen voorzien voor het beheer van de berichtsjablonen (bijvoorbeeld `%USER_NAME%`). Met variabelen kan één berichtsjabloon voor verschillende computers worden gebruikt. Bij het genereren van een bericht haalt Kaspersky Endpoint Security de waarde van de variabele op uit de instellingen van het besturingssysteem en voegt het deze in het bericht in dat overeenkomt met de specifieke computer, gebruiker en gebeurtenis.

Het berichtsjabloon voor Webcontrole in de Beheerconsole (MMC) wijzigen

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Security Controls** → **Webcontrole** in het beleidsvenster.
4. In het blok **Instellingen voor berichtsjablonen**, klikt u op de knop **Sjablonen**.
5. Configureer de berichtsjablonen van Webcontrole:

   - **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.

Als u een variabele aan de sjabloontekst wilt toevoegen, plaats dan de cursor op de gewenste positie, klik op **Variabele** en selecteer de gewenste variabele in de lijst met beschikbare opties.

U kunt de standaardsjabloontekst ook herstellen met de knop **Standaard**.

6. Sla uw wijzigingen op.

Het berichtsjabloon van Webcontrole veranderen in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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** → **Web Control**.
5. In de **Message templates** blok, klik op de **Message about website blocking** sjablonen voor Webcontrole-berichten koppelen en configureren:

   - **Warning**. 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.
   - **Message about blocking**. Het invoerveld bevat het sjabloon van het bericht dat wordt weergegeven als een regel die de toegang tot een webbron blokkeert wordt geactiveerd.
   - **Message to administrator**. 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.

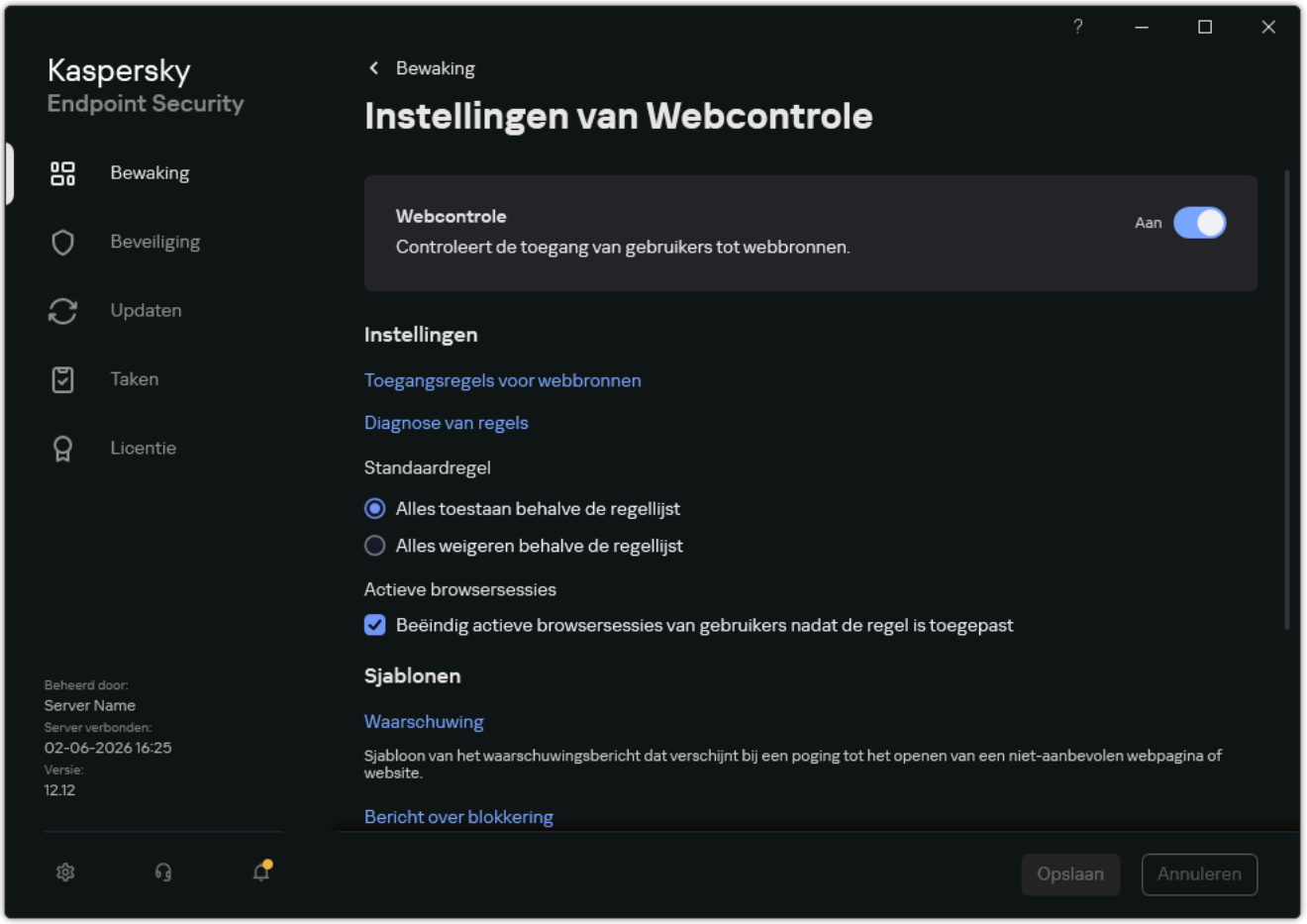
   Als u een variabele aan de sjabloontekst wilt toevoegen, plaats dan de cursor op de gewenste positie, klik op **Add variable** en selecteer de gewenste variabele in de lijst met beschikbare opties.

   U kunt de standaardsjabloontekst ook herstellen met de knop **Reset to default**.
6. Sla uw wijzigingen op.

Het berichtsjabloon voor Webcontrole in de programma-interface wijzigen

1. Klik in het hoofdvenster van het programma op de knop ⚙.

2. Selecteer **Security Controls** → **Webcontrole** in het venster met de programma-instellingen.



Webcontrole 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.

   Als u een variabele aan de sjabloontekst wilt toevoegen, plaats dan de cursor op de gewenste positie, klik op **Variabele toevoegen** en selecteer de gewenste variabele in de lijst met beschikbare opties.

   U kunt de standaardsjabloontekst ook herstellen met de knop **Opnieuw instellen**.

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.example.com/page_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 `pictures.`.
   - `http://user.pictures.example.com`. Het domeinmasker `*.` vertegenwoordigt `pictures.` en `user.`.
   - `http://example.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.example.com` wordt behandeld als `*.example.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.example.com` omvat adressen zoals `http://www.example.com/abc`, waarbij `a`, `b` en `c` willekeurige tekens zijn.

6. Als een adresmasker eindigt met het teken `/`, is de inhoud van het adresmasker gelijk aan dezelfde inhoud met het achtervoegsel `/*`.

7. De tekens `/*` op het einde van een adresmasker wordt beschouwd als `/*` of een lege tekenreeks.

8. De adressen van webbronnen worden vergeleken met een adresmasker, waarbij rekening wordt gehouden met het protocol (http of https):

   - Als het adresmasker geen netwerkprotocol bevat, omvat dit adresmasker alle adressen met een willekeurig netwerkprotocol.

     Bijvoorbeeld: het adresmasker `example.com` dekt de adressen `http://` `example.com` en `https://` `example.com`.

- Als het adresmasker een netwerkprotocol bevat, omvat dit adresmasker alleen adressen met hetzelfde netwerkprotocol als dat van het adresmasker.

  Voorbeeld: het adresmasker `http://*.example.com` omvat het adres `http://www.example.com` maar niet `https://www.example.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; 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.

Webcontrole voor virtuele machines

Webcontrole regelt het verkeer op de computer en op een virtuele machine die lokaal op de computer is geïmplementeerd. Dit werkt zonder dat u het Kaspersky Endpoint Security-programma op de lokale virtuele machine hoeft te installeren. Dit betekent dat als de gebruiker een website probeert te openen die wordt geblokkeerd door een regel voor webcontrole in een browser op de *virtuele machine*, het programma dat is geïnstalleerd op het hostbesturingssysteem van de *computer* weigert de toegang tot die website.

Webcontrole werkt anders op verschillende virtuele machines.

Oracle VM VirtualBox

Kaspersky Endpoint Security ondersteunt zonder beperkingen Webcontrol-regels op virtuele Oracle VM VirtualBox-machines. Het programma kan al het verkeer van de virtuele machine regelen. Als een filter op gebruiker is geconfigureerd in Webcontrol-regels, werkt het programma correct omdat alle processen van de virtuele machines worden gestart door de lokale gebruiker.

VMware-werkstation

Kaspersky Endpoint Security ondersteunt webcontrole-regels op virtuele machines VMware werkstation met beperkingen. Het programma ondersteunt geen regels met een filter op gebruiker geconfigureerd. Processen van virtuele machines worden uitgevoerd onder de systeemgebruiker (SYSTEM). Dit maakt het onmogelijk om de gebruiker te identificeren die de website probeert te openen op de virtuele machine.

Microsoft Hyper-V

Kaspersky Endpoint Security ondersteunt geen Webcontrol-regels op virtuele Microsoft Hyper-V-machines.

Variabelen in de berichtsjablonen van Webcontrole

U kunt de volgende variabelen gebruiken in sjablonen voor berichten voor gebruikers of berichten voor beheerders:

- **User** – `%USER_NAME%`.

  Naam van het huidige gebruikersaccount op de computer waarop het bericht is gegenereerd, in het `<device name>\<user alias>` formaat (bijvoorbeeld `DESKTOP-123\John.Smith`).

- **Web resource address** – `%CANONIC_REQUEST_URL%`.

  Adres van de geblokkeerde webbron.

- **Rule name** – `%RULE%`.

  Naam van de regel die de webbron blokkeerde.

- **Email for sending a message** – `%COMPLAIN_EMAIL%`.

  E-mailadres voor feedback over blokkering van webbronnen. Door op het e-mailadres te klikken opent zich een venster waarin de gebruiker een bericht naar de beheerder kan sturen.

- **Name of content category** – `%CONTENT_CATEGORY_LIST%`.

  Websitecategorie waartoe de geblokkeerde bron behoort (bijvoorbeeld *Payment systems*).

- **Name of data type category** – `%TYPE_CATEGORY_LIST%`.

  Categorie van het gegevenstype voor de geblokkeerde webbron (bijvoorbeeld *Graphic files*).

- **Link to requested web resource** – `%CONTINUE_PAGE%`.

  Link naar de gevraagde webpagina (bijvoorbeeld `http://www.example.com/pagename.html`).

- **Link to website** – `%CONTINUE_SITE%`.

  Link naar de website die de gevraagde webpagina bevat (bijvoorbeeld `http://www.example.com/`).

- **Link for access to domains** – `%CONTINUE_DOMAIN%`.

  Link waarop kan worden geklikt om toegang te krijgen tot alle bestaande webpagina's van de domeinnaam. Als het adres van de geblokkeerde webpagina bijvoorbeeld is: `http://www.example.com`, de `%CONTINUE_DOMAIN%` variabele is vervangt door de `http://*.example.com` link. Als u op deze link klikt, krijgt u toegang tot alle webadressen van de basisdomeinnaam `http://www.example.com/` inclusief subdomeinen, bijvoorbeeld `http://start.example.com/*` of `http://domain.domain.example.com/*`, waar de `*` karakter staat voor een willekeurige reeks tekens (inclusief een lege tekenreeks).

Apparaatcontrole

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

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 **Advanced** → **Repositories** → **Hardware**.

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 – ⊘.
  - Volgens regels (alleen printers en draagbare apparaten) – .

- Afhankelijk van verbindingsbus (behalve wifi) – .
- Blokkeren met uitzonderingen (alleen wifi) – .

- **Verbindingsbus**. Een *verbindingsbus* is een interface voor de aansluiting van apparaten op de computer (bijvoorbeeld USB of FireWire). Als **Afhankelijk van verbindingsbus** modus is geselecteerd voor het apparaattype, staat het programma de toegang tot het apparaat toe of weigert afhankelijk van de verbindings-interface (bijv. 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.

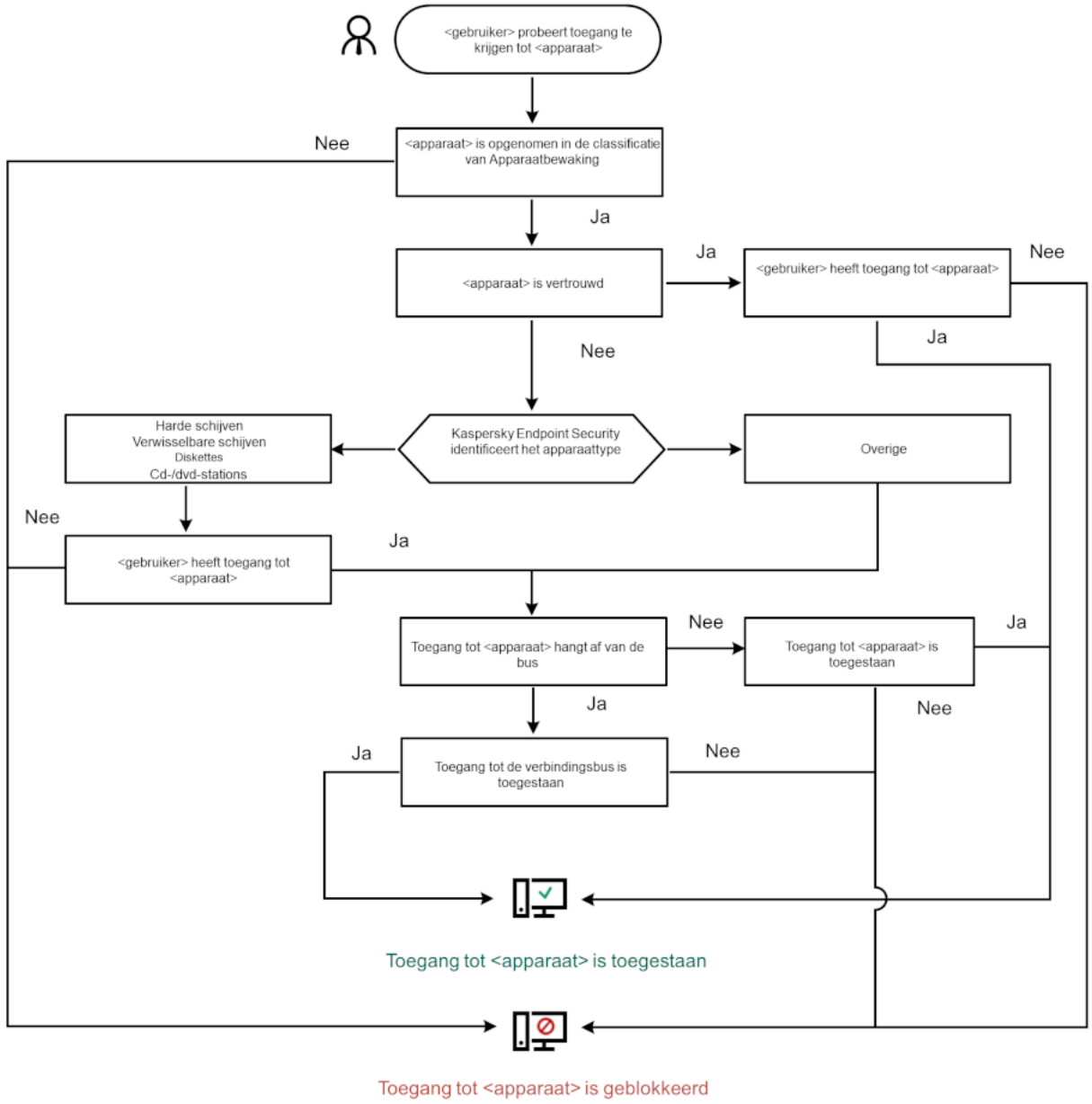
Wanneer een apparaat dat wordt geblokkeerd door Apparaatcontrole wordt aangesloten op de computer, blokkeert Kaspersky Endpoint Security de toegang en toont het een melding (zie onderstaande afbeelding).



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.

Over toegangsregels

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. 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 (inclusief USB-flashstations)	✓	✓	✓	✓	✓
Diskettes	✓	✓	✓	✓	✓
Cd-/dvd-stations	✓	✓	✓	✓	✓
Draagbare apparaten (MTP)	✓	✓	✓	✓	✓
Lokale Printers	✓	–	✓	✓	–
Netwerkprinters	✓	–	✓	✓	–
Modems	✓	–	–	–	–
Tapeapparaten	✓	–	–	–	–
Multifunctionele apparaten	✓	–	–	–	–
Smartcardlezers	✓	–	–	–	–
Windows CE USB ActiveSync-apparaten	✓	–	–	–	–
Externe netwerkadapters	✓	–	–	–	–
Bluetooth	✓	–	–	–	–
Camera's en scanners	✓	–	–	–	–

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 verbindingsbussen

Als **Afhankelijk van verbindingsbus** waarde is geselecteerd voor de toegangsregel op apparaattype, staat het programma de toegang tot het apparaat toe of weigert afhankelijk van de verbindingsinterface. Regels die de toegang tot bussen toestaan, worden standaard aangemaakt voor alle verbindingsbussen in de classificatie van het onderdeel Apparaatcontrole.

Toegangsregels voor verbindingsbussen bepalen of de aansluiting van apparaten is toegestaan (de status ✓) of verboden (de status ⊘). De prioriteit van de toegangsregels van het apparaattype is hoger dan de prioriteit van de toegangsregels voor de verbindingsbus.

Toetsenbord en muis kunnen niet worden vergrendeld met Apparaatcontrole. Als u de toegang tot de USB-verbindingsbus verbiedt, blijft de gebruiker werken met een toetsenbord en muis die via USB zijn aangesloten. Het onderdeel BadUSB Attack Prevention is ontworpen om te voorkomen dat geïnfecteerde USB-apparaten zich voordoen als toetsenborden wanneer ze op de computer worden aangesloten.

Toegang tot apparaten beheren op type

Met Apparaatbeheer kunt u de toegang tot apparaten per type beheren. Het type apparaat wordt bepaald door het besturingssysteem wanneer het apparaat wordt aangesloten. U kunt het apparaattype opzoeken met het hulpprogramma Apparaatbeheer dat in het besturingssysteem is ingebouwd. Als u de toegang tot apparaten wilt beheren, moet u regels configureren. *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. U kunt geen apparaten toevoegen die niet door Apparaatcontrole kunnen worden geclassificeerd. De toegang tot zulke apparaten is voor alle gebruikers toegestaan.

Standaard staat Apparaatbeheer alle gebruikers toegang tot alle apparaten toe.

U kunt de toegang tot apparaten als volgt configureren:

- **Toestaan**.

  Kaspersky Endpoint Security geeft alle gebruikers volledige toegang tot apparaten.

- **Blokkeren**.

  Kaspersky Endpoint Security blokkeert apparaatverbindingen. Het programma staat toe: alleen vertrouwde apparaten om verbinding te maken.

- **Afhankelijk van verbindingsbus**.

  Kaspersky Endpoint Security bepaalt de verbindingsinterface van apparaten en beperkt de toegang tot apparaten op basis van hun busverbindingsstatus. Het programma staat ook toe: vertrouwde apparaten verbinden.

- **Volgens regels**.

  Voor sommige typen apparaten kunt u individuele gebruikers of een groep gebruikers aanwijzen die apparaten mogen gebruiken, een planning voor de toegang tot apparaten instellen en lees- en schrijfrechten configureren. Het programma staat ook toe: vertrouwde apparaten verbinden.

Wees voorzichtig bij het configureren van toegang tot apparaten van het type **Harde schijven**. Als u de toegang tot de systeemschijf blokkeert, kan het programma een crash (BSOD) veroorzaken bij het opstarten van het besturingssysteem.

Als een apparaat niet past in de classificatie Apparaatcontrole, kan de toegang tot een dergelijk apparaat niet worden beperkt.

Toegang tot apparaten beheren op type in de Beheerdersconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de beheerconsole **Policies**.
3. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
4. Selecteer **Security Controls** → **Apparaatcontrole** in het beleidsvenster.
5. Selecteer onder **Instellingen van Apparaatcontrole** het tabblad **Apparaattypen**.

   Het tabblad **Apparaattypen** toont toegangsregels voor alle apparaten die zijn opgenomen in de classificatie Apparaatcontrole.
6. Toegangsregels voor apparaten configureren:

   a. Selecteer de toegangsmodus: **Toestaan**, **Blokkeren**, **Afhankelijk van verbindingsbus**, **Volgens regels**.

   Om de modus **Volgens regels** te selecteren, dubbelklik om de eigenschappen van de toegangsregel te openen.

   b. Als u de **Afhankelijk van verbindingsbus** toegangsmodus selecteert, moet u toegangsregels voor verbindingsinterfaces configureren op het tabblad **Verbindingsbussen**.

   c. In het geval van opslagapparaten (bijvoorbeeld verwisselbare media) kunt u toegangsrechten voor individuele gebruikers configureren. U kunt ook een planning voor de toegang tot apparaten instellen en lees- en schrijfrechten configureren.

   U kunt apparaten toevoegen aan de vertrouwde lijst. *Vertrouwde apparaten* zijn apparaten waartoe gebruikers die in de instellingen voor vertrouwde apparaten zijn opgegeven altijd volledige toegang hebben.

   d. Indien nodig, de afdrukregels configureren.

   e. Indien nodig, regels voor toegang tot Bluetooth-apparaten configureren.

   f. Indien nodig, regels voor de wifi-verbinding van de computer configureren.
7. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Toegang tot apparaten per type beheren in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de Webconsole het tabblad **Asset management** → **Policies**.
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** → **Device Control**.
5. Selecteer onder **Device access rules** het tabblad **Devices and Wi-Fi networks**.

   De tabel bevat toegangsregels voor alle apparaten die aanwezig zijn in de classificatie van het onderdeel Apparaatcontrole.
6. Toegangsregels voor apparaten configureren:

   a. Selecteer de toegangsmodus: **Allow**, **Block**, **Depends on bus**, **Custom**.

   Als de toegangsmodus ontbreekt in het vervolgkeuzemenu, open de eigenschappen van de toegangsregel door te dubbelklikken op het type apparaat.

   b. Als u de **Depends on bus** toegangsmodus selecteert, moet u toegangsregels voor verbindingsinterfaces configureren op het tabblad **Connection buses**.

   c. In het geval van opslagapparaten (bijvoorbeeld verwisselbare media) kunt u toegangsrechten voor individuele gebruikers configureren. U kunt ook een planning voor de toegang tot apparaten instellen en lees- en schrijfrechten configureren.

   U kunt apparaten toevoegen aan de vertrouwde lijst. *Vertrouwde apparaten* zijn apparaten waartoe gebruikers die in de instellingen voor vertrouwde apparaten zijn opgegeven altijd volledige toegang hebben.

   d. Indien nodig, de afdrukregels configureren.

   e. Indien nodig, regels voor toegang tot Bluetooth-apparaten configureren.

   f. Indien nodig, regels voor de wifi-verbinding van de computer configureren.
7. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Toegang tot apparaten beheren in de programma-interface

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Apparaatcontrole** in het venster met de programma-instellingen.
3. Klik in het blok **Toegangsinstellingen** op de koppeling **Apparaten en wifinetwerken**.

   De tabel bevat toegangsregels voor alle apparaten die aanwezig zijn in de classificatie van het onderdeel Apparaatcontrole.
4. Toegangsregels voor apparaten configureren:

   a. Selecteer de toegangsmodus: **Toestaan**, **Blokkeren**, **Afhankelijk van verbindingsbus**, **Volgens regels**.

   Als de toegangsmodus ontbreekt in het vervolgkeuzemenu, open de eigenschappen van de toegangsregel door te dubbelklikken op het type apparaat.

b. Als u de **Afhankelijk van verbindingsbus** toegangsmodus selecteert, moet u toegangsregels voor verbindingsinterfaces configureren op het tabblad **Verbindingsbussen**.

c. In het geval van opslagapparaten (bijvoorbeeld verwisselbare media) kunt u toegangsrechten voor individuele gebruikers configureren. U kunt ook een planning voor de toegang tot apparaten instellen en lees- en schrijfrechten configureren.

U kunt apparaten toevoegen aan de vertrouwde lijst. *Vertrouwde apparaten* zijn apparaten waartoe gebruikers die in de instellingen voor vertrouwde apparaten zijn opgegeven altijd volledige toegang hebben.

d. Indien nodig, de afdrukregels configureren.

e. Indien nodig, regels voor toegang tot Bluetooth-apparaten configureren.

f. Indien nodig, regels voor de wifi-verbinding van de computer configureren.

5. Sla uw wijzigingen op.

Als een gebruiker daarom probeert toegang te krijgen tot een apparaat, blokkeert het programma de toegang in overeenstemming met de regels. Kaspersky Endpoint Security registreert ook een overeenkomstige gebeurtenis. Als u toegang wilt verlenen aan afzonderlijke apparaten, kunt u: voeg deze apparaten toe aan de lijst met vertrouwde apparaten.

Toegang tot apparaten beheren via de verbindingsbus

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 verbindingsbus wilt toestaan: **Toestaan** of **Blokkeren**.

   Als u de toegang tot de verbindingsbus hebt gewijzigd **Seriële poort** (COM) of **Parallelle poort** (LPT), moet u de computer opnieuw opstarten om de toegangsregel te activeren.
6. Sla uw wijzigingen op.

Differentiatie van gebruikersrechten voor apparaten

U kunt de gebruikersrechten configureren op type apparaat of op vertrouwde apparaten.

Differentiatie van gebruikersrechten op type apparaat

Met Apparaatcontrole kunt u de gebruikersrechten tot gegevens configureren op *opslagapparaten*. Voor dergelijke apparaten kunt u schrijf- en leesrechten configureren. Apparaatcontrole ondersteunt de volgende typen: *opslagapparaten*:

- Harde schijven.
- Verwisselbare schijven (inclusief USB-flashstations).
- Diskettes.
- Cd-/dvd-stations.
- Draagbare apparaten (MTP). Draagbare apparaten (MTP) zijn bijvoorbeeld mobiele apparaten, fotocamera's, mediaspelers, enzovoort.

Op deze manier kunt u bijvoorbeeld het gebruik van verwisselbare media alleen toestaan aan de groep beheerders. Voor andere apparaattypes kunt u de toegang voor alle gebruikers weigeren of toestaan. U kunt ook gebruikersrechten configureren om printers te gebruiken.

Gebruikersrechten voor gegevens op opslagapparaten configureren in de Beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de beheerconsole **Policies**.
3. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
4. Selecteer **Security Controls** → **Apparaatcontrole** in het beleidsvenster.
5. Selecteer onder **Instellingen van Apparaatcontrole** het tabblad **Apparaattypen**.

   Het tabblad **Apparaattypen** toont toegangsregels voor alle apparaten die zijn opgenomen in de classificatie Apparaatcontrole.
6. Om toegangsregels voor opslagapparaten te configureren, dubbelklik om de lijst met regels te openen.
7. Configureer de toegangsregel voor opslagapparaten:

   a. In het blok **Toegangsregels**, klikt u op de knop **Toevoegen**.

      Dit opent een venster voor het toevoegen van een nieuwe regel voor toegang tot opslagapparaten.

   b. Stel in het veld **Prioriteit van regel** de prioriteit *regel schrijven* in. 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 ledereen en de machtiging lezen/schrijven aan de groep administrators. Om dit te doen, wijst u een prioriteit van 1 toe voor de groep administrators en een prioriteit van 0 voor de groep ledereen.

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.

c. Selecteer onder **Regel voor gebruikers en groepen** gebruikers of groepen gebruikers. U kunt gebruikers selecteren in Active Directory, in de lijst van accounts in Kaspersky Security Center, of door handmatig een lokale gebruikersnaam in te voeren. Kaspersky raadt aan om locale gebruikersaccounts alleen in speciale gevallen te gebruiken, wanneer het niet mogelijk is om domeingebruikersaccounts te gebruiken.

d. Klik op **OK**.

8. Configureer onder **Schema's voor de geselecteerde toegangsregel** een toegangsschema voor opslagapparaten voor gebruikers.

   U kunt bijvoorbeeld gebruikers toestaan opslagapparaten alleen tijdens werkuren te gebruiken.

9. De toegangsmachtigingen van gebruikers tot opslagapparaten configureren in de bestandsverkenner (**Lezen** / **Schrijven**).

10. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Gebruikersrechten voor gegevens op opslagapparaten configureren in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de Webconsole het tabblad **Asset management** → **Policies**.

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** → **Device Control**.

5. Open in het blok **Device access rules** in de tabel met toegangsregels, de eigenschappen van de toegangsregels voor opslagapparaten.

6. Selecteer in het blok **Device access rules Custom**.

7. Configureer de toegangsregel voor opslagapparaten:

   a. In het blok **Users and their rights**, klikt u op de knop **Add**.

   Dit opent een venster voor het toevoegen van een nieuwe regel voor toegang tot opslagapparaten.

   b. Stel in het veld **Priority** de prioriteit *regel schrijven* in. 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 administrators. Om dit te doen, wijst u een prioriteit van 1 toe voor de groep administrators 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.

c. Selecteer onder **User or group** gebruikers of groepen gebruikers. U kunt gebruikers selecteren in Active Directory, in de lijst van accounts in Kaspersky Security Center, of door handmatig een lokale gebruikersnaam in te voeren. Kaspersky raadt aan om locale gebruikersaccounts alleen in speciale gevallen te gebruiken, wanneer het niet mogelijk is om domeingebruikersaccounts te gebruiken.

d. Configureer onder **Access schedule** een toegangsschema voor opslagapparaten voor gebruikers.

U kunt bijvoorbeeld gebruikers toestaan opslagapparaten alleen tijdens werkuren te gebruiken.

e. De toegangsmachtigingen van gebruikers tot opslagapparaten configureren in de bestandsverkenner (**Read** / **Write**).

f. Klik op **Save**.

8. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Gebruikersrechten voor gegevens op opslagapparaten configureren in de programma-interface

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

2. Selecteer **Security Controls** → **Apparaatcontrole** in het venster met de programma-instellingen.

3. Klik in het blok **Toegangsinstellingen** op de koppeling **Apparaten en wifinetwerken**.

De tabel bevat toegangsregels voor alle apparaten die aanwezig zijn in de classificatie van het onderdeel Apparaatcontrole.

4. Om toegangsregels voor opslagapparaten te configureren, klik met de rechtermuisknop om de lijst met regels te openen.

5. Configureer de toegangsregel voor opslagapparaten:

a. In het blok **Gebruikersrechten**, klikt u op de knop **Toevoegen**.

Dit opent een venster voor het toevoegen van een nieuwe regel voor toegang tot opslagapparaten.

b. Stel in het veld **Prioriteit** de prioriteit *regel schrijven* in. 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 administrators. Om dit te doen, wijst u een prioriteit van 1 toe voor de groep administrators 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.

c. Selecteer onder **Gebruikers** gebruikers of groepen gebruikers. U kunt gebruikers in Active Directory selecteren of handmatig een lokale gebruikersnaam invoeren. Kaspersky raadt aan om locale gebruikersaccounts alleen in speciale gevallen te gebruiken, wanneer het niet mogelijk is om domeingebruikersaccounts te gebruiken.

d. Klik op **OK**.

6. Configureer onder **Schema voor toegang tot apparaten** een toegangsschema voor opslagapparaten voor gebruikers.

   U kunt bijvoorbeeld gebruikers toestaan opslagapparaten alleen tijdens werkuren te gebruiken.

7. De toegangsmachtigingen van gebruikers tot opslagapparaten configureren in de bestandsverkenner (**Lezen** / **Schrijven**).

8. Sla uw wijzigingen op.

Differentiatie van gebruikersrechten voor 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. U kunt configureren: gebruikersrechten in de eigenschappen van het vertrouwde apparaat.

Toegang tot mobiele apparaten beheren

Met Kaspersky Endpoint Security kunt u de toegang tot gegevens beheren op mobiele apparaten met Android en iOS. Mobiele apparaten behoren tot de categorie draagbare apparaten (MTP). Als u de gegevenstoegang tot mobiele apparaten wilt configureren, moet u daarom de toegangsinstellingen voor draagbare apparaten (MTP) bewerken.

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 en de geselecteerd USB-verbindingsmodus. Met Kaspersky Endpoint Security kunt u individuele toegangsmachtigingen configureren voor gegevens op mobiele apparaten in ADB-programma's, iTunes of bestandsbeheer. In alle andere gevallen biedt Apparaatbeheer toegang tot mobiele apparaten in overeenstemming met de toegangsregels voor draagbare apparaten (MTP).

Toegang tot mobiele apparaten

Mobiele apparaten behoren tot de categorie draagbare apparaten (MTP). Daarom zijn de instellingen voor hen hetzelfde. U kunt een van de volgende toegangsmodi tot mobiele apparaten selecteren:

- **Toestaan** ✓. Met Kaspersky Endpoint Security krijgt u volledige toegang tot mobiele apparaten. U kunt bestanden op mobiele apparaten openen, maken, wijzigen, kopiëren of verwijderen met behulp van bestandsbeheer of ADB- en iTunes-toepassingen. U kunt de batterij van het apparaat ook opladen door het mobiele apparaat aan te sluiten op een USB-poort van de computer.

- **Blokkeren** ⊘. Kaspersky Endpoint Security beperkt de toegang tot mobiele apparaten in bestandsbeheer en ADB- en iTunes-programma's. Het programma geeft alleen toegang tot vertrouwde mobiele apparaten. U kunt de batterij van het apparaat ook opladen door het mobiele apparaat aan te sluiten op een USB-poort van de computer.

- **Afhankelijk van verbindingsbus**. Kaspersky Endpoint Security maakt het mogelijk om verbinding te maken met mobiele apparaten afhankelijk van de USB -verbindingsstatus (**Toestaan** of **Blokkeren**).
- **Volgens regels**. Kaspersky Endpoint Security beperkt de toegang tot mobiele apparaten in overeenstemming met de regels. In de regels kunt u toegangsrechten (lezen/schrijven) configureren, gebruikers of een groep gebruikers selecteren voor toegang tot mobiele apparaten (MTP) en een toegangsschema voor mobiele apparaten configureren. U kunt ook de toegang beperken tot gegevens op mobiele apparaten die de ADB- en iTunes-programma's gebruiken.

Toegangsregels voor mobiele apparaten configureren

Toegangsregels voor draagbare apparaten (MTP), ADB-apparaten en iTunes-apparaten zijn anders geconfigureerd. Voor draagbare apparaten (MTP) en ADB-apparaten kunt u regels configureren voor individuele gebruikers of groepen gebruikers en een schema maken voor wanneer de regels worden ingeschakeld. Voor iTunes-apparaten kunt u dat niet doen. U kunt alleen toegang tot gegevens toestaan of weigeren via het iTunes-programma voor alle gebruikers.

Toegangsregels voor mobiele apparaten configureren in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Security Controls** → **Apparaatcontrole** in het beleidsvenster.
4. Selecteer onder **Instellingen van Apparaatcontrole** het tabblad **Apparaattypen**.

   De tabel bevat toegangsregels voor alle apparaten die aanwezig zijn in de classificatie van het onderdeel Apparaatcontrole.
5. Configureer in het contextmenu voor het apparaattype **Draagbare apparaten (MTP)** de toegangsmodus voor mobiele apparaten: **Toestaan**, **Blokkeren**, of **Afhankelijk van verbindingsbus**.
6. Om toegangsregels voor mobiele apparaten te configureren, dubbelklikt u om de lijst met regels te openen.
7. Configureer de toegangsregel voor mobiele apparaten:

   a. In het blok **Toegangsregels**, klikt u op de knop **Toevoegen**.

   Dit opent een venster voor het toevoegen van een nieuwe regel voor toegang tot mobiele apparaten.

   b. Stel in het veld **Prioriteit** de schrijfprioriteit van de regel in. Een regel bevat de volgende kenmerken: gebruikersaccount, planning, machtigingen (lezen/schrijven/ADB-toegang) 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 administrators. Om dit te doen, wijst u een prioriteit van 1 toe voor de groep administrators 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.

c. Selecteer onder **Regel voor gebruikers en groepen** gebruikers of groepen gebruikers. U kunt gebruikers selecteren in Active Directory, in de lijst van accounts in Kaspersky Security Center, of door handmatig een lokale gebruikersnaam in te voeren. Kaspersky raadt aan om locale gebruikersaccounts alleen in speciale gevallen te gebruiken, wanneer het niet mogelijk is om domeingebruikersaccounts te gebruiken.

d. Klik op **OK**.

8. Configureer onder **Schema's voor de geselecteerde toegangsregel** een toegangsschema voor mobiele apparaten voor gebruikers.

   Het is niet mogelijk om een afzonderlijk toegangsschema te configuereren voor ADB-apparaten. U kunt een algemeen toegangsschema configureren voor ADB-apparaten en draagbare apparaten (MTP).

9. De toegangsmachtigingen van gebruikers tot mobiele apparaten configureren in de bestandsverkenner (**Lezen** / **Schrijven**).

10. Configureer de toegang tot gegevens op een mobiel apparaat via het ADB-programma met behulp van het selectievakje **Toegang via ADB**.

    Als het selectievakje is uitgeschakeld en het mobiele apparaat is aangesloten, kan het ADB-progrmma het apparaat niet detecteren wanneer het mobiele apparaat is verbonden.

11. Configureer onder **Toegang via iTunes** toegang tot gegevens op het mobiele apparaat via het iTunes-programma.

    Kaspersky Endpoint Security past de toegangsinstellingen voor mobiele apparaten via het iTunes-programma toe voor alle gebruikers. Het is niet mogelijk om een afzonderlijk toegangsschema te configuereren voor iTunes-apparaten.

12. Sla uw wijzigingen op.

Toegangsregels voor mobiele apparaten configureren in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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** → **Device Control**.

5. Klik in het blok **Device access rules** op de koppeling **Devices and Wi-Fi networks**.

   De tabel bevat toegangsregels voor alle apparaten die aanwezig zijn in de classificatie van het onderdeel Apparaatcontrole.

6. Selecteer het apparaattype **Portable devices (MTP)**.

   Dit opent de toegangsregels voor draagbare apparaten (MTP).

7. Configureer onder de toegangsmodus voor mobiele apparaten: **Allow**, **Block**, **Depends on bus**, of **Custom**.

8. Gebruik de schakelaar **Access via iTunes for all users ENABLED** om de toegang tot gegevens op het mobiele apparaat via de iTunes-programma te configureren.

   Kaspersky Endpoint Security past de toegangsinstellingen voor mobiele apparaten via het iTunes-programma toe voor alle gebruikers. Het is niet mogelijk om een afzonderlijk toegangsschema te configuereren voor iTunes-apparaten.

9. Als u de modus **Custom** selecteert, moet u toegangsregels toevoegen voor apparaten. Klik hiervoor onder **Users and their rights** op de knop **Add** en configureer de toegangsregel voor mobiele apparaten:

   a. Stel in het veld **Priority** de schrijfprioriteit van de regel in. Een regel bevat de volgende kenmerken: gebruikersaccount, planning, machtigingen (lezen/schrijven/ADB-toegang) 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 administrators. Om dit te doen, wijst u een prioriteit van 1 toe voor de groep administrators 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.

   b. Selecteer onder **User or group** gebruikers of groepen gebruikers voor toegang tot mobiele apparaten. U kunt gebruikers selecteren in Active Directory, in de lijst van accounts in Kaspersky Security Center, of door handmatig een lokale gebruikersnaam in te voeren. Kaspersky raadt aan om locale gebruikersaccounts alleen in speciale gevallen te gebruiken, wanneer het niet mogelijk is om domeingebruikersaccounts te gebruiken.

   c. Configureer onder **Access schedule** een toegangsschema voor mobiele apparaten voor gebruikers.

      Het is niet mogelijk om een afzonderlijk toegangsschema te configuereren voor ADB-apparaten. U kunt een algemeen toegangsschema configureren voor ADB-apparaten en draagbare apparaten (MTP).

   d. De toegangsmachtigingen van gebruikers tot mobiele apparaten configureren in de bestandsverkenner (**Read** / **Write**).

   e. Configureer de toegang tot gegevens op een mobiel apparaat via het ADB-programma met behulp van het selectievakje **Access via ADB**.

      Als het selectievakje is uitgeschakeld en het mobiele apparaat is aangesloten, kan het ADB-progrmma het apparaat niet detecteren wanneer het mobiele apparaat is verbonden.

10. Sla uw wijzigingen op.

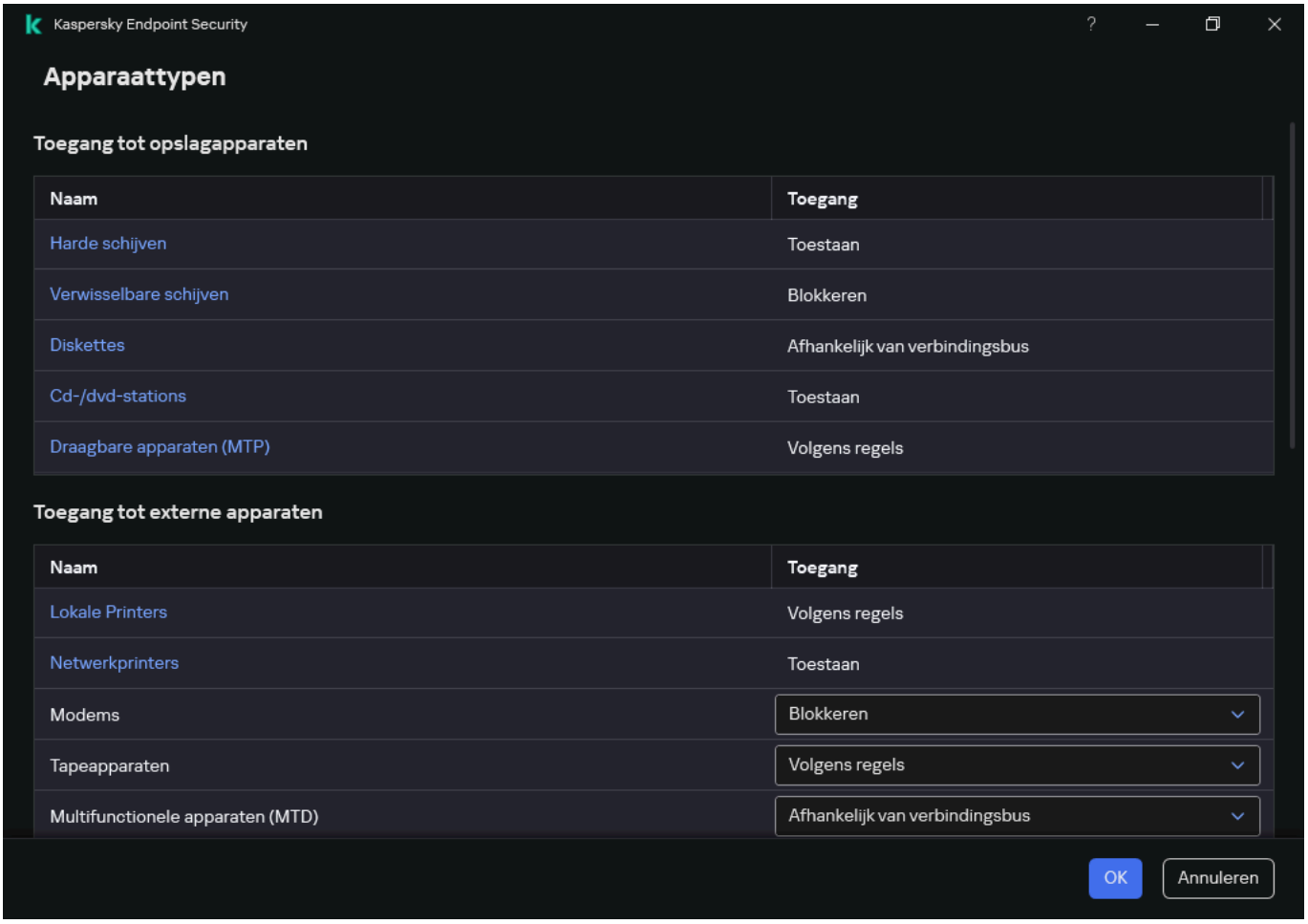
Toegangsregels voor mobiele apparaten configureren in de programma-interface

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.



Typen apparaten in het onderdeel Apparaatcontrole

4. Klik in het blok **Toegang tot opslagapparaten** op de koppeling **Draagbare apparaten (MTP)**.

   Hiermee wordt een venster geopend met de toegangsregels voor draagbare apparaten (MTP).

5. Configureer onder **Toegang** de toegangsmodus voor mobiele apparaten: **Toestaan**, **Blokkeren**, **Afhankelijk van verbindingsbus**, of **Volgens regels**.

6. Als u de modus **Volgens regels** selecteert, moet u toegangsregels toevoegen voor apparaten:

   a. In het blok **Gebruikersrechten**, klikt u op de knop **Toevoegen**.

      Dit opent een venster voor het toevoegen van een nieuwe regel voor toegang tot mobiele apparaten.

   b. Stel in het veld **Prioriteit** de schrijfprioriteit van de regel in. Een regel bevat de volgende kenmerken: gebruikersaccount, planning, machtigingen (lezen/schrijven/ADB-toegang) 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 administrators. Om dit te doen, wijst u een prioriteit van 1 toe voor de groep administrators 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.

c. Zet onder **Status** de toegangsregels aan voor mobiele apparaten.

d. Configureer onder **Toegangsregels** toegangsmachtigingen voor mobiele apparaten voor gebruikers.

- De toegangsmachtigingen van gebruikers tot mobiele apparaten configureren in de bestandsverkenner (**Lezen** / **Schrijven**).
- Configureer de toegang tot gegevens op een mobiel apparaat via het ADB-programma met behulp van het selectievakje **Toegang via ADB**.

  Als het selectievakje is uitgeschakeld en het mobiele apparaat is aangesloten, kan het ADB-progrmma het apparaat niet detecteren wanneer het mobiele apparaat is verbonden.

e. Selecteer onder **Gebruikers** gebruikers of groepen gebruikers voor toegang tot mobiele apparaten. U kunt gebruikers selecteren in Active Directory, in de lijst van accounts in Kaspersky Security Center, of door handmatig een lokale gebruikersnaam in te voeren. Kaspersky raadt aan om locale gebruikersaccounts alleen in speciale gevallen te gebruiken, wanneer het niet mogelijk is om domeingebruikersaccounts te gebruiken.

f. Configureer onder **Schema voor toegang tot apparaten** een toegangsschema voor apparaten voor gebruikers.

> Het is niet mogelijk om een afzonderlijk toegangsschema te configuereren voor ADB-apparaten. U kunt een algemeen toegangsschema configureren voor ADB-apparaten en draagbare apparaten (MTP).

g. Configureer onder **Toegang via iTunes** toegang tot gegevens op het mobiele apparaat via het iTunes-programma.

> Kaspersky Endpoint Security past de toegangsinstellingen voor mobiele apparaten via het iTunes-programma toe voor alle gebruikers. Het is niet mogelijk om een afzonderlijk toegangsschema te configuereren voor iTunes-apparaten.

7. Sla uw wijzigingen op.

Als gevolg hiervan is de toegang van gebruikers tot mobiele apparaten beperkt in overeenstemming met de regels. Als u de toegang tot mobiele apparaten in de ADB- en iTunes-programma's hebt verboden, kunnen de ADB- en iTunes-programma's het mobiele apparaat niet detecteren wanneer u een mobiel apparaat aansluit.

Vertrouwde mobiele apparaten

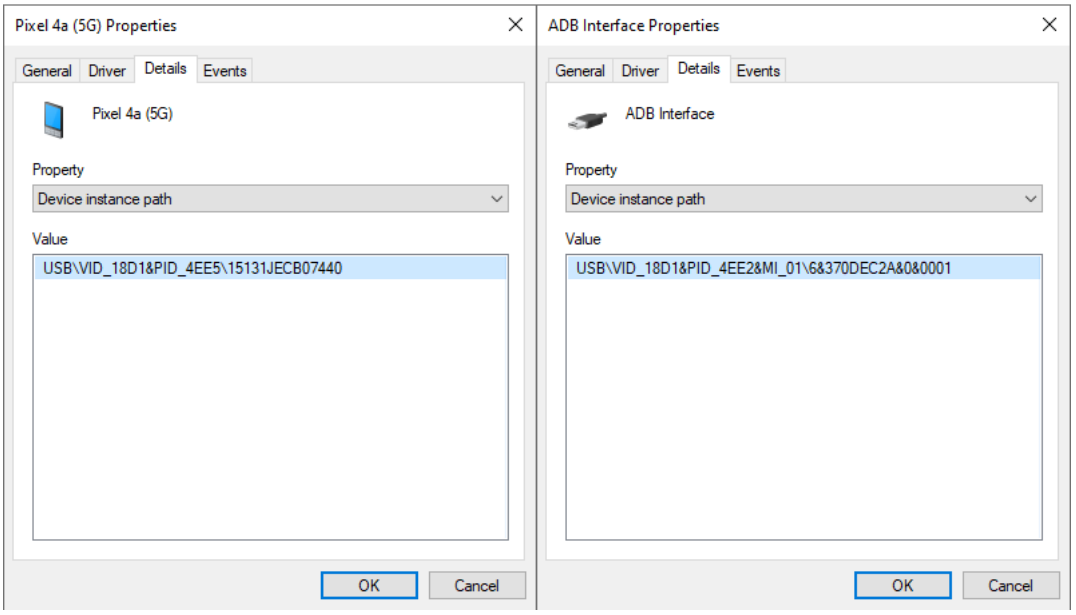
Vertrouwde apparaten zijn apparaten waartoe gebruikers die in de instellingen voor vertrouwde apparaten zijn opgegeven altijd volledige toegang hebben.

De procedure voor het toevoegen van een vertrouwd mobiel apparaat is precies hetzelfde als voor andere typen vertrouwde apparaten. U kunt een mobiel apparaat toevoegen op basis van ID of apparaatmodel.

Als u een vertrouwd mobiel apparaat per ID wilt toevoegen, hebt u een unieke ID (Hardware ID – HWID) nodig. U kunt de ID vinden in apparaateigenschappen met behulp van hulpprogramma's van het besturingssysteem (zie onderstaande afbeelding). Met het hulpprogramma Apparaatbeheer kunt u dit doen. ID's van draagbare apparaten (MTP) en Itunes- en ADB-apparaten zijn verschillend, zelfs voor hetzelfde mobiele apparaat. De ID van een draagbaar apparaat (MTP) kan er als volgt uitzien: `15131JECB07440`. De ID van een ADB-apparaat kan er als volgt uitzien: `6&370DEC2A&0&0001`. Apparaten toevoegen per ID is handig als u meerdere specifieke apparaten wilt toevoegen. U kunt ook maskers gebruiken.

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.

Als u een vertrouwd mobiel apparaat per apparaatmodel wilt toevoegen, hebt u de Vendor ID (VID) en de Product ID (PID) nodig. U kunt de ID's vinden in apparaateigenschappen met behulp van hulpprogramma's van het besturingssysteem (zie onderstaande afbeelding). Sjabloon voor de invoer van het VID en PID: `VID_18D1&PID_4EE5`. 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.



Apparaat-ID in Apparaatbeheer

Toegang tot Bluetooth apparaten beheren

Kaspersky Endpoint Security kan de toegang tot Bluetooth apparaten beheren. Bluetooth apparaten zijn bijvoorbeeld draadloze toetsenborden, muizen, headsets, printers, enz. Je kunt Bluetooth ook gebruiken voor communicatie met bijvoorbeeld een mobiel apparaat.

Wanneer Bluetooth apparaten zijn verbonden of losgekoppeld, kan het programma meerdere gebeurtenissen over het apparaat aanmaken. De reden is dat het besturingssysteem een Bluetooth apparaat kan detecteren als meerdere apparaten van verschillende typen. Kaspersky Endpoint Security beheert ook de Bluetooth-adapter waarmee het apparaat is verbonden als een afzonderlijk apparaat. Daarom maakt het programma voor elk van de gedetecteerde apparaten een gebeurtenis aan.

U kunt een van de volgende toegangsmodi tot Bluetooth apparaten selecteren:

- **Toestaan en niet registreren** . Kaspersky Endpoint Security maakt verbinding met alle Bluetooth apparaten mogelijk en slaat geen informatie over de verbinding op in het gebeurtenislogboek. U kunt Bluetooth-invoerapparaten (toetsenborden, muizen, enz.) aansluiten, gegevens verzenden via Bluetooth, andere Bluetooth apparaten beheren (headset, hoofdtelefoon, enz.).

- **Toestaan** . Kaspersky Endpoint Security maakt verbinding met alle Bluetooth apparaten mogelijk. U kunt Bluetooth-invoerapparaten (toetsenborden, muizen, enz.) aansluiten, gegevens verzenden via Bluetooth, andere Bluetooth apparaten beheren (headset, hoofdtelefoon, enz.).

- **Blokkeren** . Kaspersky Endpoint Security beperkt toegang tot Bluetooth-apparaten. U kunt toestaan dat alleen Bluetooth-invoerapparaten (de Human Interface Devices-klasse) verbinding kunnen maken. Deze apparaten omvatten toetsenborden, muisapparaten, joysticks, enz.

Het is niet mogelijk om een lijst met vertrouwde Bluetooth apparaten aan te maken. Als u beperkte toegang tot Bluetooth apparaten heeft, kunt u alleen verbinding maken met Bluetooth-invoerapparaten.

Toegangsregels voor Bluetooth apparaten configureren in de Beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de beheerconsole **Policies**.
3. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
4. Selecteer **Security Controls** → **Apparaatcontrole** in het beleidsvenster.
5. Selecteer onder **Instellingen van Apparaatcontrole** het tabblad **Apparaattypen**.

   De tabel bevat toegangsregels voor alle apparaten die aanwezig zijn in de classificatie van het onderdeel Apparaatcontrole.
6. Configureer in het contextmenu voor het apparaattype **Bluetooth** de toegangsmodus voor Bluetooth apparaten: **Toestaan** , **Blokkeren** , of **Toestaan en niet registreren** .
7. Als u de **Blokkeren**-modus selecteert, kunt u toestaan dat alleen Bluetooth-invoerapparaten (toetsenborden, muizen, enz.) worden aangesloten. Om dit te doen, onder **Uitzonderingen**, selecteer het selectievakje **Invoerapparaten (muizen en toetsenborden)**.
8. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Toegangsregels voor Bluetooth apparaten configureren in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de Webconsole het tabblad **Asset management** → **Policies**.
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** → **Device Control**.

5. Klik in het blok **Device access rules** op de koppeling **Devices and Wi-Fi networks**.

   De tabel bevat toegangsregels voor alle apparaten die aanwezig zijn in de classificatie van het onderdeel Apparaatcontrole.

6. Selecteer het apparaattype **Bluetooth devices**.

   Hiermee worden de toegangsinstellingen voor het Bluetooth apparaat geopend.

7. Configureer de toegangsmodus voor het Bluetooth apparaat: **Allow**, **Block**, **Allow and do not log**.

8. Als u de **Block**-modus selecteert, kunt u toestaan dat alleen Bluetooth-invoerapparaten (toetsenborden, muizen, enz.) worden aangesloten. Om dit te doen, onder **Exclusions**, selecteer het selectievakje **Input devices (mice and keyboards)**.

9. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

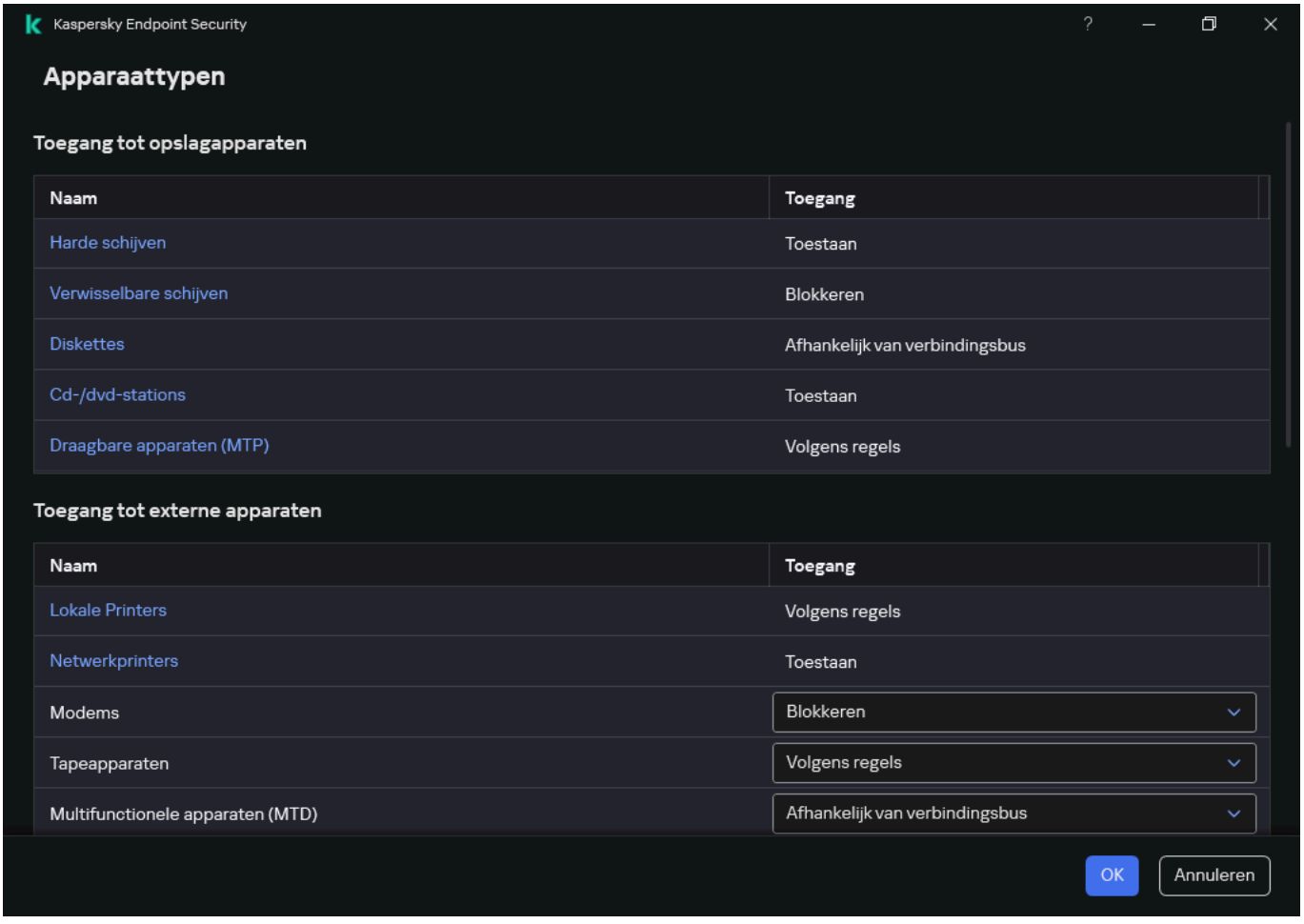
Toegangsregels voor Bluetooth apparaten configureren in de programma-interface

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.



Typen apparaten in het onderdeel Apparaatcontrole

4. Klik in het blok **Toegang tot externe apparaten** op de koppeling **Bluetooth**.

   Hiermee worden de toegangsinstellingen voor het Bluetooth apparaat geopend.

5. Configureer onder **Toegang** de toegangsmodus voor Bluetooth apparaten: **Toestaan**, **Blokkeren**, **Sta toe en registreer niet**.

6. Als u de **Blokkeren**-modus selecteert, kunt u toestaan dat alleen Bluetooth-invoerapparaten (toetsenborden, muizen, enz.) worden aangesloten. Om dit te doen, onder **Uitzonderingen**, selecteer het selectievakje **Invoerapparaten (muizen en toetsenborden)**.

7. Sla uw wijzigingen op.

Afdrukbeheer

Afdrukbeheer wordt niet ondersteund op Arm-computers.

U kunt Afdrukbeheer gebruiken om gebruikerstoegang tot lokale en netwerkprinters te configureren.

Beheer van lokale printers

Kaspersky Endpoint Security maakt het configureren van toegang tot lokale printers op twee niveaus mogelijk: *verbinden* en *afdrukken*.

Kaspersky Endpoint Security regelt de lokale printerverbinding via de volgende bussen: USB, Seriële poort (COM), parallelle poort (LPT).

Kaspersky Endpoint Security controleert de verbinding van lokale printers met COM- en LPT-poorten alleen op busniveau. Om printerverbindingen via COM- en LPT-poorten te voorkomen, moet u dus de toegangsmodus Afhankelijk van verbindingsbus selecteren voor lokale printers en verbindingen met COM- en LPT-bussen verbieden.

Voor printers die via USB zijn aangesloten, regelt het programma op twee niveaus: apparaattype (lokale printers) en verbindingsbus (USB).

U kunt een van de volgende toegangsmodi tot lokale printers via USB selecteren:

- **Toestaan** ✓. Kaspersky Endpoint Security verleent volledige toegang tot lokale printers aan alle gebruikers. Gebruikers kunnen printers aansluiten en documenten afdrukken met behulp van de middelen die het besturingssysteem biedt.

- **Blokkeren** ⊘. Kaspersky Endpoint Security blokkeert de verbinding van lokale printers. Het programma staat alleen verbinding toe met vertrouwde printers.

- **Afhankelijk van verbindingsbus**. Kaspersky Endpoint Security staat toe verbinding te maken met lokale printers in overeenstemming met de status van de USB-busverbinding (**Toestaan** or **Blokkeren**).
- **Volgens regels**. Om afdrukken te beheren, moet u *printingregels* toevoegen. In de regels kunt u gebruikers of een groep gebruikers selecteren waarvoor u toegang tot het afdrukken van documenten op lokale printers wilt toestaan of blokkeren.

Beheer van netwerkprinters

Met Kaspersky Endpoint Security kunt u toegang configureren tot afdrukken op netwerkprinters. U kunt een van de volgende toegangsmodi naar netwerkprinters selecteren:

- **Toestaan en niet registreren**. Kaspersky Endpoint Security heeft geen controle over het afdrukken op netwerkprinters. Het programma verleent alle gebruikers toegang tot afdrukken en slaat geen informatie over het afdrukken op in het gebeurtenislogboek.
- **Toestaan**. Kaspersky Endpoint Security geeft alle gebruikers toegang tot afdrukken op netwerkprinters.
- **Blokkeren**. Kaspersky Endpoint Security beperkt de toegang tot netwerkprinters voor alle gebruikers. Het programma geeft alleen toegang tot vertrouwde printers.
- **Volgens regels**. Kaspersky Endpoint Security verleent toegang tot afdrukken in overeenstemming met de afdrukregels. In de regels kunt u gebruikers of een groep gebruikers selecteren die documenten wel of niet mogen afdrukken op een netwerkprinter.

Afdrukregels voor printers toevoegen

Een afdrukregel toevoegen in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Security Controls** → **Apparaatcontrole** in het beleidsvenster.
4. Selecteer onder **Instellingen van Apparaatcontrole** het tabblad **Apparaattypen**.

   De tabel bevat toegangsregels voor alle apparaten die aanwezig zijn in de classificatie van het onderdeel Apparaatcontrole.
5. In het contextmenu voor de apparaattypes **Lokale printers** en **Netwerkprinters**, configureert u de toegangsmodus voor de relevante printers: **Toestaan**, **Blokkeren**, **Toestaan en niet registreren** (alleen voor netwerkprinters) of **Afhankelijk van verbindingsbus** (alleen voor lokale printers).
6. Als u afdrukregels wilt configureren op lokale en netwerkprinters, dubbelklik dan op de lijsten met regels om deze te openen.
7. Selecteer **Volgens regels** als de toegangsmodus voor printers.

8. Selecteer de gebruikers of groep gebruikers waarop u de regel voor afdrukken wilt toepassen.

    a. Klik op **Toevoegen**.

    Dit opent een venster voor het toevoegen van een nieuwe regel voor afdrukken.

    b. Wijs een prioriteit aan de regel toe. Een regel bevat de volgende kenmerken: gebruikersaccount, actie (toestaan/blokkeren) 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 administrators. Om dit te doen, wijst u een prioriteit van 1 toe voor de groep administrators 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.

    c. Configureer onder **Actie** de gebruikerstoegang om af te drukken op de printer.

    d. Klik **Gebruikers en groepen** en selecteer gebruikers of groepen gebruikers voor toegang tot afdrukken. U kunt gebruikers selecteren in Active Directory, in de lijst van accounts in Kaspersky Security Center, of door handmatig een lokale gebruikersnaam in te voeren. Kaspersky raadt aan om locale gebruikersaccounts alleen in speciale gevallen te gebruiken, wanneer het niet mogelijk is om domeingebruikersaccounts te gebruiken.

    e. Klik op **OK**.

9. Sla uw wijzigingen op.

Een aangepaste regel voor afdrukking toevoegen in de Webconsole en de Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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** → **Device Control**.

5. Klik in het blok **Device access rules** op de koppeling **Devices and Wi-Fi networks**.

    De tabel bevat toegangsregels voor alle apparaten die aanwezig zijn in de classificatie van het onderdeel Apparaatcontrole.

6. Selecteer het apparaattype **Local printers** of **Network printers**.

    Hiermee worden de toegangsregels voor de printer geopend.

7. Configureer de toegangsmodus voor de relevante printers: **Allow**, **Block**, **Allow and do not log** (alleen voor netwerkprinters), **Depends on bus** (alleen voor lokale printers) of **Custom**.

8. Als u de modus **Custom** selecteert, moet u regels voor afdrukken toevoegen voor lokale of netwerkprinters. Klik hiervoor op de knop **Add** in de tabel met afdrukregels.

    Dit opent de instellingen van de nieuwe afdrukregel.

9. Wijs een prioriteit aan de regel toe. Een regel bevat de volgende kenmerken: gebruikersaccount, actie (toestaan/blokkeren) 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 administrators. Om dit te doen, wijst u een prioriteit van 1 toe voor de groep administrators 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.

10. Configureer onder **Action** de gebruikerstoegang om af te drukken op de printer.

11. Selecteer onder **User or group** gebruikers of groepen gebruikers voor toegang tot afdrukken. U kunt gebruikers selecteren in Active Directory, in de lijst van accounts in Kaspersky Security Center, of door handmatig een lokale gebruikersnaam in te voeren. Kaspersky raadt aan om locale gebruikersaccounts alleen in speciale gevallen te gebruiken, wanneer het niet mogelijk is om domeingebruikersaccounts te gebruiken.

12. Sla uw wijzigingen op.

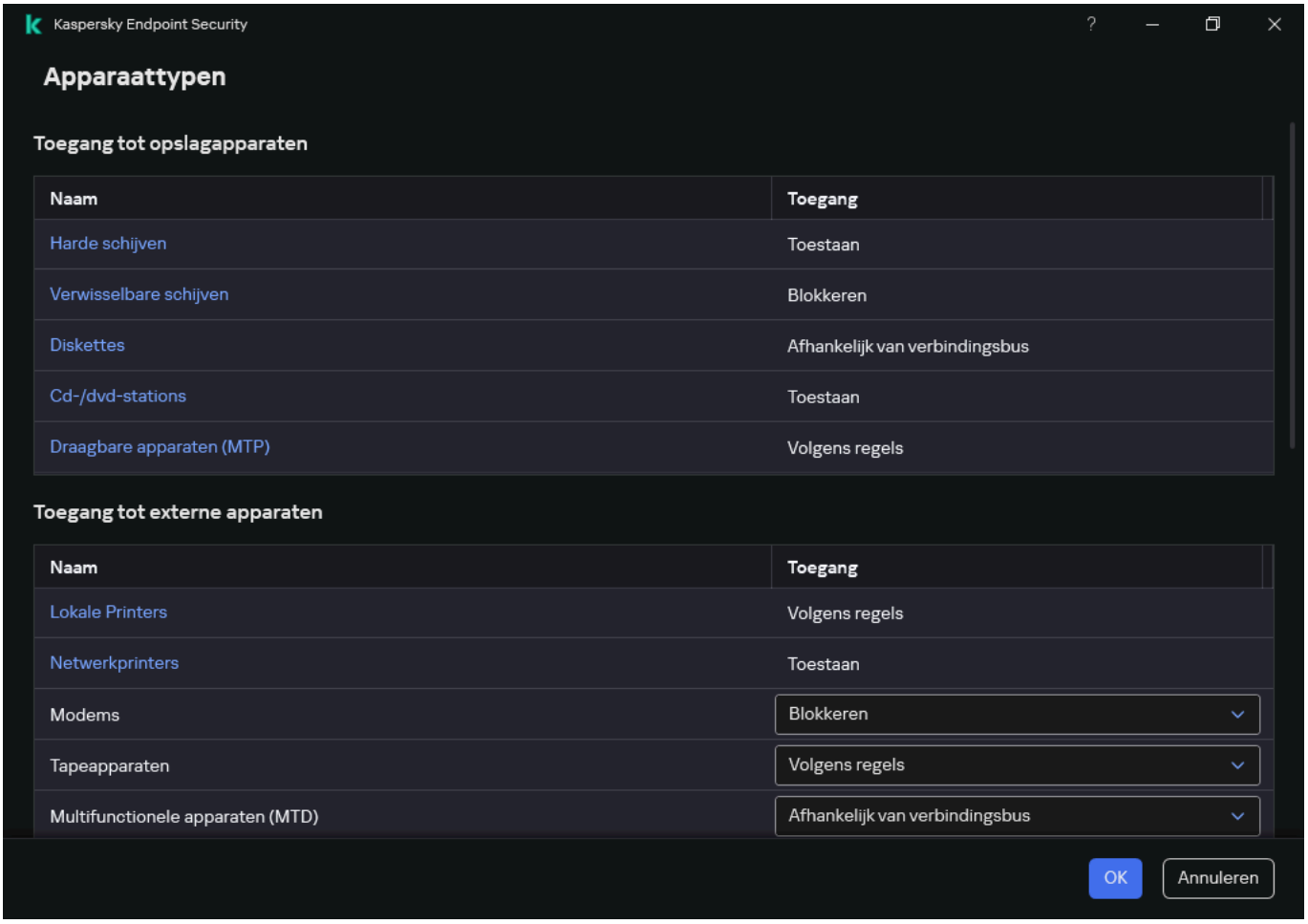
Een afdrukregel maken in de programma-interface

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.



Typen apparaten in het onderdeel Apparaatcontrole

4. Klik onder **Toegang tot externe apparaten** op **Lokale Printers** of **Netwerkprinters**.

   Dit opent een venster met de toegangsregels voor de printer.

5. Configureer onder **Toegang tot lokale printers** of **Toegang tot netwerkprinters** de toegangsmodus voor printers: **Toestaan**, **Blokkeren**, **Sta toe en registreer niet** (alleen voor netwerkprinters), **Afhankelijk van verbindingsbus** (alleen voor lokale printers) of **Volgens regels**.

6. Als u de modus **Volgens regels** selecteert, moet u regels voor afdrukken toevoegen voor printers. Selecteer de gebruikers of groep gebruikers waarop u de regel voor afdrukken wilt toepassen.

   a. Klik op **Toevoegen**.

      Dit opent een venster voor het toevoegen van een nieuwe regel voor afdrukken.

   b. Wijs een prioriteit aan de regel toe. Een regel bevat de volgende kenmerken: gebruikersaccount, Machtigingen (toestaan/blokkeren) 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 ledereen en de machtiging lezen/schrijven aan de groep administrators. Om dit te doen, wijst u een prioriteit van 1 toe voor de groep administrators en een prioriteit van 0 voor de groep ledereen.

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.

c. Condefigureer onder **Actie** gebruikersmachtigingen voor toegang tot afdrukken.

d. Selecteer onder **Gebruikers en groepen** gebruikers of groepen gebruikers voor toegang tot afdrukken. U kunt gebruikers selecteren in Active Directory, in de lijst van accounts in Kaspersky Security Center, of door handmatig een lokale gebruikersnaam in te voeren. Kaspersky raadt aan om locale gebruikersaccounts alleen in speciale gevallen te gebruiken, wanneer het niet mogelijk is om domeingebruikersaccounts te gebruiken.

7. Sla uw wijzigingen op.

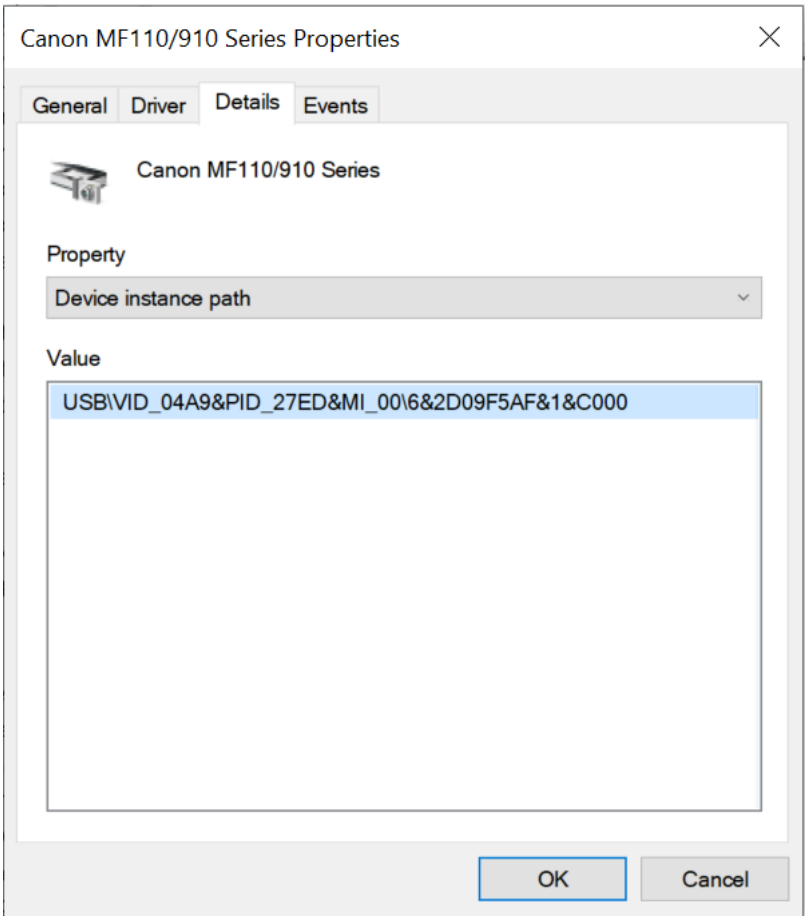
Vertrouwde printers

Vertrouwde apparaten zijn apparaten waartoe gebruikers die in de instellingen voor vertrouwde apparaten zijn opgegeven altijd volledige toegang hebben.

De procedure voor het toevoegen van vertrouwde printers is precies hetzelfde als voor andere typen vertrouwde apparaten. U kunt lokale printers toevoegen op basis van ID of apparaatmodel. U kunt alleen netwerkprinters toevoegen per apparaat-ID.

Als u een vertrouwde lokale printer per ID wilt toevoegen, hebt u een unieke ID (Hardware ID – HWID) nodig. U kunt de ID vinden in apparaateigenschappen met behulp van hulpprogramma's van het besturingssysteem (zie onderstaande afbeelding). U kunt dit doen met het hulpprogramma Device Manager. De ID van een lokale printer kan er als volgt uitzien: `6&2D09F5AF&1&C000`. Apparaten toevoegen per ID is handig als u meerdere specifieke apparaten wilt toevoegen. U kunt ook maskers gebruiken.

Als u een vertrouwde lokale printer per apparaatmodel wilt toevoegen, hebt u de Vendor ID (VID) en de Product ID (PID) nodig. U kunt de ID's vinden in apparaateigenschappen met behulp van hulpprogramma's van het besturingssysteem (zie onderstaande afbeelding). Sjabloon voor de invoer van het VID en PID: `VID_04A9&PID_27FD`. 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.



Apparaat-ID in Apparaatbeheer

Als u een vertrouwde netwerkprinter wilt toevoegen, hebt u de bijbehorende apparaat-ID nodig. Voor netwerkprinters kan de apparaat-ID de netwerknaam van de printer (naam van de gedeelde printer), het IP-adres van de printer of de URL van de printer zijn.

Controle van Wifi-verbindingen

Met Apparaatcontrole kunt u de Wifi-verbinding van de computer (laptop) beheren. Openbare Wifi-netwerken kunnen onveilig zijn en het gebruik van dergelijke netwerken kan leiden tot gegevensverlies. Met apparaatbeheer kunt u voorkomen dat een gebruiker verbinding maakt met wifi of alleen verbinding kan maken met vertrouwde netwerken. U kunt bijvoorbeeld toestaan dat alleen verbinding wordt gemaakt met het wifi-netwerk van het bedrijf dat voldoende veilig is. Apparaatcontrole blokkeert de toegang tot alle wifinetwerken behalve de netwerken die in de lijst Vertrouwd zijn opgegeven.

Op computers met Windows 11 moet u Locatiediensten inschakelen om Wi-Fi-verbindingen te beheren. Hiervoor moet u de schakelaar **Locatiediensten** inschakelen in de instellingen van het besturingssysteem (**Instellingen** → **Privacy & security** → **Locatie**). Als Locatiediensten is uitgeschakeld, controleert Kaspersky Endpoint Security geen verbindingen met Wi-Fi-netwerken.

Wifi-verbindingen beperken in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Security Controls** → **Apparaatcontrole** in het beleidsvenster.
4. Selecteer onder **Instellingen van Apparaatcontrole** het tabblad **Apparaattypen**.

   De tabel bevat toegangsregels voor alle apparaten die aanwezig zijn in de classificatie van het onderdeel Apparaatcontrole.
5. Selecteer in het contextmenu voor het apparaattype **Wifi** de actie voor apparaatcontrole die wordt genomen bij het verbinden met wifi: **Toestaan** (), **Blokkeren** (), of **Blokkeren met uitzonderingen** ().
6. Als u de optie **Blokkeren met uitzonderingen** hebt geselecteerd, creëer dan een lijst met vertrouwde wifi-netwerken:

   a. Dubbelklik om de lijst met vertrouwde Wifi-netwerken te openen.

   b. In het blok **Vertrouwde wifinetwerken**, klikt u op de knop **Toevoegen**.

   c. Dit opent een venster; configureer in dat venster het vertrouwde wifi-netwerk (zie onderstaande afbeelding):

   - **Netwerknaam**. Naam of SSID (Service Set Identifier) van het wifi-netwerk.
   - **Authenticatietype**. Verificatietype dat wordt gebruikt wanneer u verbinding maakt met het wifi-netwerk.

     Vanaf Kaspersky Endpoint Security voor Windows versie 12.0 is WPA3-protocolondersteuning aan het programma toegevoegd. Als een beleid van Kaspersky Endpoint Security versie 12.2 wordt toegepast op een computer, wordt het WPA2-protocol geselecteerd op computers met Kaspersky Endpoint Security versie 11.11.0 en eerder; WPA2 / WPA3 is geselecteerd voor versies 12.0 tot 12.1; WPA3 is geselecteerd voor versie 12.2 en later.
   - **Encryptietype**. Type versleuteling dat wordt gebruikt om het wifi-verkeer te beschermen.
   - **Opmerking**. Meer info over het toegevoegde wifi-netwerk.

   U kunt de instellingen van het vertrouwde wifi-netwerk bekijken in de routerinstellingen.

   Een wifinetwerk wordt als vertrouwd beschouwd als de instellingen ervan overeenkomen met alle opgegeven instellingen in de regel.

7. Sla uw wijzigingen op.



Instellingen vertrouwde wifinetwerken

Wifiverbindingen beperken in Webconsole en Cloudconsole.

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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** → **Device Control**.
5. Selecteer onder **Device access rules** het tabblad **Devices and Wi-Fi networks**.

   De tabel bevat toegangsregels voor alle apparaten die aanwezig zijn in de classificatie van het onderdeel Apparaatcontrole.
6. Klik in het blok **Wi-Fi networks** op de koppeling **Wi-Fi**.
7. In het venster dat verschijnt, selecteer de Apparaatcontrole actie die moet worden uitgevoerd bij het verbinden met wifi: **Allow**, **Block**, of **Block with exclusions**.
8. Als u de optie **Block with exclusions** hebt geselecteerd, creëer dan een lijst met vertrouwde wifi-netwerken:

   a. Dubbelklik om de lijst met vertrouwde Wifi-netwerken te openen.

   b. In het blok **Trusted Wi-Fi networks**, klikt u op de knop **Add**.

   c. Dit opent een venster; configureer in dat venster het vertrouwde wifi-netwerk (zie onderstaande afbeelding):

   - **Name**. Naam of SSID (Service Set Identifier) van het wifi-netwerk.
   - **Authentication type**. Verificatietype dat wordt gebruikt wanneer u verbinding maakt met het wifi-netwerk.

     Vanaf Kaspersky Endpoint Security voor Windows versie 12.0 is WPA3-protocolondersteuning aan het programma toegevoegd. Als een beleid van Kaspersky Endpoint Security versie 12.2 wordt toegepast op een computer, wordt het WPA2-protocol geselecteerd op computers met Kaspersky Endpoint Security versie 11.11.0 en eerder; WPA2 / WPA3 is geselecteerd voor versies 12.0 tot 12.1; WPA3 is geselecteerd voor versie 12.2 en later.

- **Encryption type**. Type versleuteling dat wordt gebruikt om het wifi-verkeer te beschermen.
- **Comment**. Meer info over het toegevoegde wifi-netwerk.

U kunt de instellingen van het vertrouwde wifi-netwerk bekijken in de routerinstellingen.

> Een wifinetwerk wordt als vertrouwd beschouwd als de instellingen ervan overeenkomen met alle opgegeven instellingen in de regel.

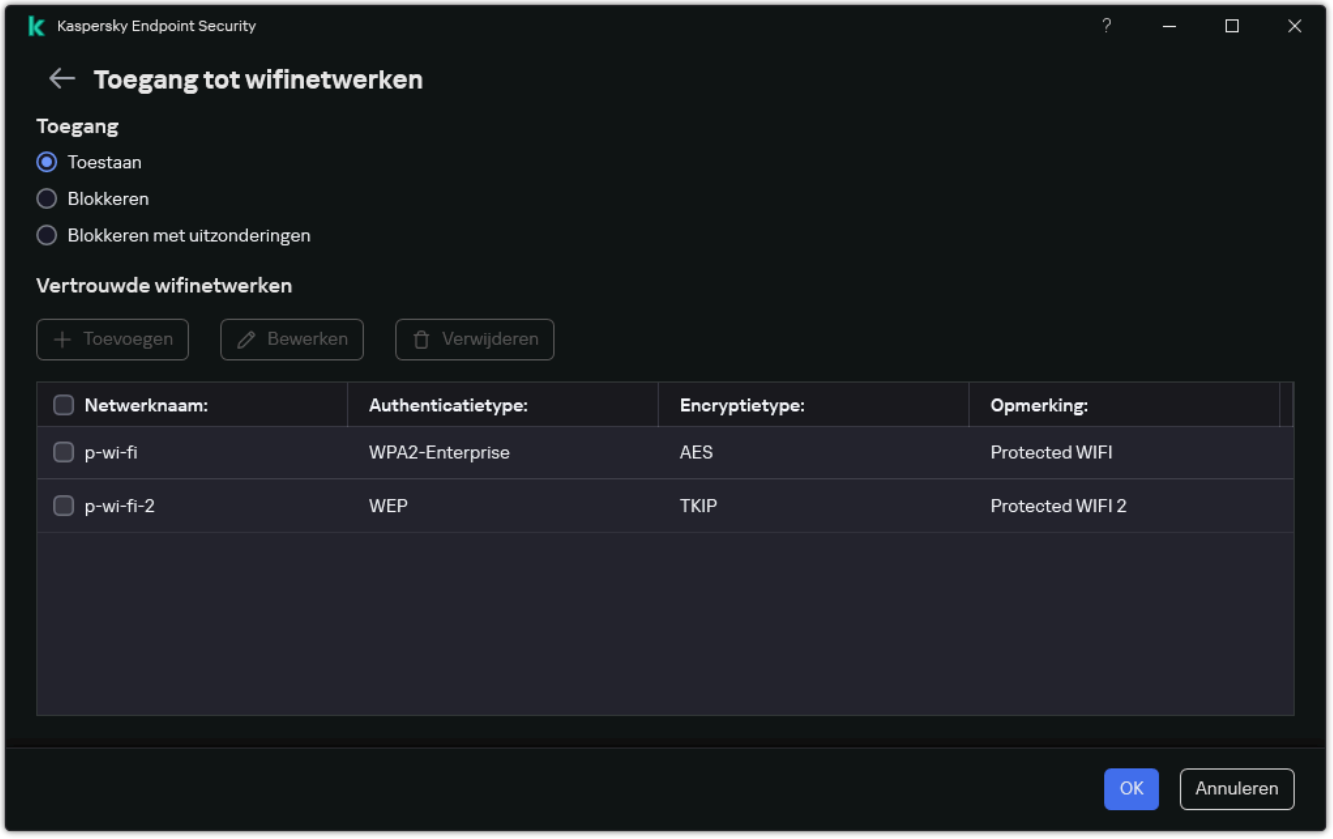
9. Sla uw wijzigingen op.

Wifi-verbindingen beperken in de programma-interface

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.



Instellingen wifi-toegang

5. Selecteer onder **Toegang**, de actie voor apparaatcontrole die u wil nemen bij het verbinden met wifi: **Toestaan**, **Blokkeren**, of **Blokkeren met uitzonderingen**.

6. Als u de optie **Blokkeren met uitzonderingen** hebt geselecteerd, creëer dan een lijst met vertrouwde wifi-netwerken:

   a. In het blok **Vertrouwde wifinetwerken**, klikt u op de knop **Toevoegen**.

   b. Dit opent een venster; configureer in dat venster het vertrouwde wifi-netwerk (zie onderstaande afbeelding):

   - **Netwerknaam**. Naam of SSID (Service Set Identifier) van het wifi-netwerk.
   - **Authenticatietype**. Verificatietype dat wordt gebruikt wanneer u verbinding maakt met het wifi-netwerk.

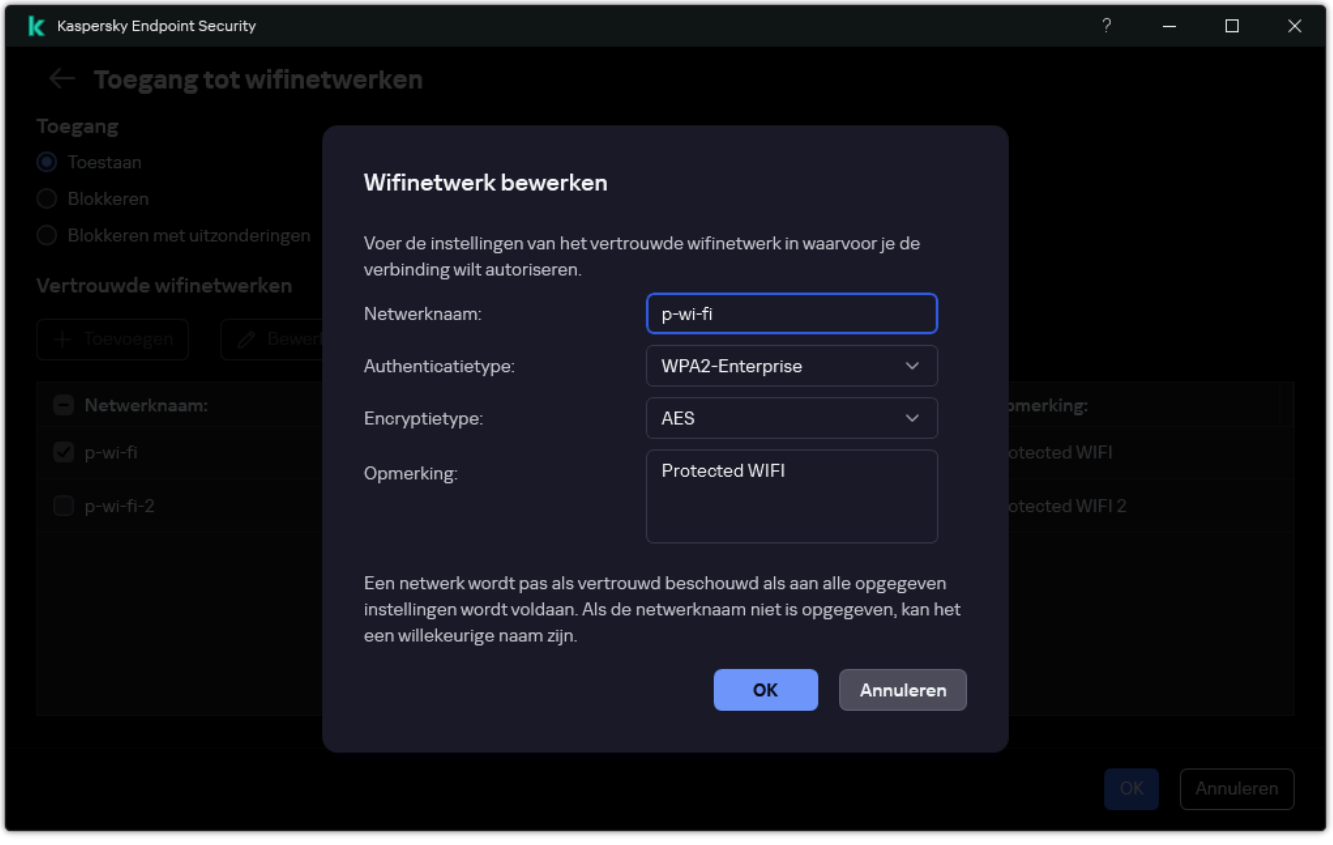
     Vanaf Kaspersky Endpoint Security voor Windows versie 12.0 is WPA3-protocolondersteuning aan het programma toegevoegd. Als een beleid van Kaspersky Endpoint Security versie 12.2 wordt toegepast op een computer, wordt het WPA2-protocol geselecteerd op computers met Kaspersky Endpoint Security versie 11.11.0 en eerder; WPA2 / WPA3 is geselecteerd voor versies 12.0 tot 12.1; WPA3 is geselecteerd voor versie 12.2 en later.

   - **Encryptietype**. Type versleuteling dat wordt gebruikt om het wifi-verkeer te beschermen.
   - **Opmerking**. Meer info over het toegevoegde wifi-netwerk.

   U kunt de instellingen van het vertrouwde wifi-netwerk bekijken in de routerinstellingen.

   Een wifinetwerk wordt als vertrouwd beschouwd als de instellingen ervan overeenkomen met alle opgegeven instellingen in de regel.

7. Sla uw wijzigingen op.



Instellingen vertrouwde wifinetwerken

Als gevolg hiervan, wanneer een gebruiker probeert verbinding te maken met een wifinetwerk dat niet als vertrouwd vermeld staat, blokkeert het programma de verbinding en geeft een melding weer (zie onderstaande afbeelding).



Melding van Apparaatcontrole

Bewaking op het gebruik van verwisselbare schijven

De bewaking van het gebruik van verwisselbare schijven omvat:

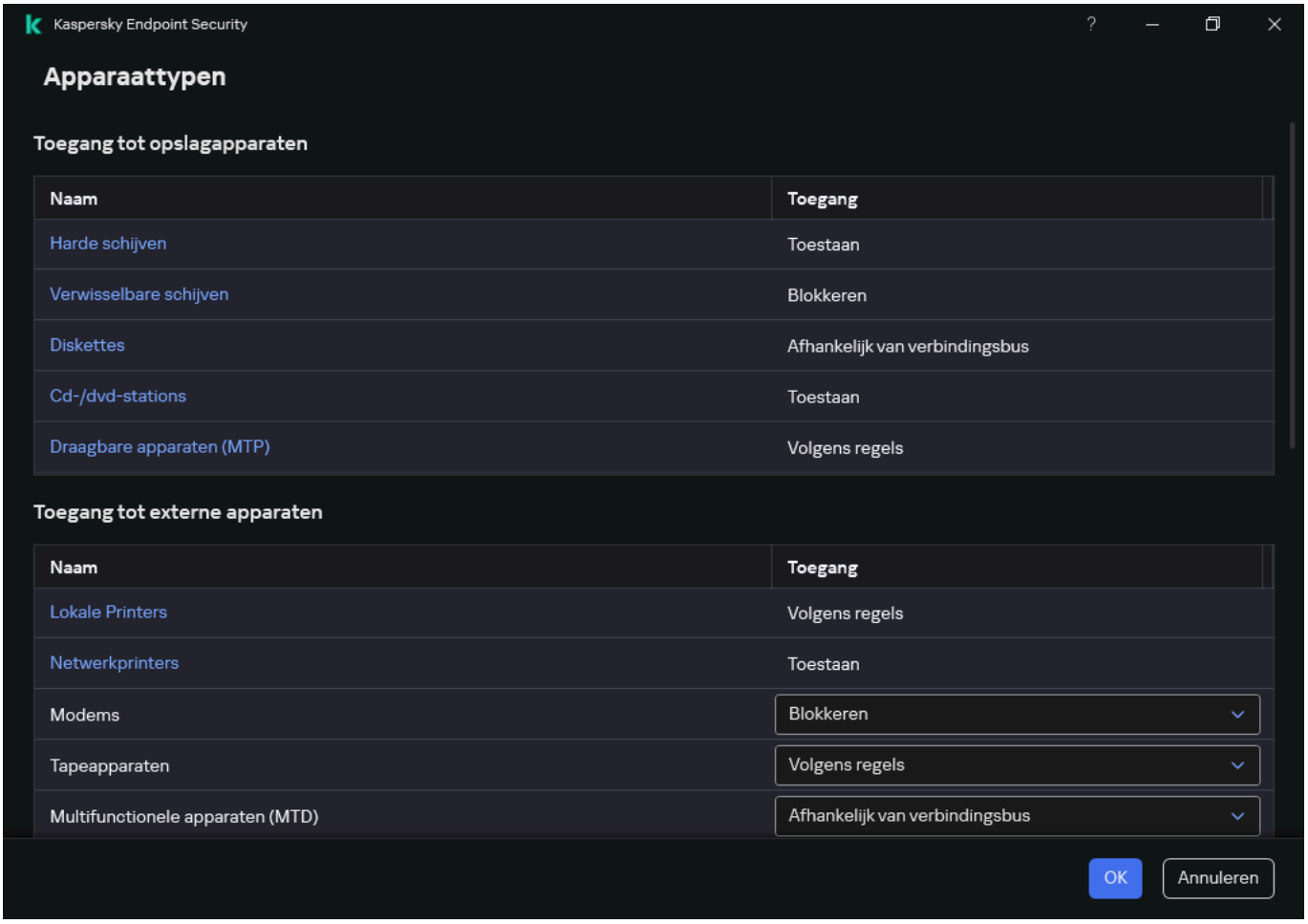
- De bewaking van bewerkingen met bestanden op verwisselbare schijven.
- De bewaking van de aansluiting en verwijdering van vertrouwde verwisselbare schijven.

  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 het urgentieniveau *Informatief bericht*.

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**.

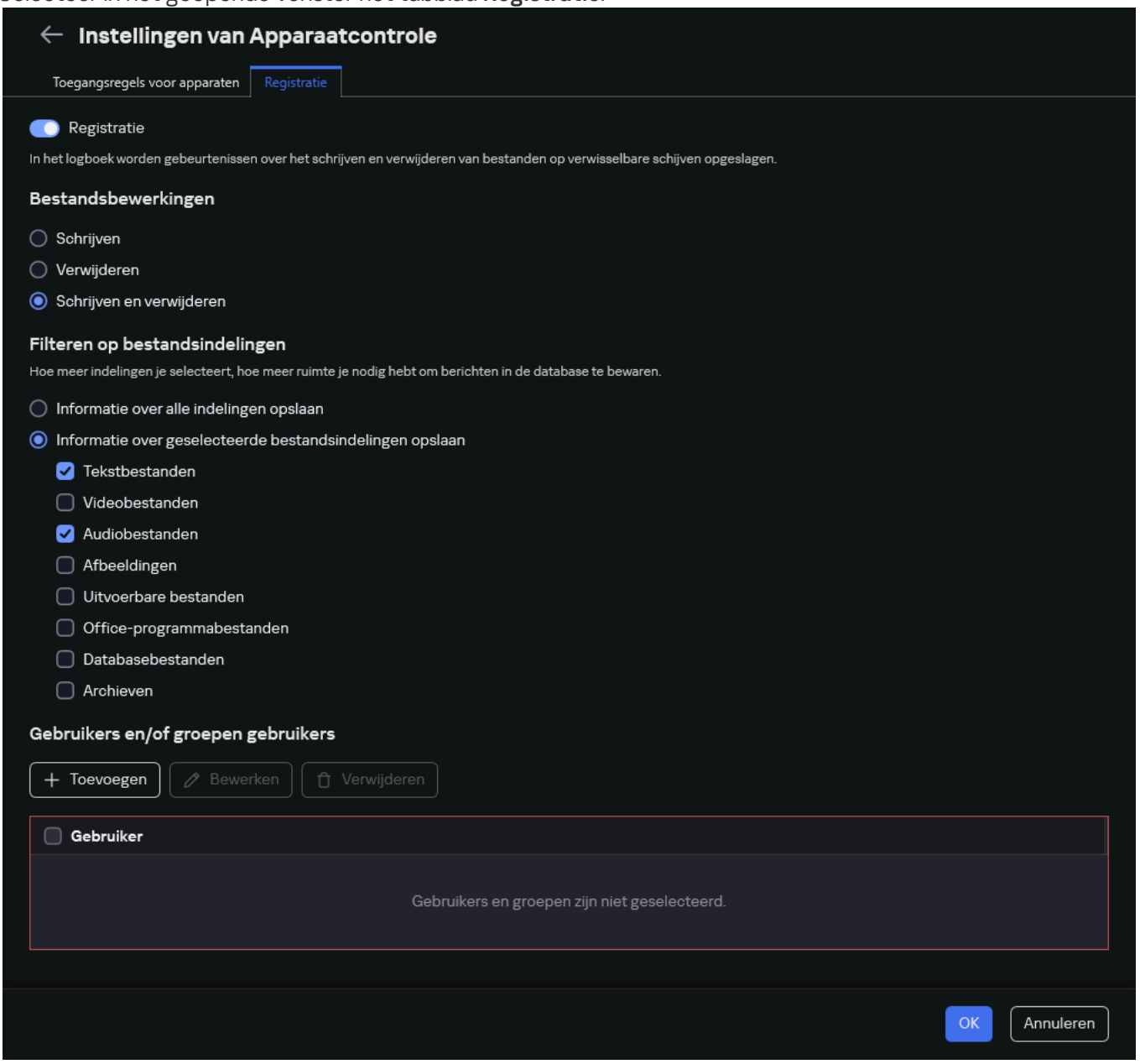
Het geopende venster toont toegangsregels voor alle apparaten die zijn opgenomen in de componentclassificatie Apparaatcontrole.



Typen apparaten in het onderdeel Apparaatcontrole

4. Selecteer in het blok **Toegang tot opslagapparaten Verwisselbare schijven**.

5. Selecteer in het geopende venster het tabblad **Registratie**.



De instellingen voor de bewaking van het gebruik van verwisselbare schijven

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 **Events**. 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 is niet aanbevolen om meer dan 5000 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 *Informational messages*.

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 vervolgkeuzelijst **Toon aangesloten apparaten**.

5. Selecteer in de lijst met apparaten het apparaat dat u aan de vertrouwde lijst wilt toevoegen.

   Kaspersky Endpoint Security biedt geen ondersteuning voor het toevoegen van apparaten van het type **Diskettes** aan de vertrouwde lijst.

6. In het veld **Opmerking** kunt u alle relevante informatie over het vertrouwde apparaat opgeven.

7. Selecteer de gebruikers of groepen gebruikers waarvoor u toegang tot vertrouwde apparaten wilt toestaan.

   U kunt gebruikers selecteren in Active Directory, in de lijst van accounts in Kaspersky Security Center, of door handmatig een lokale gebruikersnaam in te voeren. Kaspersky raadt aan om locale gebruikersaccounts alleen in speciale gevallen te gebruiken, wanneer het niet mogelijk is om domeingebruikersaccounts te gebruiken.

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_*`.

Het wijzigen van de lijst met vertrouwde apparaten kan worden geblokkeerd door de eigenschappen van het bovenliggende beleid. Om de lijst te wijzigen, moet u toestaan dat de instellingen van vertrouwde zone in de Webconsole (het "hangslot" moet ontgrendeld zijn).

Vertrouwde zones zijn verschillend gegroepeerd in de Beheerconsole (MMC) en de Webconsole. Ook de manier waarop wijziging in de parameters voor de vertrouwde zone worden voorkomen, verschilt (verschillende "hangsloten"). We raden aan dat u alleen de Webconsole gebruikt om het programma te beheren. Als u de vertrouwde zone in verschillende consoles configureert, kan de beheerplug-in het "hangslot" terugzetten naar de standaardstatus.

Apparaten aan de lijst met vertrouwde apparaten toevoegen.

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.

2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

3. Selecteer **Security Controls** → **Apparaatcontrole** in het beleidsvenster.

4. Selecteer rechts in het venster het tabblad **Vertrouwde apparaten**.

5. 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.

6. Klik op de knop **Toevoegen** en selecteer een methode om een apparaat aan de vertrouwde lijst toe te voegen.

7. Om apparaten te filteren, selecteert u een apparaattype in de vervolgkeuzelijst **Apparaattype** (bijvoorbeeld **Verwisselbare schijven**).

   Kaspersky Endpoint Security biedt geen ondersteuning voor het toevoegen van apparaten van het type **Diskettestations** aan de vertrouwde lijst.

8. 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 **Refresh** klikt. Om de lijst met apparaten correct weer te geven, kunt u apparaten toevoegen op apparaat-ID-masker.

9. Om apparaten te filteren, voert u in het veld **Computer** 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.

10. Klik op de knop **Refresh**.

    De tabel toont een lijst met apparaten die voldoen aan de gedefinieerde filtercriteria.

11. Schakel de selectievakjes in naast de namen van de apparaten die u aan de lijst met vertrouwde apparaten wilt toevoegen.

12. Voer in het veld **Opmerking** een beschrijving in van de reden voor het toevoegen van apparaten aan de vertrouwde lijst.

13. Klik op de knop **Select** aan de rechterkant van het veld **Sta toe aan gebruikers en/of groepen gebruikers**.

14. U kunt gebruikers selecteren in Active Directory, in de lijst van accounts in Kaspersky Security Center, of door handmatig een lokale gebruikersnaam in te voeren. Kaspersky raadt aan om locale gebruikersaccounts alleen in speciale gevallen te gebruiken, wanneer het niet mogelijk is om domeingebruikersaccounts te gebruiken.

    Standaard is toegang tot vertrouwde apparaten toegestaan voor de groep ledereen.

15. 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 verbindingsbus 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.
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 verbindingsbus 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 verlengen via de Beheerconsole.

Online modus voor het verlenen van toegang

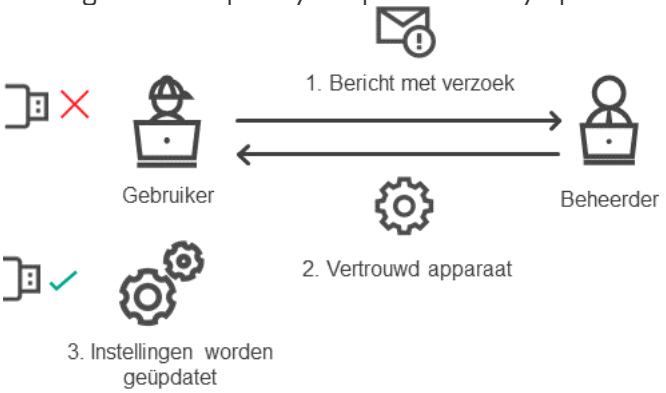
U kunt alleen toegang verlenen tot een geblokkeerd apparaat in de online modus als Kaspersky Security Center in het bedrijf is geïmplementeerd en een beleid op de computer is toegepast. De computer moet verbinding kunnen maken met de Administration Server.

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 ontvangt een bericht met het verzoek in de Kaspersky Security Center-console.

   De Kaspersky Security Center-console heeft een vooraf ingestelde evenementselectie *User requests* voor het eenvoudig volgen van berichten van gebruikers.
3. 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.
4. 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

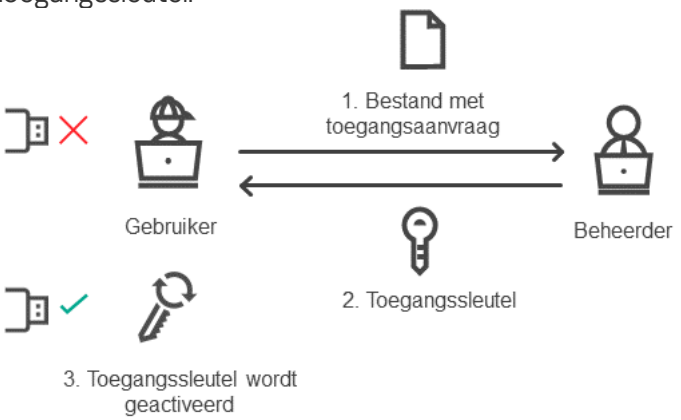
Offline modus voor het verlenen van toegang

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 **Aanvragen voor tijdelijke toegang toestaan** 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 toegangsaanvraag aan en verstuurt het naar de beheerder.
2. De beheerder maakt een toegangssleutel op basis van het bestand met de toegangsaanvraag 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**.



Melding van Apparaatcontrole

Vervolgens ontvangt de beheerder in de Kaspersky Security Center-console het: *Bericht over blokkering van toegang tot apparaat aan beheerder*-evenement. De gebeurtenis bevat gebruikersnaam, computernaam, details van het apparaat waartoe de gebruiker toegang probeert te krijgen, en andere informatie. U kunt configureren hoe de beheerder op de hoogte wordt gesteld van dergelijke gebeurtenissen en, bijvoorbeeld, e-mailmeldingen selecteren. De Kaspersky Security Center-console heeft een vooraf ingestelde evenementselectie *User requests* voor het eenvoudig volgen van berichten van gebruikers.

Om toegang toe te staan, moet u het apparaat toevoegen aan de vertrouwde lijst. Nadat u de instellingen van Kaspersky Endpoint Security op de computer bijgewerkt, kan de gebruiker toegang krijgen tot het apparaat.

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 **Aanvragen 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. Dit opent een venster; selecteer in dat 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 **Asset management** → **Assets (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 toegangsaanvraag 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 toegangsaanvraag 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 **Toegangsaanvraag**, 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 gebruikt 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. Kaspersky-experts verstrekken een sjabloon van een bericht aan de gebruiker waarin de redenen worden beschreven waarom de toegang tot het apparaat werd geblokkeerd (zie onderstaande afbeelding).

Er zijn speciale variabelen voorzien voor het beheer van de berichtsjablonen (bijvoorbeeld `%USER_NAME%`). Met variabelen kan één berichtsjabloon voor verschillende computers worden gebruikt. Bij het genereren van een bericht haalt Kaspersky Endpoint Security de waarde van de variabele op uit de instellingen van het besturingssysteem en voegt het deze in het bericht in dat overeenkomt met de specifieke computer, gebruiker en gebeurtenis.



Melding van Apparaatcontrole

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. Om dit te doen, moet de gebruiker klikken op **Toegang vragen** of **Tijdelijke toegang aanvragen** knoppen en stuur een bericht naar de beheerder met een beschrijving van de situatie. U kunt ook een sjabloon maken van het bericht aan de beheerder, en er gegevens aan toevoegen die u kunnen helpen bij uw beslissing om de toegang tot het apparaat toe te staan of te blokkeren. 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.

De berichtsjablonen voor Apparaatcontrole in de Beheerconsole (MMC) wijzigen

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Security Controls** → **Apparaatcontrole** in het beleidsvenster.
4. In het blok **Instellingen voor berichtsjablonen**, klikt u op de knop **Sjablonen**.

5. Dit opent een venster. Configureer in dat venster het sjabloon Programmacontrole:

   - **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.

   Als u een variabele aan de sjabloontekst wilt toevoegen, plaats dan de cursor op de gewenste positie, klik op **Variabele** en selecteer de gewenste variabele in de lijst met beschikbare opties.

   U kunt ook de standaardsjabloontekst herstellen.

6. Sla uw wijzigingen op.

De berichtsjablonen van Apparaatcontrole veranderen in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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** → **Device Control**.

5. Configureer in het blok **Message templates** de sjablonen voor berichten over programmacontrole:

   - **Message to user**. 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.

   - **Message to administrator**. 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.

   Als u een variabele aan de sjabloontekst wilt toevoegen, plaats dan de cursor op de gewenste positie, klik op **Add variable** en selecteer de gewenste variabele in de lijst met beschikbare opties.

   U kunt ook de standaardsjabloontekst herstellen.

6. Sla uw wijzigingen op.

De berichtsjablonen voor Apparaatcontrole in de programma-interface wijzigen

1. Klik in het hoofdvenster van het programma op de knop ⚙.

2. Selecteer **Security Controls** → **Programmacontrole** in het venster met de programma-instellingen.

3. Configureer in het blok **Berichtsjablonen** de sjablonen voor berichten over programmacontrole:

   - **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.

   Als u een variabele aan de sjabloontekst wilt toevoegen, plaats dan de cursor op de gewenste positie, klik op **Variabele toevoegen** en selecteer de gewenste variabele in de lijst met beschikbare opties.

   U kunt ook de standaardsjabloontekst herstellen.

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 **Rule triggers in Smart Training state**.

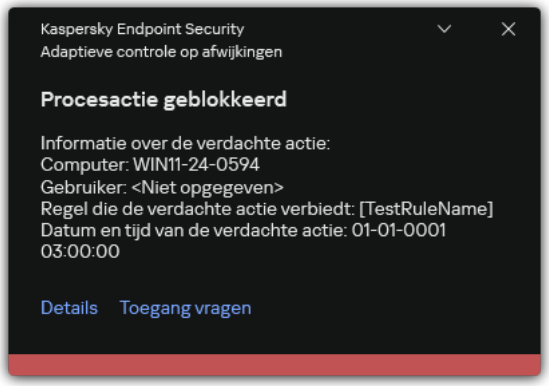
2. Rapport over activering van regels analyseren.

   De beheerder analyseert het rapport over de activering van regels of de inhoud van de opslagplaats **Rule triggers 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 via de volgende kanalen geconfigureerd:

- Adaptieve controle op afwijkingen begint automatisch 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 **Rule triggers in Smart Training state**. We raden aan dat u het rapport over het activeren van regels en de inhoud van de **Rule triggers in Smart Training state** opslag controleert.

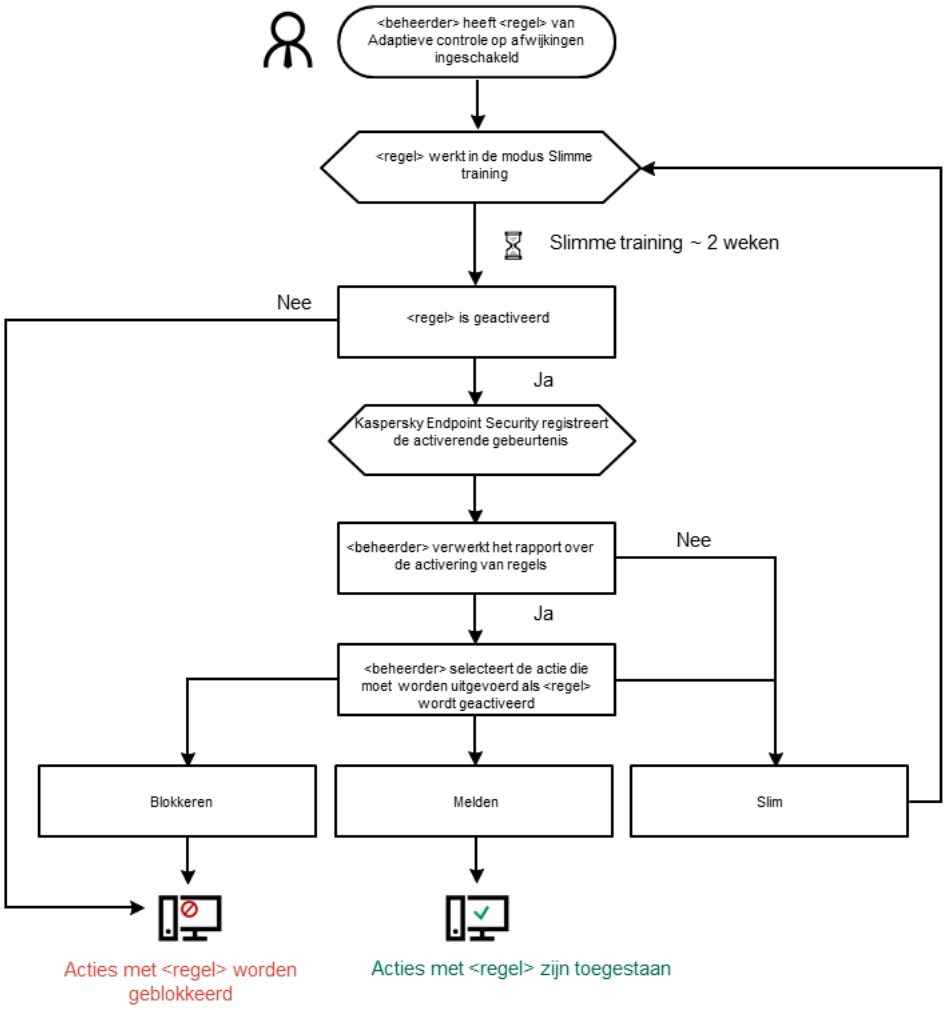
Wanneer een schadelijk programma een actie probeert uit te voeren, blokkeert Kaspersky Endpoint Security de actie en toont het een melding (zie onderstaande afbeelding).



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 trainen

Adaptieve controle op afwijkingen bevat een reeks regels (gedragspatronen). 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. Adaptieve controle op afwijkingen blokkeert geen programma-activiteit op de computer, maar brengt alleen de beheerder op de hoogte. U kunt ook handmatig de actie selecteren die moet worden uitgevoerd wanneer een regel van Adaptieve controle wordt geactiveerd.

Bekijk de lijst met regels van Adaptieve controle op afwijkingen Beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de beheerconsole **Policies**.
3. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
4. Selecteer **Security Controls** → **Adaptive Anomaly Control** in het beleidsvenster.
5. Selecteer het selectievakje **Adaptieve controle op afwijkingen**.
6. Onder **Instellingen van regels van Adaptieve controle op afwijkingen**, bekijk de lijst met regels.
   Standaard werken alle regels in de **Slim** modus.
7. Bevestig indien nodig de update van de regel voor Adaptieve controle op afwijkingen.
8. Selecteer indien nodig een actie wanneer een regel van Adaptieve controle op afwijkingen wordt geactiveerd:
   - **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.
9. Schakel indien nodig de regels uit die u niet wilt gebruiken.
10. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Bekijk regels voor Adaptieve controle op afwijkingen in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de Webconsole het tabblad **Asset management** → **Policies**.
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** → **Adaptive Anomaly Control**.
5. Zet de schakelaar **Adaptive Anomaly Control ENABLED** aan.
6. Onder **Rules**, bekijk de lijst met regels.
   Standaard werken alle regels in de **Smart** modus.
7. Bevestig indien nodig de update van de regel voor Adaptieve controle op afwijkingen.

8. Selecteer indien nodig een actie wanneer een regel van Adaptieve controle op afwijkingen wordt geactiveerd:

    - **Block**. 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.

    - **Inform**. 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.

9. Schakel indien nodig de regels uit die u niet wilt gebruiken.

10. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

De lijst met regels voor Adaptieve controle op afwijkingen in de programma-interface bekijken

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

2. Selecteer **Security Controls** → **Adaptive Anomaly Control** in het venster met de programma-instellingen.

3. Zet de schakelaar **Adaptieve controle op afwijkingen** aan.

4. Klik in het blok **Regels** op de koppeling **Regels bewerken**.

    Het venster met de lijst met Regels voor Adaptieve controle op afwijkingen wordt geopend. Standaard werken alle regels in de **Slim** modus.

5. Bevestig indien nodig de update van de regel voor Adaptieve controle op afwijkingen.

6. Selecteer indien nodig een actie wanneer een regel van Adaptieve controle op afwijkingen wordt geactiveerd:

    - **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. Schakel indien nodig de regels uit die u niet wilt gebruiken.

8. Sla uw wijzigingen op.

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 tijdens de training een regel nooit wordt geactiveerd, beschouwt Adaptieve controle op afwijkingen dergelijk gedrag als atypisch en wijzigt het de status van de regel in **Slim blokkeren**. Vervolgens blokkeert het programma alle activiteiten die aan deze regel voldoen.

Als een regel wordt geactiveerd tijdens de training, moet u de actie die het programma toepast op gedetecteerde activiteit die overeenkomt met deze regel, handmatig configureren. Als u de actie niet selecteert wanneer de regel wordt geactiveerd, gaat Adaptieve controle op afwijkingen verder in de trainingsmodus.

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 van Windows PowerShell via Office-programma*).
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 **Rule triggers in Smart Training state** 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 `file.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 `file.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. In het blok **Uitzonderingen**, klikt u 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.

   U kunt gebruikers selecteren in Active Directory, in de lijst van accounts in Kaspersky Security Center, of door handmatig een lokale gebruikersnaam in te voeren. Kaspersky raadt aan om locale gebruikersaccounts alleen in speciale gevallen te gebruiken, wanneer het niet mogelijk is om domeingebruikersaccounts te gebruiken.

   > 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\File.exe` of `Dir\*.exe`).
   - **Hash van bronproces**. SHA256-hash van het bestand.
   - **Bronobject**. Pad of masker van het pad naar het bestand of de map met bestanden (bijvoorbeeld `C:\Dir\File.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.example.com`, `object://VBA`, `object://ipconfig`, `object://HKEY_USERS`. U kunt ook maskers gebruiken, zoals `object://*C:\Windows\temp\*`.
   - **Hash van bronobject**. SHA256-hash van het bestand.

   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\File.exe` of `Dir\*.exe`).
    - **Hash van doelproces**. SHA256-hash van het bestand.
    - **Doelobject**. De opdracht om het doelproces te starten. Geef de opdracht op in de volgende structuur: `object://<command>`. 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**. SHA256-hash van het bestand.

    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 uitzonderingen 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.

Er zijn speciale sjablonen beschikbaar voor berichten aan de beheerder over het blokkeren van mogelijk schadelijke acties. Er zijn speciale variabelen voorzien voor het beheer van de berichtsjablonen (bijvoorbeeld `%USER_NAME%`). Met variabelen kan één berichtsjabloon voor verschillende computers worden gebruikt. Bij het genereren van een bericht haalt Kaspersky Endpoint Security de waarde van de variabele op uit de instellingen van het besturingssysteem en voegt het deze in het bericht in dat overeenkomt met de specifieke computer, gebruiker en gebeurtenis.

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.

   Als u een variabele aan de sjabloontekst wilt toevoegen, plaats dan de cursor op de gewenste positie, klik op **Variabele toevoegen** en selecteer de gewenste variabele in de lijst met beschikbare opties.

   U kunt de standaardsjabloontekst ook herstellen met de knop **Opnieuw instellen**.
4. Sla uw wijzigingen op.

Monitoring van de bewerkingen van Adaptieve controle op afwijkingen

Adaptieve controle op afwijkingen bevat verschillende monitoring-tools. Het belangrijkste doel van de monitoring van Adaptieve controle op afwijkingen is de configuratie van het onderdeel tijdens de training.

Rapporten van Adaptieve controle op afwijkingen

Adaptieve controle op afwijkingen gebruikt de volgende rapporten:

- **Rapport over de status van de regels van Adaptieve controle op afwijkingen**. Het rapport bevat informatie over de status van regels voor Adaptieve controle op afwijkingen (*Off*, *Smart Training*, *Smart Block*, *Notify*, *Block*). Met dit rapport kunt u het trainingsniveau van Adaptieve controle op afwijkingen analyseren en het aantal regels evalueren dat is overgeschakeld van de modus *Smart Training* naar de normale modus (bijvoorbeeld *Smart Block*).
- **Rapport over geactiveerde regels van Adaptieve controle op afwijkingen**. Het rapport bevat informatie over activeren van regels. Het rapport toont ook de modus voor het activeren van de regel: *Block* (inclusief *Smart Block*)) of *Notify*. Met dit rapport kunt u de activiteit van Adaptieve controle op afwijkingen op de computers van gebruikers evalueren.

Rapporten van Adaptieve controle op afwijkingen bekijken in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Security Controls** → **Adaptieve controle op afwijkingen** in het beleidsvenster.
4. Doe een van de volgende acties:
   - Klik op de link **Rapport over de status van de regels van Adaptieve controle op afwijkingen** als u het rapport over de staat van de regels van Adaptieve controle op afwijkingen wilt bekijken.
   - Klik opde link **Rapport over geactiveerde regels van Adaptieve controle op afwijkingen** als u het rapport over de geactiveerde regels van Adaptieve controle op afwijkingen wilt bekijken.
5. Het rapport wordt gemaakt.

   Het rapport wordt in een nieuw venster weergegeven.

Rapporten van Adaptieve controle op afwijkingen bekijken in de Webconsole

1. Selecteer in het hoofdvenster van de Webconsole het tabblad **Asset management** → **Policies**.
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** → **Adaptive Anomaly Control**.
5. Doe in het blok **Rules** een van het volgende:
   - Selecteer **View report** → **Rules state** als u het rapport over de staat van de regels van Adaptieve controle op afwijkingen wilt bekijken.
   - Klik op **View report** → **Detections** als u het rapport over de geactiveerde regels van Adaptieve controle op afwijkingen wilt bekijken.
6. Het rapport wordt gemaakt.

   Het rapport wordt in een nieuw venster weergegeven.

Als u rapporten wilt genereren in de Kaspersky Security Center-console, moet u gegevensoverdracht naar Beheerserver inschakelen. Gegevensoverdracht is standaard ingeschakeld.

Gegevensoverdracht inschakelen voor Adaptieve controle op afwijkingen in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Algemene instellingen** → **Rapporten en Opslag** in het beleidsvenster.
4. In het blok **Gegevensoverdracht naar Administration Server**, klikt u op de knop **Instellingen**.

5. Vink de volgende vakjes aan:

   - **Rapport over de status van de regels van Adaptieve controle op afwijkingen**.
   - **Rapport over geactiveerde regels van Adaptieve controle op afwijkingen**.

6. Sla uw wijzigingen op.

Gegevensoverdracht voor Adaptieve controle op afwijkingen inschakelen in de Webconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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** → **KSC Integration**.
5. Onder **Data transfer to Administration Server**, selecteer de volgende selectievakje:

   - **Report on Adaptive Anomaly Control rules state**.
   - **Report on triggered Adaptive Anomaly Control rules**.

6. Sla uw wijzigingen op.

Rule triggers in Smart Training state opslag

In de trainingsmodus verstuurt Adaptieve controle op afwijkingen informatie over geactiveerde regels naar een aparte opslag, **Rule triggers in Smart Training state**. Informatie over geactiveerde regels wordt in de opslag weergegeven als een lijst met gebeurtenissen. Als u Adaptieve controle op afwijkingen wilt afstemmen, kunt u het atypische gedrag op de computer bevestigen of een uitzondering voor de regel toevoegen.

Gebeurtenissen van Adaptieve controle op afwijkingen

Adaptieve controle op afwijkingen registreert gebeurtenissen voor geactiveerde regels in de *Block*(inclusief *Smart Block*) en *Notify* modi. De volgende gebeurtenissen zijn hiervoor bedoeld:

Process action blocked

Process action skipped

Gebeurtenissen bevatten informatie over de verdachte activiteit, waaronder controlesommen van bestanden, de betrokken gebruikers, het tijdstip waarop de regel wordt geactiveerd en de computernaam. Na analyse van de gebeurtenis kunt u onmiddellijk uitzonderingen op de regel toevoegen als u vindt dat de activiteit legitiem is.

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* of een andere categorie), 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. De beheerder kan veel regels maken. Eén programma kan voldoen aan de criteria van meerdere regels. De prioriteit van een Blokkeren-regel is hoger dan die van een Toestaan-regel. Telkens wanneer het programma wordt gestart, controleert Kaspersky Endpoint Security of een programma overeenkomt met een regel. Kaspersky Endpoint Security vergelijkt het programma achtereenvolgens met alle regels van Programmacontrole.

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.

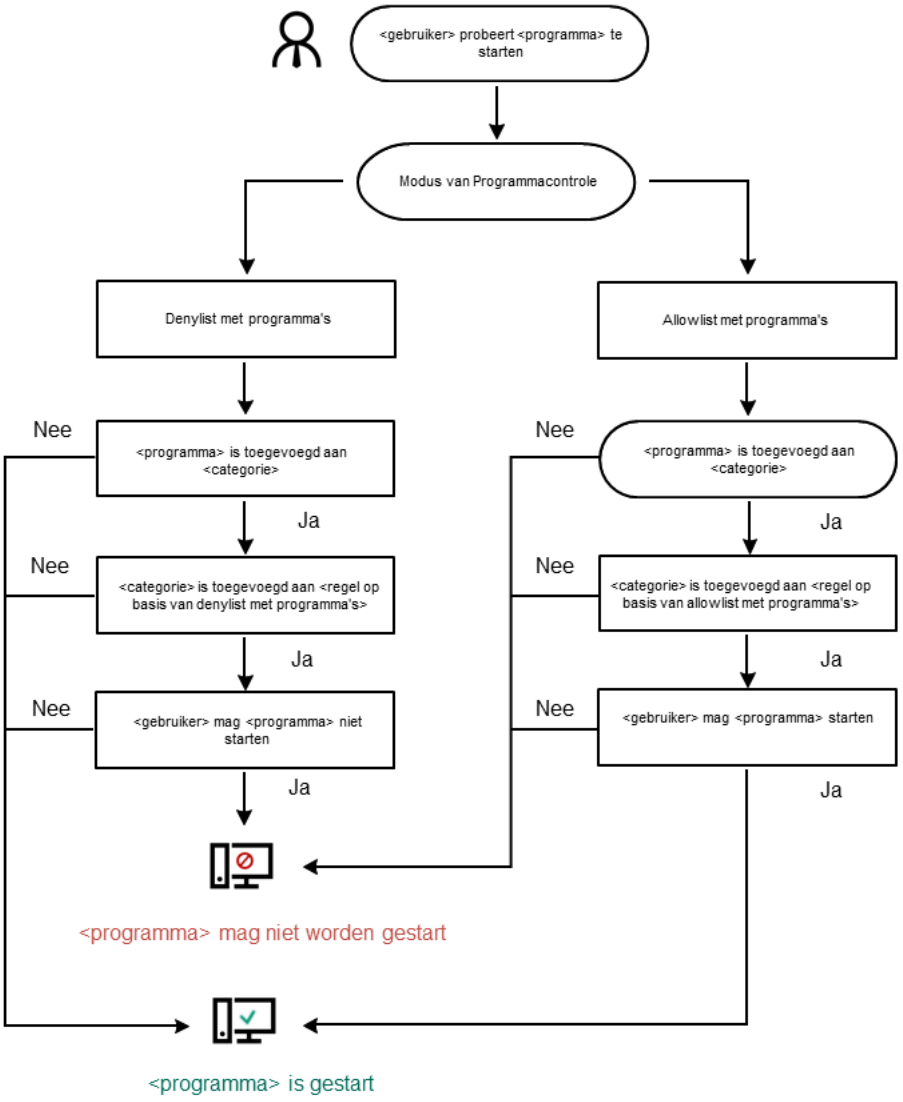
  De regels van Programmacontrole die worden aangemaakt in de Beheerconsole van Kaspersky Security Center zijn gebaseerd op aangepaste categorieën van programma's en niet op uitvoerings- of uitzonderingsvoorwaarden zoals in de lokale interface van Kaspersky Endpoint Security.

- 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.
- 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 software\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

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.

Programma-informatie bekijken

Informatie over geïnstalleerde programma's wordt geleverd door Kaspersky Security Center Network Agent. Informatie over geïnstalleerde programma's zijn beschikbaar in Kaspersky Security Center console in de map **Applications registry**. Network Agent werkt de informatie bij elke synchronisatie met Kaspersky Security Center bij. Voor meer details over de informatie verzonden door de Network Agent raadpleegt u de Help van Kaspersky Security Center.

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 **Advanced** → **Application management** → **Applications registry**.
3. Selecteer een programma.
4. Selecteer in het contextmenu van het programma de optie **Properties**.

Informatie bekijken over uitvoerbare bestanden

U kunt de belasting van de database verminderen wanneer u informatie over uitvoerbare bestanden opvraagt. Hiervoor raden we u aan de taak *Inventarisatie* uit te voeren op verschillende referentiecomputers waarop de standaard softwareset is geïnstalleerd.

U kunt een lijst met uitvoerbare bestanden krijgen met de taak *Inventarisatie* van Kaspersky Endpoint Security. U kunt de lijst met uitvoerbare bestanden bekijken in de Kaspersky Security Center-console in de map **Executable files**.

Voordat u de taak *Inventarisatie* start, controleert u of de database voldoet aan de aanbevelingen van Kaspersky Security Center. Voor meer informatie over databasebeperkingen, raadpleegt u Kaspersky Security Center Help.

Inventarisatie uitvoeren in de beheerconsole (MMC)

1. Selecteer **Tasks** in de structuur van de Beheerconsole van Kaspersky Security Center.

   De lijst met taken wordt geopend.

2. Klik op **New task**.

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

Stap 1. Een taaktype selecteren

Selecteer **Kaspersky Endpoint Security voor Windows 14.1.** → **Inventarisatie**.

Stap 2. Inventarisbereik

Maak een lijst met mappen waarin u wilt dat Kaspersky Endpoint Security zoekt naar uitvoerbare bestanden. Configureer de inventarisinstellingen (zie onderstaande tabel).

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: Het account selecteren om de taak uit te voeren

Selecteer een account om de *Inventarisatie* uit te voeren. Kaspersky Endpoint Security start de taak standaard met de rechten van een lokaal gebruikersaccount. Als het inventarisbereik netwerkstations of andere objecten met beperkte toegang omvat, selecteert u een gebruikersaccount met voldoende toegangsrechten.

Stap 5. Een taakstartschema configureren

Configureer het taakschema bijvoorbeeld handmatig.

Stap 6. Taaknaam definiëren

Voer een naam in voor de taak, bijvoorbeeld *Basisinventaris*.

Stap 7. Aanmaak van de taak voltooien

Verlaat de wizard verlaten. Schakel indien nodig het selectievakje **Run the task after the wizard finishes** in. U kunt de voortgang van de taak volgen in de taakeigenschappen. Als resultaat worden de uitvoerbare bestanden op de computers van de gebruikers doorzocht volgens het geconfigureerde schema.

Een taak Inventarisatie starten via de Webconsole en Cloudconsole

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

   De lijst met taken wordt geopend.

2. Klik op **Add**.

   De wizard Taak wordt gestart.

3. Configureer de taakinstellingen:

   a. Selecteer in de vervolgkeuzelijst **Application** de optie **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. Selecteer in de vervolgkeuzelijst **Task type** de optie **Inventory**.

   c. Typ in het veld **Task name** een korte omschrijving, zoals *Basisinventaris*.

   d. Selecteer in het gedeelte **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. Ga naar de volgende stap.

5. Selecteer een account om de taak uit te voeren. Kaspersky Endpoint Security start de taak standaard met de rechten van een lokaal gebruikersaccount.

6. Verlaat de wizard verlaten.

   U ziet een nieuwe taak in de lijst met taken.

7. Ga naar de taakeigenschappen om de taak te configureren (zie de onderstaande tabel).

8. Schakel het selectievakje naast de taak in.

9. Klik op **Start**.

   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. Als gevolg hiervan worden uitvoerbare bestanden doorzocht op de computers van de gebruiker in overeenstemming met het opgegeven schema.

Inventarisinstellingen

Parameter	Beschrijving
Inventory scopes	Lijst met objecten die het inventarisbereik vormen.
DLL modules inventory	Kaspersky Endpoint Security zoekt naar DLL-modules in het inventarisbereik en verzendt informatie naar Kaspersky Security Center. Als u de inventaris van DLL-modules inschakelt, duurt het aanzienlijk langer om de taak Inventaris te voltooien en wordt de omvang van de database aanzienlijk groter.
Script files inventory	Kaspersky Endpoint Security zoekt naar scripts in het inventarisbereik en verstuurt de informatie naar Kaspersky Security Center. Als u de inventaris van scriptbestanden inschakelt, duurt het aanzienlijk langer om de taak Inventaris te voltooien en wordt de omvang van de database aanzienlijk groter.
Run only when the computer is idle	Uitgestelde start van de taak 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. Met deze planningsoptie kunt u computervermogen besparen wanneer de computer wordt gebruikt.
Scan only new and modified files	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.
Skip file that is scanned for longer than (sec) N s	De taakuitvoeringstijd 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.

Parameter	Beschrijving
Scan archives	ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE en andere bestanden scannen. Het programma 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 (een archief in een archief).
Scan distribution packages	Distributiepakketten van programma's van derden scannen.
Do not unpack large compound files	Als dit selectievakje is ingeschakeld, scant het programma geen samengestelde bestanden als ze groter zijn dan de opgegeven waarde. Als dit selectievakje is uitgeschakeld, worden samengestelde bestanden van alle grootten gescand door het programma. Het programma scant grote bestanden die uit archieven worden gehaald, ongeacht of het selectievakje is ingeschakeld of niet.

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 **Advanced** → **Application management** → **Executable files**.
3. Selecteer een uitvoerbaar bestand.
4. Selecteer in het contextmenu van het uitvoerbare bestand de optie **Properties**.

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**.

Bijwerken van de informatie over geïnstalleerde programma's en uitvoerbare bestanden

Vanaf Kaspersky Endpoint Security 12.3 voor Windows is de werking van het onderdeel Programmacontrole met de database van uitvoerbare bestanden geoptimaliseerd. Kaspersky Endpoint Security 12.3 voor Windows werkt de database automatisch bij nadat het bestand van de computer is verwijderd. Hierdoor kan de database up-to-date worden gehouden en kunnen bronnen van Kaspersky Security Center worden bespaard.

Om de database van geïnstalleerde programma's up-to-date te houden, moet het verzenden van programma-informatie naar de Administration Server zijn ingeschakeld (het is standaard ingeschakeld).

Schakel de indiening van programma-informatie in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Algemene instellingen** → **Rapporten en Opslag** in het beleidsvenster.
4. In het blok **Gegevensoverdracht naar Administration Server**, klikt u op de knop **Instellingen**.
5. Selecteer het selectievakje **Gestarte programma's**.
6. Sla uw wijzigingen op.

Schakel de indiening van programma-informatie in Webconsole en Cloudconsole in

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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** → **KSC Integration**.
5. In het blok **Data transfer to Administration Server**, klikt u op de knop **Advanced settings**.
6. Selecteer in het venster dat opent het selectievakje **About started applications**.
7. Sla uw wijzigingen op.

De modus Geblokkeerde programma's inschakelen

De modus *Geblokkeerde programma's* is de modus waarin Programmacontrole toestaat dat alle gebruikers alle programma's starten, behalve de programma's die verboden zijn in Programmacontrole. Dat wil zeggen, als er geen regel voor het weigeren is, staat Programmacontrole het starten van het programma toe. Deze modus van Programmacontrole is standaard ingeschakeld.

Voordat u de modus *Geblokkeerde programma's* inschakelt, raden we u aan de regels van Programmacontrole te testen. Hiervoor kunt u: de testmodus inschakelen.

De modus Geblokkeerde programma's inschakelen in de Beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de beheerconsole **Policies**.
3. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
4. Selecteer **Security Controls** → **Programmacontrole** in het beleidsvenster.
5. Selecteer het selectievakje **Programmacontrole**.
6. Gebruik in het blok **Instellingen van Programmacontrole** de vervolgkeuzelijst **Controlemodus** om de **Denylist** te selecteren.
7. Selecteer in de vervolgkeuzelijst **Actie** de acie Programmacontrole:

   - **Regels testen**. Programmacontrole blokkeert geen programma's die volgens de regels niet mogen worden uitgevoerd, maar genereert gebeurtenissen over de werking van programma's die anders zouden worden geblokkeerd.
   - **Regels toepassen**. Programmacontrole blokkeert de geblokkeerde programma's en genereert overeenkomstige gebeurtenissen.

8. Selecteer de status voor de regel van Programmacontrole:

- **Aan**. Deze status geeft aan dat de regel wordt gebruikt als het onderdeel Programmacontrole actief is.
- **Uit**. 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 de regel van toepassing is maar informatie over de opstart van zulke programma's in het rapport registreert.

Indien nodig, voeg nieuwe regels toe voor Programmacontrole.

9. Configureer de geavanceerde instellingen van Programmacontrole:

- **Het laden van DLL-modules controleren (verhoogt de systeembelasting aanzienlijk)**. 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.

  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 "**Golden Image\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.

  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 degene die zijn geladen voordat Kaspersky Endpoint Security opstart.

- **Strikte digitale handtekeningsverificatie gebruiken**. U kunt een certificaat selecteren als activerende voorwaarden voor een programmacontrole-regel. Als dit selectievakje is ingeschakeld, past Kaspersky Endpoint Security regels toe op programma's die alleen zijn ondertekend met certificaten uit het vertrouwde certificaatarchief van het systeem. Programma's die met een dergelijk certificaat zijn ondertekend, worden ook door de beschermingsonderdelen, bijvoorbeeld de *Malware-scan*-taak, als vertrouwd beschouwd. Als u echter een certificaat uit een ander archief opgeeft in een programmacontrole-regel, past Kaspersky Endpoint Security een dergelijke regel niet toe.

  Als het selectievakje is uitgeschakeld, past Kaspersky Endpoint Security regels toe op programma's die zijn ondertekend door een certificaat uit het Windows Trusted Root Certificate Store. Dergelijke programma's maken geen deel uit van de vertrouwde zone. Beschermingsonderdelen bewaken de activiteit van dergelijke programma's.

- **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.
- **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.

10. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Schakel de modus Geblokkeerde programma's in de Webconsole en Cloudconsole in

1. Selecteer in het hoofdvenster van de Webconsole het tabblad **Asset management** → **Policies**.
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** → **App Control**.
5. Zet de schakelaar **Application Control ENABLED** aan.
6. Selecteer in het blok **Operating mode Block all except the rules list**.
7. In de **Action** blok, selecteer de actie voor Programmacontrole:

   - **Inform**. Programmacontrole blokkeert geen programma's die volgens de regels niet mogen worden uitgevoerd, maar genereert gebeurtenissen over de werking van programma's die anders zouden worden geblokkeerd.
   - **Apply rules**. Programmacontrole blokkeert de geblokkeerde programma's en genereert overeenkomstige gebeurtenissen.
8. Selecteer de status voor de regel van Programmacontrole:

   - **Enabled**. Deze status geeft aan dat de regel wordt gebruikt als het onderdeel Programmacontrole actief is.
   - **Disabled**. Deze status geeft aan dat de regel wordt genegeerd als het onderdeel Programmacontrole actief is.
   - **Test mode**. 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.

   Indien nodig, voeg nieuwe regels toe voor Programmacontrole.
9. Configureer de geavanceerde instellingen van Programmacontrole:

   - **Monitor loading of DLL modules**. 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.

     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 "**Golden Image\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.

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 degene die zijn geladen voordat Kaspersky Endpoint Security opstart.

- **Use strict digital signature verification**. U kunt een certificaat selecteren als activerende voorwaarden voor een programmacontrole-regel. Als dit selectievakje is ingeschakeld, past Kaspersky Endpoint Security regels toe op programma's die alleen zijn ondertekend met certificaten uit het vertrouwde certificaatarchief van het systeem. Programma's die met een dergelijk certificaat zijn ondertekend, worden ook door de beschermingsonderdelen, bijvoorbeeld de *Malware-scan*-taak, als vertrouwd beschouwd. Als u echter een certificaat uit een ander archief opgeeft in een programmacontrole-regel, past Kaspersky Endpoint Security een dergelijke regel niet toe.

  Als het selectievakje is uitgeschakeld, past Kaspersky Endpoint Security regels toe op programma's die zijn ondertekend door een certificaat uit het Windows Trusted Root Certificate Store. Dergelijke programma's maken geen deel uit van de vertrouwde zone. Beschermingsonderdelen bewaken de activiteit van dergelijke programma's.

- **Message to user**. Sjabloon van het bericht dat wordt weergegeven bij de activering van een regel van Programmacontrole die de start van een programma blokkeert.

- **Message to administrator**. 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.

10. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Schakel de modus Geblokkeerde progrmma's in de programma-interface in

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Security Controls** → **Programmacontrole** in het venster met de programma-instellingen.
3. Zet de schakelaar **Programmacontrole** aan.
4. Selecteer in het blok **Modus van Controle van programma-opstart Denylist. Alle programma's, behalve deze op de lijst met regels, zijn toegestaan**.
5. In de **Actie op startende aanvragen geblokkeerd door regels** blok, selecteer de actie voor Programmacontrole:

   - **Informeer (Testmodus) en log gebeurtenissen in een rapport**. Programmacontrole blokkeert geen programma's die volgens de regels niet mogen worden uitgevoerd, maar genereert gebeurtenissen over de werking van programma's die anders zouden worden geblokkeerd.

   - **Blokkeren**. Programmacontrole blokkeert de geblokkeerde programma's en genereert overeenkomstige gebeurtenissen.

6. Selecteer de status voor de regel van Programmacontrole:

- **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.
- **Testmodus**. 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.

Indien nodig, voeg nieuwe regels toe voor Programmacontrole.

7. Configureer de geavanceerde instellingen van Programmacontrole:

- **Controleer het laden van DLL-modules**. 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.

  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 "**Golden Image\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.

  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 degene die zijn geladen voordat Kaspersky Endpoint Security opstart.

- **Strikte digitale-handtekeningsverificatie gebruiken**. U kunt een certificaat selecteren als activerende voorwaarden voor een programmacontrole-regel. Als dit selectievakje is ingeschakeld, past Kaspersky Endpoint Security regels toe op programma's die alleen zijn ondertekend met certificaten uit het vertrouwde certificaatarchief van het systeem. Programma's die met een dergelijk certificaat zijn ondertekend, worden ook door de beschermingsonderdelen, bijvoorbeeld de *Malware-scan*-taak, als vertrouwd beschouwd. Als u echter een certificaat uit een ander archief opgeeft in een programmacontrole-regel, past Kaspersky Endpoint Security een dergelijke regel niet toe.

  Als het selectievakje is uitgeschakeld, past Kaspersky Endpoint Security regels toe op programma's die zijn ondertekend door een certificaat uit het Windows Trusted Root Certificate Store. Dergelijke programma's maken geen deel uit van de vertrouwde zone. Beschermingsonderdelen bewaken de activiteit van dergelijke programma's.

- **Sjablonen van berichten over programmablokkering**. Sjabloon van het bericht dat wordt weergegeven bij de activering van een regel van Programmacontrole die de start van een programma blokkeert.

- **Berichttekst die wordt weergegeven wanneer het starten van een programma wordt geblokkeerd**. 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.

8. Sla uw wijzigingen op.

Als gevolg hiervan blokkeert Programmacontrole de geblokkeerde programma's. Kaspersky Endpoint Security genereert ook *Programma mag niet worden gestart* gebeurtenissen. U kunt deze gebeurtenissen gebruiken om de *Report on prohibited applications* rapport in de Kaspersky Security Center-console. In het overzicht van het rapport ziet u de lijst met programma's en computers waarop de regel van Programmacontrole is geactiveerd.

Programmacontrole op basis van een basiscomputer

U kunt een basiscomputer gebruiken om een afbeelding te maken met een set programma's die u nodig hebt. U kunt deze afbeedling vervolgens gebruiken om het besturingssysteem en de programma's op andere computers te implementeren. Het is niet altijd haalbaar om de afbeelding up-to-date te houden. Met Programmacontrole kunt u een lijst met toegestane programma's bijhouden op basis van een basiscomputer. Programmacontrole bepaalt automatisch welke programma's zijn geïnstalleerd op de basiscomputer en werkt de categorie bij. Op deze manier krijgen de computers een bijgewerkte lijst met toegestane programma's.

De configuratie van Programmacontrole op basis van een basiscomputer omvat de volgende stappen:

1. Een categorie maken die automatisch wordt bijgewerkt. Wanneer u de nieuwe categorie aanmaakt, selecteer de **Category that includes executable files from a specific folder** categorie en selecteer uw basiscomputer.

   Automatisch een bijgewerkte categorie aanmaken in de Beheerconsole (MMC)

   1. Open de Beheerconsole van Kaspersky Security Center.

   2. Selecteer in de structuur van de Beheerconsole de map **Advanced** → **Application management** → **Application categories**.

   3. Klik op de knop **New category** in de werkruimte.

      Hiermee start u de wizard voor het maken van programmacategorieën.

   4. Volg de instructies van de wizard voor het aanmaken van een programmacategorie.

Stap 1. Een soort categorie selecteren

Selecteer **Category that includes executable files from selected devices** als het categorietype.

Stap 2. Een aangepaste categorienaam invoeren

Tijdens deze stap geeft u een naam voor de programmacategorie op.

Stap 3. 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 SHA256 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.

Stap 4. Filter

Configureer bij deze stap een filter voor bestanden.

U kunt het bestandstype opgeven dat u wilt gebruiken om de programmacategorie te maken.

- **All files**. De categorie komt overeen met alle bestanden. Deze optie is standaard geselecteerd.
- **Only files outside the application categories**. De categorie komt alleen overeen met bestanden buiten de programmacategorieën.

U kunt mappen van geselecteerde computers opgeven die bestanden bevatten die u wilt gebruiken om de programmacategorie te maken.

- **All folders**. De categorie komt overeen met alle mappen. Deze optie is standaard geselecteerd.
- **Specified folder**. De categorie komt alleen overeen met de opgegeven map. Als u deze optie selecteert, moet u een pad naar de map opgeven.

Stap 5. Een aangepaste categorie maken

Verlaat de wizard verlaten.

Een categorie aanmaken met inhoud die automatisch wordt toegevoegd in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole **Operations** → **Third-party applications** → **Application categories**.

   Dit opent de lijst met programmacategorieën.

2. Klik op **Add**.

   Hiermee start u de wizard voor het maken van programmacategorieën.

3. Configureer de algemene instellingen van de programmacategorie:

   - Naam van de categorie.
   - Methode voor het maken van categorieën. Selecteer **Category that includes executable files from selected devices** als het categorietype.

   Ga naar de volgende stap.

4. Configureer de geavanceerde instellingen van de programmacategorie:

   - Geef de computers op vanaf welke Kaspersky Security Center uitvoerbare bestanden aan de categorie van het programma moet toevoegen. Alle uitvoerbare bestanden van de opgegeven computers die in de map **Executable files** worden weergegeven, worden door Kaspersky Security Center toegevoegd aan de programmacategorie.
   - Selecteer een algoritme voor de berekening van hashfunctie.
   - Configureer een interval voor de synchronisatie van gegevens met de Beheerserver-opslag.
   - Configureer een filter voor bestanden.

5. Verlaat de wizard verlaten.

Wanneer u een categorie aanmaakt die automatisch wordt bijgewerkt, kan het handig zijn om de bestanden in meerdere categorieën onder te verdelen. Bijvoorbeeld bestanden van het besturingssysteem en bestanden van de Program Files map. Hiervoor kunt u een filter in de categorie-instellingen gebruiken en afzonderlijke mappen selecteren.

2. De modus van Programmacontrole selecteren. U moet voorkomen dat alle programma's worden uitgevoerd die niet expliciet zijn toegestaan. Selecteer hiervoor de modus *Geblokkeerde programma's*.

3. Regel van programmacontrole maken. Selecteer in de regelinstellingen de categorie waartoe de uitvoerbare bestanden van de basiscomputer behoren.

   Configureer Programmacontrole op basis van een basiscomputer in de Beheerconsole (MMC)

   1. Open de Beheerconsole van Kaspersky Security Center.
   2. Selecteer in de beheerconsole **Policies**.

3. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

4. Selecteer **Security Controls** → **Programmacontrole** in het beleidsvenster.

5. Selecteer het selectievakje **Programmacontrole**.

6. Gebruik in het blok **Instellingen van Programmacontrole** de vervolgkeuzelijst **Controlemodus** om de **Denylist** te selecteren.

7. Selecteer in de vervolgkeuzelijst **Actie** de acie Programmacontrole:

   - **Regels testen**. Programmacontrole blokkeert geen programma's die volgens de regels niet mogen worden uitgevoerd, maar genereert gebeurtenissen over de werking van programma's die anders zouden worden geblokkeerd.

   - **Regels toepassen**. Programmacontrole blokkeert de geblokkeerde programma's en genereert overeenkomstige gebeurtenissen.

8. Klik in de lijst van regels van Programmacontrole op de knop **Toevoegen**.

   Hiermee start u de wizard voor het toevoegen van een regel van Programmacontrole.

9. In de **Categorie** vervolgkeuzelijst selecteer een categorie die automatisch wordt bijgewerkt op basis van de basiscomputer.

10. Selecteer de gebruikers of groep gebruikers waarop u de regel voor Programmacontrole wilt toepassen.

11. Configureer de geavanceerde instellingen van de regel van Programmacontrole:

    - **Weigeren voor andere gebruikers**. Het programma verhindert de start van programma's die behoren tot de geselecteerde categorie voor alle gebruikers die niet in de lijst staan.

    - **Vertrouwde updaters**. Kaspersky Endpoint Security beschouwt programma's uit de geselecteerde categorie als vertrouwde updaters die andere uitvoerbare bestanden mogen aanmaken die daarna mogen worden uitgevoerd.

12. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Configureer Programmacontrole op basis van een basiscomputer in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de Webconsole het tabblad **Asset management** → **Policies**.

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** → **App Control**.

5. Zet de schakelaar **Application Control ENABLED** aan.

6. Selecteer in het blok **Operating mode Block all except the rules list**.

7. In de **Action** blok, selecteer de actie voor Programmacontrole:

   - **Inform**. Programmacontrole blokkeert geen programma's die volgens de regels niet mogen worden uitgevoerd, maar genereert gebeurtenissen over de werking van programma's die anders zouden worden geblokkeerd.

   - **Apply rules**. Programmacontrole blokkeert de geblokkeerde programma's en genereert overeenkomstige gebeurtenissen.

8. Klik in de lijst van regels van Programmacontrole op de knop **Add**.

   Hiermee start u de wizard voor het toevoegen van een regel van Programmacontrole.

9. Onder **Categories/Applications**, selecteer een categorie die automatisch wordt bijgewerkt op basis van de computer in de basislijn.

10. Selecteer de gebruikers of groep gebruikers waarop u de regel voor Programmacontrole wilt toepassen.

11. Configureer de geavanceerde instellingen van de regel van Programmacontrole:

    - **Users**. Het programma verhindert de start van programma's die behoren tot de geselecteerde categorie voor alle gebruikers die niet in de lijst staan.

    - **Trusted Updaters**. Kaspersky Endpoint Security beschouwt programma's uit de geselecteerde categorie als vertrouwde updaters die andere uitvoerbare bestanden mogen aanmaken die daarna mogen worden uitgevoerd.

12. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Configureer Programmacontrole op basis van een basiscomputer in de programma-interface

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

2. Selecteer **Security Controls** → **Programmacontrole** in het venster met de programma-instellingen.

3. Zet de schakelaar **Programmacontrole** aan.

4. Selecteer in het blok **Modus van Controle van programma-opstart Denylist. Alle programma's, behalve deze op de lijst met regels, zijn toegestaan**.

5. In de **Actie op startende aanvragen geblokkeerd door regels** blok, selecteer de actie voor Programmacontrole:

   - **Informeer (Testmodus) en log gebeurtenissen in een rapport**. Programmacontrole blokkeert geen programma's die volgens de regels niet mogen worden uitgevoerd, maar genereert gebeurtenissen over de werking van programma's die anders zouden worden geblokkeerd.

   - **Blokkeren**. Programmacontrole blokkeert de geblokkeerde programma's en genereert overeenkomstige gebeurtenissen.

6. Klik in de lijst van regels van Programmacontrole op de knop **Toevoegen**.

   Hiermee start u de wizard voor het toevoegen van een regel van Programmacontrole.

7. Onder **Categorie**, selecteer een categorie die automatisch wordt bijgewerkt op basis van de computer in de basislijn.

8. Selecteer de gebruikers of groep gebruikers waarop u de regel voor Programmacontrole wilt toepassen.

9. Configureer de geavanceerde instellingen van de regel van Programmacontrole:

    - **Weigeren voor andere gebruikers**. Het programma verhindert de start van programma's die behoren tot de geselecteerde categorie voor alle gebruikers die niet in de lijst staan.

    - **Vertrouwde updaters**. Kaspersky Endpoint Security beschouwt programma's uit de geselecteerde categorie als vertrouwde updaters die andere uitvoerbare bestanden mogen aanmaken die daarna mogen worden uitgevoerd.

10. Sla uw wijzigingen op.

Regels van programmacontrole beheren

Kaspersky Endpoint Security regelt het opstarten van programma's door gebruikers met behulp van regels. 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.
- **Testmodus**. 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 activeringsvoorwaarde voor een regel van Programmacontrole toevoegen

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.

Een programmacategorie maken in de Beheerconsole:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de structuur van de Beheerconsole de map **Advanced** → **Application management** → **Application categories**.
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. Data of executable files is manually added to the category Als u dit type categorie hebt geselecteerd, kunt u in de stap *Configuring conditions for inclusion of applications in categories* en de stap *Configuring conditions for exclusion of applications from categories* de criteria definiëren voor de opname van uitvoerbare bestanden in de categorie.
- Category that includes executable files from selected devices. These executable files are processed automatically and their metrics are added to the category Als u deze soort categorie hebt geselecteerd, kunt u tijdens de stap *Settings* een computer opgeven waarvan de uitvoerbare bestanden automatisch moeten worden toegevoegd aan de categorie.
- Category that includes executable files from a specific folder. Executable files of applications copied to the specified folder are automatically processed and their metrics are added to the category Als u deze soort categorie hebt geselecteerd, kunt u tijdens de stap *Repository folder* 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

Wanneer u een groot aantal voorwaarden toevoegt aan de programmacontroleregels (bijvoorbeeld bestandshashes), neemt het verbruik van computerbronnen toe. Wanneer het totale aantal voorwaarden 50.000 bereikt, kunnen prestatieproblemen optreden. Voor optimale prestaties wordt aanbevolen om het aantal voorwaarden te bekijken en te verminderen.

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 fingerprint** 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 Applications* 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 (masks supported)**. 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 fingerprint** niet is opgegeven in de eigenschappen van de voorwaarden, wordt u aanbevolen deze voorwaarden niet te gebruiken.

  U kunt het certificaatarchief kiezen. Standaard past Programmacontrole alleen regels toe voor programma's die zijn ondertekend met een certificaat uit het vertrouwde systeemcertificaatarchief. Dit wordt mogelijk gemaakt door het **Strikte digitale handtekeningsverificatie gebruiken** selectievakje.

- **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 Applications* 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 (masks supported)**. 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 SHA256 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.

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 SHA256 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 **Scan interval (1–168 hours)** veld. 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.

  Het veld is beschikbaar als het selectievakje **Force folder scan for changes** is ingeschakeld.

Stap 7. Een aangepaste categorie maken

Verlaat de wizard verlaten.

Zo voegt u een nieuwe activeringsvoorwaarde voor een regel van Programmacontrole toe in de programma-interface:

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: N** of **Uitzonderingen: N** 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 `*` en `?` tekens voor het invoeren van een masker in metadata: **File name**, **Application name**, **Vendor**.
- 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 **Certificaathouder** 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**.

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 **Advanced → Application management → Executable files**.
3. Selecteer in de werkruimte 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.
   - Selecteer in het blok **Rule type** 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 SHA256 hashes for files without a certificate)**.
  - **Certificate details (files without a certificate will be skipped)**.
  - **Only SHA256 (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.
   - Selecteer in het blok **Rule type** 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

Zo kunt u een regel van Programmacontrole toevoegen via Kaspersky Security Center:

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Security Controls** → **Programmacontrole** in het beleidsvenster.
   Rechts in het venster ziet u de instellingen van het onderdeel Programmacontrole.
4. Klik op **Toevoegen**.
   Het venster **Regel van Programmacontrole** wordt geopend.
5. 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.

6. Klik in de tabel **Gebruikers en hun rechten** op de knop **Toevoegen**.

   U kunt gebruikers selecteren in Active Directory, in de lijst van accounts in Kaspersky Security Center, of door handmatig een lokale gebruikersnaam in te voeren. Kaspersky raadt aan om locale gebruikersaccounts alleen in speciale gevallen te gebruiken, wanneer het niet mogelijk is om domeingebruikersaccounts te gebruiken.

7. In de tabel **Gebruikers 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 **Blokkeren** bij de relevante rijen uit.

8. Schakel het selectievakje **Weigeren voor andere gebruikers** in als u wilt instellen dat alle gebruikers die niet in de kolom **Gebruiker of groep** verschijnen en die geen lid zijn van de opgegeven groep gebruikers in de kolom **Gebruiker of groep** geen programma's mogen starten die tot de geselecteerde categorie behoren.

9. 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.

10. Sla uw wijzigingen op.

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. Klik in de tabel **Gebruikers en hun rechten** op de knop **Toevoegen**.

      U kunt gebruikers selecteren in Active Directory, in de lijst van accounts in Kaspersky Security Center, of door handmatig een lokale gebruikersnaam in te voeren. Kaspersky raadt aan om locale gebruikersaccounts alleen in speciale gevallen te gebruiken, wanneer het niet mogelijk is om domeingebruikersaccounts te gebruiken.

      De regel geldt standaard voor alle gebruikers.

      > Als er geen gebruiker in de tabel is opgegeven, kan de regel niet worden opgeslagen.

d. Gebruik in de tabel **Gebruikers 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 **Gebruikers en hun rechten** en die geen lid zijn van gebruikersgroepen vermeld in de tabel **Gebruikers 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 **Gebruikers en hun rechten** en die niet behoren tot opgegeven groepen gebruikers in de tabel **Gebruikers 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: N** de lijst met inclusievoorwaarden voor activering van de regel.
7. Maak of bewerk op het tabblad **Uitzonderingen: N** 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.

De status van een regel van Programmacontrole wijzigen via Kaspersky Security Center

Zo wijzigt u de status van een regel van programmacontrole in de beheerconsole:

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Security Controls** → **Programmacontrole** in het beleidsvenster.

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

4. 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 het onderdeel Programmacontrole actief is.
   - **Uit**. 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 de regel van toepassing is maar informatie over de opstart van zulke programma's in het rapport registreert.

5. Sla uw wijzigingen op.

Zo wijzigt u de status van een regel van programmacontrole in de programma-interface:

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.
   - **Testmodus**. 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 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 rogrammacontrole 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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Security Controls** → **Programmacontrole** in het beleidsvenster.
4. 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 koppeling **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.
5. Een lijst met regels van programmacontrole importeren:
   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.
6. Sla uw wijzigingen op.

Een lijst met regels van programmacontrole exporteren en importeren in de Webconsole en de Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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** → **App Control**.
5. Selecteer onder **Operating mode** een lijst met regels: denylist of allowlist voor programma's.
6. De lijst met regels exporteren:
   a. Selecteer de regels die u wilt exporteren.
   b. Klik op de knop → **Export**.
      Kaspersky Endpoint Security exporteert de lijst met regels naar een JSON-bestand in de standaard downloadmap.

7. De lijst met regels importeren:

   a. Klik op de knop → **Import**.

      Selecteer in het geopende venster het JSON-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 JSON-bestand.

8. Sla uw wijzigingen op.

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 **Events**.
5. Klik op de knop **Clear all**.
6. Schakel in de tabel **Events** 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 **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** selecteer **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. 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.

In- en uitschakelen van testen van regels van Programmacontrole

Zo schakelt u het testen voor regels van Programmacontrole in Kaspersky Security Center in of uit:

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.

2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

3. Selecteer **Security Controls → Programmacontrole** in het beleidsvenster.

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

4. Selecteer in de vervolgkeuzelijst **Controlemodus** een van de volgende opties:

   - **Denylist**. Als deze optie is geselecteerd, staat Programmacontrole toe dat alle gebruikers programma's kunnen starten, behalve in gevallen die voldoen aan de voorwaarden van de blokkeringsregels van Programmacontrole.

   - **Allowlist**. Als deze optie is geselecteerd, staat Programmacontrole niet toe dat gebruikers een programma starten, behalve in gevallen waarbij aan de voorwaarden van de uitvoeringsregels van Programmacontrole is voldaan.

5. 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.

6. Sla uw wijzigingen op.

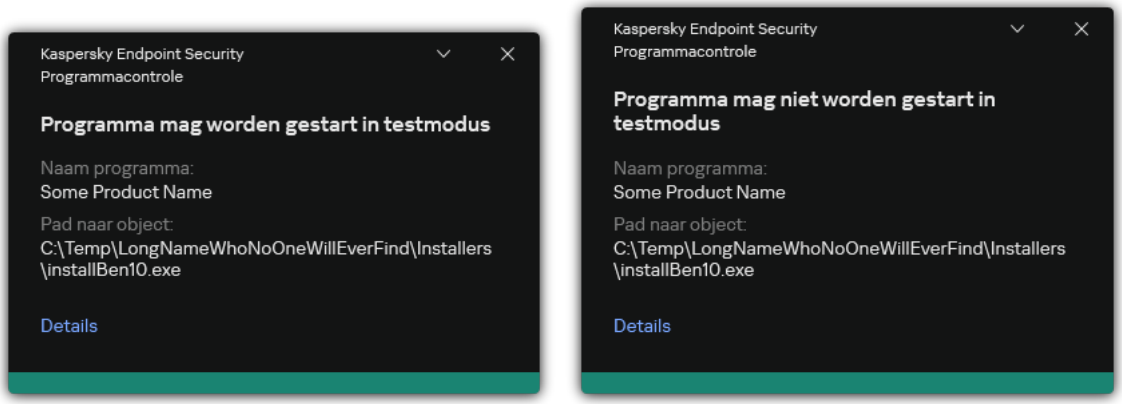
Zo schakelt u het testen van de regels van Programmacontrole in of selecteert u een blokkerende actie voor Programmacontrole:

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 **Testmodus**.

   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

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 **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 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 **Events**.
5. Klik op de knop **Clear all**.
6. Schakel in de tabel de selectievakjes **Events 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**.

Bewaking van programma-activiteit

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.

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 in het hoofdvenster van het programma naar **Bewaking** 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 een 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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Algemene instellingen** → **Interface** in het beleidsvenster.
4. Gebruik het selectievakje **Bewaking van programma-activiteit verbergen** om de toegang tot de tool te verlenen of in te trekken.
5. Sla uw wijzigingen op.

Bewaking van programma-activiteit verbergen in de programma-interface via de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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** → **User Interaction**.

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.

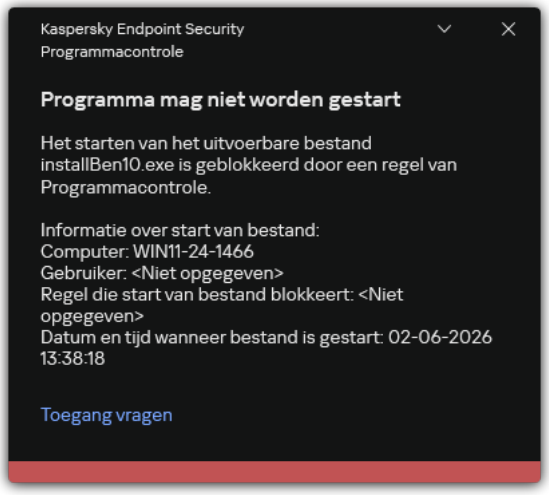
U kunt de volgende normale tekens gebruiken om het masker van een bestands- of mapnaam te maken:

- 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:\Folder\???.txt` omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam `Folder` 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. Kaspersky-experts verstrekken een sjabloon van een bericht aan de gebruiker waarin de redenen worden beschreven waarom het programma werd geblokkeerd (zie de onderstaande afbeelding). Er zijn speciale variabelen voorzien voor het beheer van de berichtsjablonen (bijvoorbeeld `%USER_NAME%`). Met variabelen kan één berichtsjabloon voor verschillende computers worden gebruikt. Bij het genereren van een bericht haalt Kaspersky Endpoint Security de waarde van de variabele op uit de instellingen van het besturingssysteem en voegt het deze in het bericht in dat overeenkomt met de specifieke computer, gebruiker en gebeurtenis.



Melding van programmacontrole

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. Om dit te doen, moet de gebruiker klikken op de **Toegang vragen** en stuur een bericht naar de beheerder met een beschrijving van de situatie. U kunt ook een sjabloon maken van het bericht aan de beheerder, en er gegevens aan toevoegen die u kunnen helpen bij uw beslissing om toegang tot het programma toe te staan of te blokkeren. 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.

Het berichtensjabloon van de Programmacontrole in de beheerconsole (MMC) bewerken

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Security Controls → Programmacontrole** in het beleidsvenster.
4. In het blok **Instellingen voor berichtsjablonen**, klikt u op de knop **Sjablonen**.
5. Dit opent een venster. Configureer in dat venster het sjabloon 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.

     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.

   Als u een variabele aan de sjabloontekst wilt toevoegen, plaats dan de cursor op de gewenste positie, klik op **Variabele** en selecteer de gewenste variabele in de lijst met beschikbare opties.

   U kunt de standaardsjabloontekst ook herstellen met de knop **Standaard**.
6. Sla uw wijzigingen op.

Het berichtensjabloon van de Programmacontrole in de Webconsole en Cloudonsole bewerken

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management → Policies**.
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 → App Control**.

5. In de **Message templates** blok, klik op de **Messages about application startup block** sjablonen voor Programmacontrole-berichten koppelen en configureren:

   - **Message to user**. Sjabloon van het bericht dat wordt weergegeven bij de activering van een regel van Programmacontrole die de start van een programma blokkeert.

     U kunt geen berichtsjablonen configureren voor programmacontrole in testmodus. Programmacontrole in testmodus geeft vooraf ingestelde meldingen weer.

   - **Message to administrator**. 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.

   Als u een variabele aan de sjabloontekst wilt toevoegen, plaats dan de cursor op de gewenste positie, klik op **Add variable** en selecteer de gewenste variabele in de lijst met beschikbare opties.

   U kunt de standaardsjabloontekst ook herstellen met de knop **Reset to default**.

6. Sla uw wijzigingen op.

Het berichtensjabloon van de Programmacontrole in het programma-interface bewerken

1. Klik in het hoofdvenster van het programma op de knop ⚙.

2. Selecteer **Security Controls** → **Programmacontrole** in het venster met de programma-instellingen.

3. Configureer in het blok **Sjablonen van berichten over programmablokkering** de 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.

     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.

   Als u een variabele aan de sjabloontekst wilt toevoegen, plaats dan de cursor op de gewenste positie, klik op **Variabele toevoegen** en selecteer de gewenste variabele in de lijst met beschikbare opties.

   U kunt de standaardsjabloontekst ook herstellen met de knop **Opnieuw instellen**.

4. Sla uw wijzigingen op.

Variabelen in berichtsjablonen van Programmacontrole

U kunt de volgende variabelen gebruiken in sjablonen voor berichten voor gebruikers of berichten voor beheerders:

- **Naam van de regel die is geactiveerd** – `%RULE%`.

  Naam van de regel die de uitvoering van een bestand blokkeerde.

- **Huidige datum** – `%DATE%`.

  Datum waarop de uitvoering van het bestand werd geblokkeerd in het formaat DD.MM.YYYY.

- **Huidige tijd** – `%TIME%`.

  Tijdstip waarop de uitvoering van bestanden in het formaat UU:MM werd geblokkeerd.

- **Gebruikersnaam** – `%USER_NAME%`.

  Naam van het huidige gebruikersaccount op de computer waarop de uitvoering van het bestand is geblokkeerd, in het `<device name>\<user alias>` formaat (bijvoorbeeld `DESKTOP-123\John.Smith`).

- **Computernaam** – `%COMPUTER_NAME%`.

  Naam van de computer waarop de uitvoering van het bestand is geblokkeerd.

- **Naam van uitvoerbaar bestand** – `%FILE_NAME%`.

  Naam van het uitvoerbare bestand van het geblokkeerde programma.

- **KL-categorie van het uitvoerbare bestand** – `%KL_CAT%`.

  KL-categorie waartoe het geblokkeerde programma behoort (bijvoorbeeld *Browsers* of een andere categorie).

- **Pad naar uitvoerbaar bestand** – `%FILE_PATH%`.

  Volledig pad naar het uitvoerbare bestand van het geblokkeerde programma.

- **Versie van uitvoerbaar bestand** – `%FILE_VERSION%`.

  Versie van het uitvoerbare bestand van het geblokkeerde programma.

- **Oorspronkelijke naam van het uitvoerbare bestand** – `%ORIGINAL_FILE_NAME%`.

  Oorspronkelijke naam van het uitvoerbare bestand van het geblokkeerde programma. De bestandsnaam wordt opgegeven in de eigenschappen van het uitvoerbare bestand van het programma.

- **Leverancier** – `%FILE_PUBLISHER%`.

  Leverancier van het geblokkeerde programma.

- **Naam programma** – `%FILE_PRODUCT_NAME%`.

  Naam van het geblokkeerde programma.

- **Programmaversie** – `%PRODUCT_VERSION%`.

  Versie van het geblokkeerde programma.

- **Hash van uitvoerbaar bestand** – `%FILE_HASH%`.

  Hash van het uitvoerbare bestand van het geblokkeerde programma.

- **Certificaatverlener** – `%CERT_ISSUER%`.

  Verstrekker van het certificaat waarmee het uitvoerbare bestand is ondertekend.

- **Certificaathouder** – `%CERT_SUBJECT%`.

  Onderwerp van het certificaat waarmee het uitvoerbare bestand is ondertekend.

- **Vingerafdruk van certificaat** – `%CERT_THUMBPRINT%`.

  Vingerafdruk van het certificaat waarmee het uitvoerbare bestand is ondertekend.

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 doen:

   a. Start de inventarisatietaak.

      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 **Application folder** is mogelijk onveilig omdat alle programma's uit de opgegeven map mogen worden gestart. Het is aanbevolen om de programmacategorieën die de voorwaarde **Application folder** 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 **Executable files**

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 Programmacontrole-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 **Application folder** en geef het pad naar die map op. Maak vervolgens een Toestaan-regel en selecteer deze categorie.

  Het gebruik van de voorwaarde **Application folder** is mogelijk onveilig omdat alle programma's uit de opgegeven map mogen worden gestart. Het is aanbevolen om de programmacategorieën die de voorwaarde **Application folder** 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, Web Threat Protection, Gedragsdetectie en Exploit-preventie 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.

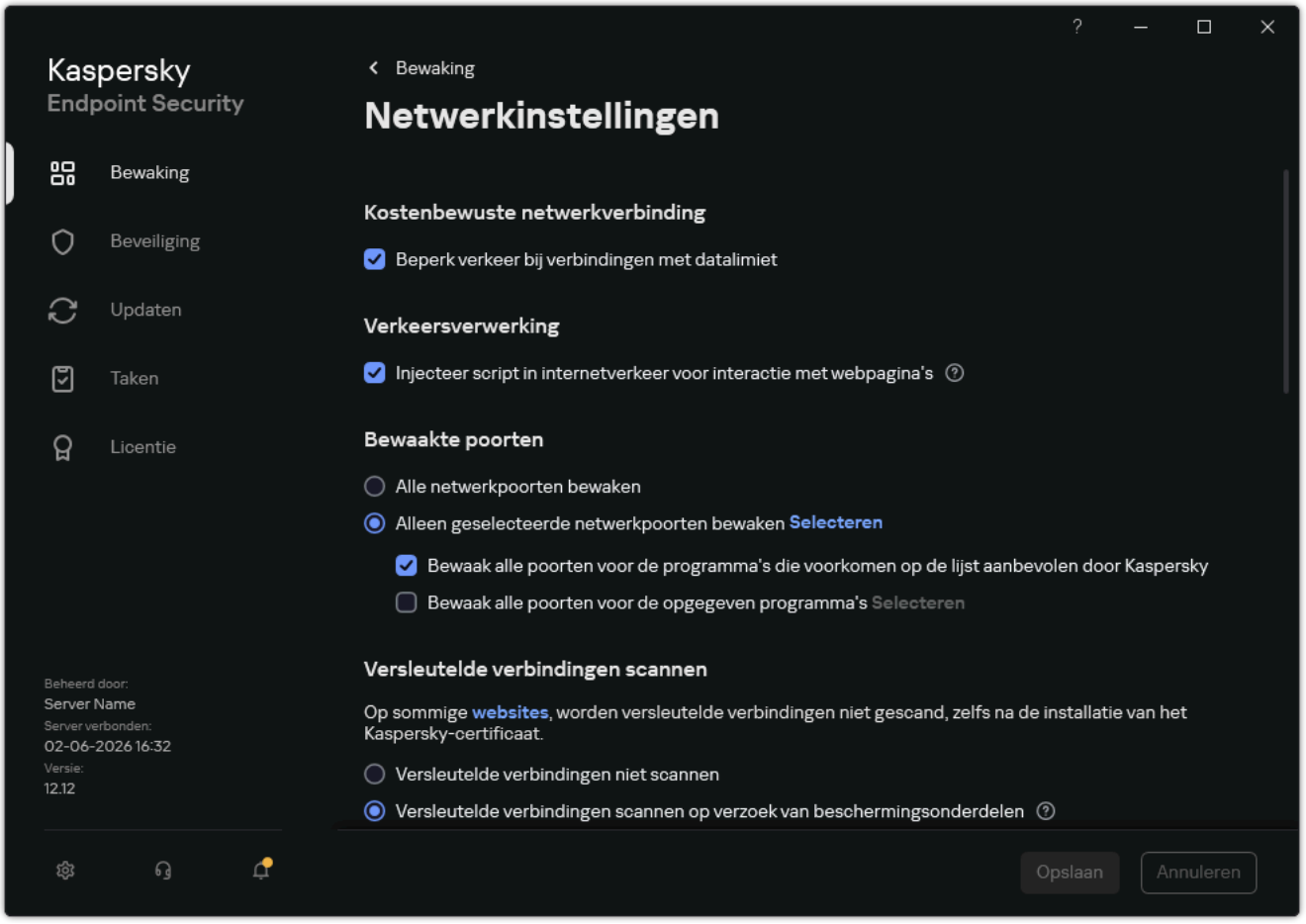
Kaspersky Endpoint Security verdeelt TCP- en UDP-poorten van de computer van de gebruiker in verschillende groepen, afhankelijk van het mogelijke gevaar via deze poorten. Sommige netwerkpoorten zijn voorbehouden voor kwetsbare services. U wordt aanbevolen om deze poorten nauwlettend te bewaken omdat ze veel meer kans hebben om het doelwit van netwerkaanvallen te zijn. Als u niet-standaardservices gebruikt die niet-standaardnetwerkpoorten nodig hebben, kunnen deze netwerkpoorten ook het doelwit zijn van een aanvallende computer. U kunt lijsten maken met netwerkpoorten en programma's die netwerktoegang vragen. Deze poorten en programma's krijgen dan bijzondere aandacht van de onderdelen Mail Threat Protection en Web Threat Protection tijdens het monitoren van het netwerkverkeer.

Om de beveiliging van de computer te waarborgen, Gedragsdetectie en Exploit-preventie onderdelen bewaken ook gegevensstromen die via netwerkpoorten gaan. De onderdelen monitoren continu het netwerkverkeer op individuele processen die mogelijk bedreigend zijn.

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.



Instellingen voor het bewaken van netwerkpoorten

3. Selecteer in het blok **Bewaakte poorten** **Alle netwerkpoorten bewaken**.
4. Sla uw wijzigingen op.

Een lijst met bewaakte netwerkpoorten aanmaken

Het wijzigen van de lijst met bewaakte netwerkpoorten wordt mogelijk geblokkeerd door de eigenschappen van het bovenliggende beleid. Om de lijst te wijzigen, moet u toestaan dat de instellingen van vertrouwde zone in de Webconsole (het "hangslot" moet ontgrendeld zijn).

Vertrouwde zones zijn verschillend gegroepeerd in de Beheerconsole (MMC) en de Webconsole. Ook de manier waarop wijziging in de parameters voor de vertrouwde zone worden voorkomen, verschilt (verschillende "hangsloten"). We raden aan dat u alleen de Webconsole gebruikt om het programma te beheren. Als u de vertrouwde zone in verschillende consoles configureert, kan de beheerplug-in het "hangslot" terugzetten naar de standaardstatus.

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 Acrobat Reader.
   - Apple Application Support.
   - Google Chrome.
   - Microsoft Edge.
   - Mozilla Firefox.
   - Internet Explorer.
   - Java.
   - mIRC.
   - Opera.
   - Pidgin.
   - Safari.
   - Mail.ru Agent.
   - Yandex Browser.
5. Selecteer het selectievakje **Bewaak alle poorten voor de opgegeven programma's**.

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. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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** → **Network Settings**.

5. De lijst met netwerkpoorten 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.

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.

2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

3. Selecteer **Algemene instellingen** → **Netwerkinstellingen** in het beleidsvenster.

4. Selecteer in het blok **Bewaakte poorten Alleen geselecteerde netwerkpoorten bewaken**.

5. 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.

6. De lijst met netwerkpoorten 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.

7. De lijst met programma's exporteren waarvan de poorten worden bewaakt door Kaspersky Endpoint Security:

    a. Selecteer het selectievakje **Bewaak alle poorten voor de opgegeven programma's**.

    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.

8. 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.

9. 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.

10. Sla uw wijzigingen op.

Log Inspectie

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

Vanaf versie 11.11.0 omvat Kaspersky Endpoint Security voor Windows het onderdeel Log Inspectie. Log Inspectie bewaakt de integriteit van de beschermde omgeving op basis van de inspectiere van het Windows-gebeurtenislogboek. Wanneer het programma tekenen van atypisch gedrag in het systeem detecteert, informeert het de beheerder, omdat dit gedrag kan wijzen op een poging tot cyberaanval.

Kaspersky Endpoint Security analyseert Windows-gebeurtenislogboeken en detecteert overtreding van de regels. De component bevat voorgedefinieerde regels. Voorgedefinieerde regels worden aangedreven door heuristische analyse. U kunt ook uw eigen regels toevoegen (aangepaste regels). Wanneer een regel wordt geactiveerd, maakt hete programma een gebeurtenis met de status *Critical* (zie onderstaande afbeelding).

Als u log inspectie wilt gebruiken, zorg er dan voor dat de beveiligingsinstellingen van het auditbeleid zijn geconfigureerd en dat het systeem de relevante gebeurtenissen vastlegt (raadpleeg de technische ondersteuningswebsite van Microsoft voor details).



Melding log inspectie

Voorgedefinieerde regels configureren

Voorgedefinieerde regels bevatten sjablonen van abnormale activiteit op de beveiligde computer. Abnormale activiteit kan een poging tot aanval omvatten. Voorgedefinieerde regels worden aangedreven door heuristische analyse. Er zijn zeven vooraf gedefinieerde regels beschikbaar voor Log Inspectie. U kunt al deze regels inschakelen of uitschakelen. Voorgedefinieerde regels kunnen niet worden verwijderd.

U kunt de activeringscriteria configureren voor regels die de volgende gebeurtenissen bewaken:

- Detectie brute-force-aanval wachtwoorden
- Netwerk login detectie

Voorgedefinieerde regels configureren in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Security Controls** → **Log Inspectie** in het beleidsvenster.
4. Zorg ervoor dat het selectievakje **Log Inspectie** ingeschakeld is.
5. In het blok **Voorgedefinieerde regels**, klikt u op de knop **Instellingen**.
6. Schakel selectievakjes in of uit om vooraf gedefinieerde regels te configureren:
   - **Er zijn patronen van een mogelijke brute-force aanval in het systeem**.
   - **Er is een ongewone activiteit gedetecteerd tijdens een netwerk aanmeldsessie**.
   - **Er zijn patronen van mogelijk misbruik van Windows-gebeurtenislogboek**.
   - **Ongewone acties gedetecteerd in naam van een nieuwe geïnstalleerde service**.
   - **Ongewone aanmelding die expliciete referenties gebruikt gedetecteerd**.
   - **Er zijn patronen van een mogelijke Kerberos vervalste PAC (MS14-068) aanval in het systeem**.
   - **Verdachte wijzigingen gedetecteerd in de bevoorrechte ingebouwde Beheerders groep**.
7. Configureer indien nodig de regel **Er zijn patronen van een mogelijke brute-force aanval in het systeem**:
   a. Klik op de knop **Instellingen** onder de regel.
   b. Geef in het geopende venster het aantal pogingen en een tijdsperiode waarbinnen pogingen om een wachtwoord in te voeren moeten worden uitgevoerd om de regel te activeren.
   c. Klik op **OK**.
8. Als u de regel **Er is een ongewone activiteit gedetecteerd tijdens een netwerk aanmeldsessie** hebt geselecteerd, dan moet u de instellingen configureren:
   a. Klik op de knop **Instellingen** onder de regel.
   b. Specificeer in het blok **Netwerk aanmeld detectie** het begin en het einde van het tijdsinterval.

      Kaspersky Endpoint Security beschouwt aanmeldingspogingen die tijdens dit gedefinieerde interval worden uitgevoerd als abnormale activiteit.

      Het interval is standaard niet ingesteld en het programma controleert de aanmeldingspogingen niet. Stel de interval in op 00:00 - 23:59 zodat het programma voortdurend aanmeldingspogingen controleert. Het begin en het einde van het interval mogen niet samenvallen. Als ze hetzelfde zijn, controleert de toepassing de aanmeldingspogingen niet.

c. Maak de lijst met vertrouwde gebruikers en vertrouwde IP-adressen (IPv4 en IPv6).

U kunt gebruikers selecteren in Active Directory, in de lijst van accounts in Kaspersky Security Center, of door handmatig een lokale gebruikersnaam in te voeren. Kaspersky raadt aan om locale gebruikersaccounts alleen in speciale gevallen te gebruiken, wanneer het niet mogelijk is om domeingebruikersaccounts te gebruiken. Kaspersky Endpoint Security controleert geen aanmeldingspogingen van deze gebruikers en computers.

d. Klik op **OK**.

9. Sla uw wijzigingen op.

Voorgedefinieerde regels configureren via de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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** → **Log Inspection**.
5. Zorg ervoor dat de schakelaar **Log Inspection ENABLED** ingeschakeld is.
6. In het blok **Predefined rules**, schakel de voorgedefinieerde regels in of uit met behulp van de schakelaars:
   - **There are patterns of a possible brute-force attack in the system**.
   - **There is an atypical activity detected during a network logon session**.
   - **There are patterns of a possible Windows Event Log abuse**.
   - **Atypical actions detected on behalf of a new service installed**.
   - **Atypical logon that uses explicit credentials detected**.
   - **There are patterns of a possible Kerberos forged PAC (MS14-068) attack in the system**.

   a. **Suspicious changes detected in the privileged built-in Administrators group**.
7. Configureer indien nodig de regel **There are patterns of a possible brute-force attack in the system**:

   a. Klik op **Settings** onder de regel.

   b. Geef in het geopende venster het aantal pogingen en een tijdsperiode waarbinnen pogingen om een wachtwoord in te voeren moeten worden uitgevoerd om de regel te activeren.

   c. Klik op **OK**.
8. Als u de regel **There is an atypical activity detected during a network logon session** hebt geselecteerd, dan moet u de instellingen configureren:

   a. Klik op **Settings** onder de regel.

   b. Specificeer in het blok **Network logon detection** het begin en het einde van het tijdsinterval.

Kaspersky Endpoint Security beschouwt aanmeldingspogingen die tijdens dit gedefinieerde interval worden uitgevoerd als abnormale activiteit.

Het interval is standaard niet ingesteld en het programma controleert de aanmeldingspogingen niet. Stel de interval in op 00:00 - 23:59 zodat het programma voortdurend aanmeldingspogingen controleert. Het begin en het einde van het interval mogen niet samenvallen. Als ze hetzelfde zijn, controleert de toepassing de aanmeldingspogingen niet.

c. In het blok **Exclusions**, voeg vertrouwde gebruikers en vertrouwde IP-adressen toe (IPv4 en IPv6).

U kunt gebruikers selecteren in Active Directory, in de lijst van accounts in Kaspersky Security Center, of door handmatig een lokale gebruikersnaam in te voeren. Kaspersky raadt aan om locale gebruikersaccounts alleen in speciale gevallen te gebruiken, wanneer het niet mogelijk is om domeingebruikersaccounts te gebruiken. Kaspersky Endpoint Security controleert geen aanmeldingspogingen van deze gebruikers en computers.

d. Klik op **OK**.

9. Sla uw wijzigingen op.

Voorgedefinieerde regels configureren via de programma-interface

1. Klik in het hoofdvenster van het programma op de knop ⚙.
2. Selecteer **Security Controls** → **Log Inspectie** in het venster met de programma-instellingen.
3. Zorg ervoor dat de schakelaar **Log Inspectie** ingeschakeld is.
4. In het blok **Voorgedefinieerde regels**, klikt u op de knop **Configureren**.
5. Schakel selectievakjes in of uit om vooraf gedefinieerde regels te configureren:
   - **Er zijn patronen van een mogelijke brute-force aanval in het systeem**.
   - **Er is een ongewone activiteit gedetecteerd tijdens een netwerk aanmeldsessie**.
   - **Er zijn patronen van mogelijk misbruik van Windows-gebeurtenislogboek**.
   - **Ongewone acties gedetecteerd in naam van een nieuwe geïnstalleerde service**.
   - **Ongewone aanmelding die expliciete referenties gebruikt gedetecteerd**.
   - **Er zijn patronen van een mogelijke Kerberos vervalste PAC (MS14-068) aanval in het systeem**.

   a. **Verdachte wijzigingen gedetecteerd in de bevoorrechte ingebouwde Beheerders groep**.
6. Configureer indien nodig de regel **Er zijn patronen van een mogelijke brute-force aanval in het systeem**:

   a. Klik op **Instellingen** onder de regel.

   b. Geef in het geopende venster het aantal pogingen en een tijdsperiode waarbinnen pogingen om een wachtwoord in te voeren moeten worden uitgevoerd om de regel te activeren.

7. Als u de regel **Er is een ongewone activiteit gedetecteerd tijdens een netwerk aanmeldsessie** hebt geselecteerd, dan moet u de instellingen configureren:

   a. Klik op **Instellingen** onder de regel.

   b. Specificeer in het blok **Netwerk logon detectie** het begin en het einde van het tijdsinterval.

      Kaspersky Endpoint Security beschouwt aanmeldingspogingen die tijdens dit gedefinieerde interval worden uitgevoerd als abnormale activiteit.

      Het interval is standaard niet ingesteld en het programma controleert de aanmeldingspogingen niet. Stel de interval in op 00:00 - 23:59 zodat het programma voortdurend aanmeldingspogingen controleert. Het begin en het einde van het interval mogen niet samenvallen. Als ze hetzelfde zijn, controleert de toepassing de aanmeldingspogingen niet.

   c. In het blok **Uitzonderingen**, voeg vertrouwde gebruikers en vertrouwde IP-adressen toe (IPv4 en IPv6).

      U kunt gebruikers selecteren in Active Directory, in de lijst van accounts in Kaspersky Security Center, of door handmatig een lokale gebruikersnaam in te voeren. Kaspersky raadt aan om locale gebruikersaccounts alleen in speciale gevallen te gebruiken, wanneer het niet mogelijk is om domeingebruikersaccounts te gebruiken. Kaspersky Endpoint Security controleert geen aanmeldingspogingen van deze gebruikers en computers.

8. Sla uw wijzigingen op.

Als gevolg hiervan maakt Kaspersky Endpoint Security bij het activeren van de regel een *Kritieke gebeurtenis*.

Aangepaste regels toevoegen

U kunt uw eigen activeringscriteria voor Log inspectie regels instellen. Hiervoor moet je een gebeurtenis-ID invoeren en een gebeurtenisbron selecteren. Je kunt de gebeurtenis-ID opzoeken op de website voor technische support van Microsoft. U kunt een gebeurtenisbron selecteren uit de standaardlogboeken: *Application*, *Security* or *System*. U kunt ook het logboek van een programma van derden specificeren. U kunt de naam van het logboek van het programma van derden achterhalen met behulp van de tool Event Viewer. Logboeken van programma's van derden worden bewaard in de map Application and Services Logs (bijvoorbeeld het logboek *Windows PowerShell*).

> Het programma controleert niet of het opgegeven logboek daadwerkelijk aanwezig is in het Windows-gebeurtenislogboek. Als de naam van het logboek een fout bevat, controleert het programma de gebeurtenissen uit dat logboek niet.

De lijst met aangepaste regels bevat al drie regels die zijn gemaakt door Kaspersky-experts.

Een aangepaste regel toevoegen in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Security Controls** → **Log Inspectie** in het beleidsvenster.
4. Zorg ervoor dat het selectievakje **Log Inspectie** ingeschakeld is.
5. In het blok **Aangepaste regels**, klikt u op de knop **Instellingen**.
6. Schakel in het venster dat opent de selectievakjes in naast de aangepaste regels die u wilt inschakelen.

7. Klik indien nodig op **Toevoegen** om uw eigen aangepaste regels te creëren.

8. Dit opent een venster. Configureer in dat venster de aangepaste regel:

   - **Regelnaam**.
   - **Log naam**. Windows-gebeurtenislogboeken. De volgende logboeken zijn beschikbaar: *Application*, *Security*, *System*.
   - **Bron**. Programmalogboeken van derden. U kunt de naam van het logboek van het programma van derden achterhalen met behulp van de tool Event Viewer. Logboeken van programma's van derden worden bewaard in de map Application and Services Logs (bijvoorbeeld het logboek *Windows PowerShell*).
   - **Gebeurtenis-identificators**. Gebeurtenis-ID's in het Windows-gebeurtenislogboek. U kunt de gebeurtenis-ID opzoeken in de technische documentatie van Microsoft.

9. Sla uw wijzigingen op.

Een aangepaste regel toevoegen in de Webconsole en de Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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** → **Log Inspection**.
5. Zorg ervoor dat de schakelaar **Log Inspection ENABLED** ingeschakeld is.
6. Selecteer in het blok **Custom rules** de aangepaste regels die u wilt bewerken.
7. Klik indien nodig op **Add** om uw eigen aangepaste regels te creëren.
8. Dit opent een venster. Configureer in dat venster de aangepaste regel:

   - **Rule name**.
   - **Custom log name**. Windows-gebeurtenislogboeken. De volgende logboeken zijn beschikbaar: *Application*, *Security*, *System*.
   - **Origin**. Programmalogboeken van derden. U kunt de naam van het logboek van het programma van derden achterhalen met behulp van de tool Event Viewer. Logboeken van programma's van derden worden bewaard in de map Application and Services Logs (bijvoorbeeld het logboek *Windows PowerShell*).
   - **Event Identifiers**. Gebeurtenis-ID's in het Windows-gebeurtenislogboek. U kunt de gebeurtenis-ID opzoeken in de technische documentatie van Microsoft.

9. Sla uw wijzigingen op.

Een aangepaste regel maken in de programma-interface

1. Klik in het hoofdvenster van het programma op de knop ⚙.
2. Selecteer **Security Controls** → **Log Inspectie** in het venster met de programma-instellingen.

3. Zorg ervoor dat de schakelaar **Log Inspectie** ingeschakeld is.

4. In het blok **Aangepaste regels**, klikt u op de knop **Configureren**.

5. Schakel in het venster dat opent de selectievakjes in naast de aangepaste regels die u wilt inschakelen.

6. Klik indien nodig op **Toevoegen** om uw eigen aangepaste regels te creëren.

7. Dit opent een venster. Configureer in dat venster de aangepaste regel:

   - **Regelnaam**.
   - **Log naam**. Windows-gebeurtenislogboeken. De volgende logboeken zijn beschikbaar: *Application*, *Security*, *System*.
   - **Bron**. Programmalogboeken van derden. U kunt de naam van het logboek van het programma van derden achterhalen met behulp van de tool Event Viewer. Logboeken van programma's van derden worden bewaard in de map Application and Services Logs (bijvoorbeeld het logboek *Windows PowerShell*).
   - **Gebeurtenis identificator**. Gebeurtenis-ID's in het Windows-gebeurtenislogboek. U kunt de gebeurtenis-ID opzoeken in de technische documentatie van Microsoft.

8. Sla uw wijzigingen op.

Als gevolg hiervan maakt Kaspersky Endpoint Security bij het activeren van de regel een *Critical* gebeurtenis.

Systeemintegriteitscontrole

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

Vanaf versie 12.6, omvat Kaspersky Endpoint Security voor Windows het onderdeel Systeemintegriteitscontrole in plaats van de Bestandsintegriteitsmonitor onderdeel. Het onderdeel Systeemintegriteitscontrole omvat alle functionaliteit van Bestandsintegriteitsmonitor en maakt het bovendien mogelijk om registerwijzigingen en de aansluiting van externe apparaten te monitoren.

Het onderdeel Systeemintegriteitscontrole bewaakt veranderingen in het besturingssysteem die kunnen wijzen op inbreuken op de beveiliging van de computer. Wanneer dergelijke wijzigingen worden gedetecteerd, genereert Kaspersky Endpoint Security overeenkomstige gebeurtenissen en waarschuwt de beheerder. Systeemintegriteitscontrole kan in realtime werken en kan op verzoek ook Systeemintegriteitscheck uitvoeren.

Realtime systeemintegriteitscontrole

In realtime-modus, Systeemintegriteitscontrole houdt wijzigingen bij in objecten die u hebt opgenomen in het bereik van de onderdelen (de *bewakingsbereik*). Met Systeemintegriteitscontrole kan ook ongeautoriseerde toegang tot dergelijke objecten in realtime worden geblokkeerd.

On-demand systeemintegriteitscontrole

On-demand systeemintegriteitscontrole is een taak die u handmatig of volgens een schema kunt uitvoeren. Om de uit te voeren *Systeemintegriteitscheck* taak, moet u het bereik van het onderdeel configureren (de *bewakingsbereik*) en maak een basislijn. Een *basislijn* is een geregistreerde staat van objecten in het systeem, die het programma als referentie gebruikt bij het vergelijken met de huidige staat.

Instellingen voor Bestandsintegriteitsmonitor File migreren

Wanneer u Kaspersky Endpoint Security bijwerkt naar versie 12.6, worden de instellingen van Bestandsintegriteitsmonitor automatisch gemigreerd. Als onderdeel van de migratie verplaatst het programma de monitoringregels naar Systeemintegriteitscontrole. Regels voor bestandsintegriteitsmonitor worden ook gemigreerd naar Systeemintegriteitscontrole wanneer: migreren van KSWS naar KES.

Om een correcte werking van Systeemintegriteitscontrole te garanderen, moeten het Kaspersky Endpoint Security-programma en de beheerplug-in worden bijgewerkt naar versie 12.6. Als u een eerdere versie van de beheerplug-in hebt geïnstalleerd, kunt u Systeemintegriteitscontrole niet configureren omdat de beheerplug-in het gedeelte **Systeemintegriteitscontrole** mist.

Over regels voor Systeemintegriteitscontrole

Om Systeemintegriteitscontrole te laten werken, moet u minimaal één regel toevoegen. een *Regel voor Systeemintegriteitscontrole* is een set criteria die de toegang van gebruikers tot bestanden en het register definiëren. Systeemintegriteitscontrole detecteert wijzigingen in de bestanden en het register binnen de opgegeven *bewakingsbereik*. Het bereik van de controle is een van de criteria van een regel voor Systeemintegriteitscontrole.

Met Systeemintegriteitscontrole kunt u de volgende objecten bewaken:

- Bestanden
- Register
- Externe apparaten

Speciale overwegingen bij bestandsbewaking

Systeemintegriteitscontrole bewaakt wijzigingen in bestanden en mappen, evenals bestanden die worden toegevoegd aan het bewakingsbereik of eruit worden verwijderd. Deze wijzigingen kunnen wijzen op inbreuk van de computerbeveiliging. We raden aan om zelden gewijzigde objecten of objecten toe te voegen waartoe alleen de beheerder toegang heeft. Dit zal het aantal gebeurtenissen van de Systeemintegriteitscontrole verminderen.

> Systeemintegriteitscontrole bewaakt geen wijzigingen in bestanden in de gedeelde servermappen. Systeemintegriteitscontrole kan alleen lokaal worden gebruikt.

Kaspersky Endpoint Security controleert de wijzigingen van bestanden en mappen alleen op die schijven die waren aangesloten toen Realtime systeemintegriteitscontrole begon te werken. Als er geen schijf was aangesloten toen Realtime systeemintegriteitscontrole begon te werken, controleert de toepassing de wijzigingen van bestanden en mappen op die schijf niet, zelfs niet als de bestanden en mappen worden toegevoegd aan het bewakingsgbereik.

Speciale overwegingen bij registerbewaking

Systeemintegriteitscontrole bewaakt het register. Deze wijzigingen kunnen wijzen op inbreuk van de computerbeveiliging.

Systeemintegriteitscontrole controleert de volgende hoofdsleutels van het register:

- `HKCR`
- `HKLM`
- `HKU`
- `HKCC`

- HKEY_CLASSES_ROOT
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG (alleen beschikbaar in Realtime systeemintegriteitscontrole)
- HKEY_CURRENT_USER (alleen beschikbaar in Realtime systeemintegriteitscontrole)

> De taak *Systeemintegriteitscheck* ondersteund de HKEY_CURRENT_USER-sleutel niet. U kunt een sleutel specificeren onder HKEY_USERS als HKEY_USERS\<user profile ID>\<key>.

Speciale overwegingen bij bewaking van externe apparaten

Systeemintegriteitscontrole bewaakt het aansluiten en loskoppelen van externe apparaten. Dit is nodig om de computer te beschermen tegen beveiligingsrisico's die het gevolg kunnen zijn van bestandsuitwisseling met dergelijke apparaten. Systeemintegriteitscontrole controleert de toegang tot externe apparaten niet en blokkeert de bestandsuitwisseling niet. U kunt de toegang tot apparaten configureren met een ander programmacomponent, Apparaatcontrole.

> Tijdens het uitvoeren van de taak *Baseline systeemintegriteitsmonitor* negeert het programma het opnieuw verbinden van externe apparaten als de apparaten dezelfde schijfletter in het besturingssysteem hebben. Om te worden geregistreerd, moeten de opnieuw verbonden apparaten andere schijfletters hebben.

Systeemintegriteitscontrole bewaakt de aansluiting van de volgende typen externe apparaten:

- Verwisselbare schijf (inclusief USB-flashstations)
- Harde schijf
- Externe netwerkadapter
- CD/DVD/Blu-ray-station
- Scanner / camera

Realtime systeemintegriteitscontrole

Met Systeemintegriteitscontrole kunnen wijzigingen in het besturingssysteem in realtime worden gevolgd. U kunt wijzigingen volgen die kunnen wijzen op inbreuken op de beveiliging op de computer. Met de onderdelen kunnen deze wijzigingen worden geblokkeerd of alleen wijzigingsgebeurtenissen worden geregistreerd.

Om Systeemintegriteitscontrole te laten werken, moet u minimaal één regel toevoegen. een *Regel voor Systeemintegriteitscontrole* is een set criteria die de toegang van gebruikers tot bestanden en het register definiëren. Systeemintegriteitscontrole detecteert wijzigingen in de bestanden en het register binnen de opgegeven *bewakingsbereik*. Het bereik van de controle is een van de criteria van een regel voor Systeemintegriteitscontrole.

Modi van Realtime systeemintegriteitscontrole

Om ervoor te zorgen dat de regels voor Systeemintegriteitscontrole geen acties blokkeren met bronnen die essentieel zijn voor het functioneren van het besturingssysteem of andere services, raden we aan de testmodus in te schakelen en te analyseren hoe het onderdeel het systeem beïnvloedt. Als de testmodus is ingeschakeld, blokkeert Kaspersky Endpoint Security geen gebruikersactiviteit die door de regels is verboden, maar genereert het *Waarschuwing* ⚠ evenementen.

Het onderdeel Realtime systeemintegriteitscontrole heeft twee modi:

- Blokkeren

  In deze modus houdt Systeemintegriteitscontrole veranderingen in het systeem bij en voert het een actie uit in overeenstemming met de regels: **Toestaan** of **Blokkeren**. Systeemintegriteitscontrole genereert ook een overeenkomstige gebeurtenis en wijzigt de status van het apparaat in de Kaspersky Security Center-console.

- Melden

  In deze modus staat Systeemintegriteitscontrole acties toe met bestanden en registersleutels uit het bewakingsbereik. Als de actie met bestanden of het register is verboden, genereert het programma een gebeurtenis: *De verboden bewerking was toegestaan in testmodus*. Om te analyseren hoe regels het systeem beïnvloeden, kunt u kijken naar: rapporten.

Realtime systeemintegriteitscontrole inschakelen

Realtime systeemintegriteitscontrole inschakelen in de beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Security Controls** → **Systeemintegriteitscontrole** in het beleidsvenster.
4. Selecteer het selectievakje **Systeemintegriteitscontrole**.
5. Onder **Uitvoermodus voor het blokkeren van regels**, selecteer een modus voor Realtime systeemintegriteitscontrole:
   - **Blokkeren**. In deze modus blokkeert Systeemintegriteitscontrole acties met bestanden en registersleutels uit het bewakingsbereik en genereert het een overeenkomstige gebeurtenis.
   - **Melden**. In deze modus staat Systeemintegriteitscontrole acties toe met bestanden en registersleutels uit het bewakingsbereik en genereert het een overeenkomstige gebeurtenis.
6. Schakel in het blok **Realtime systeemintegriteitscontrole** het selectievakje **Realtime systeemintegriteitscontrole** in.

7. Externe apparaatbewaking configureren:

   a. Selecteer het selectievakje **Apparaten bewaken**.

   b. In de **Ernstniveau van gebeurtenis** vervolgkeuzelijst, selecteer het belangniveau van externe apparaatbewakingsgebeurtenissen: *Informatief*, *Waarschuwing*, *Kritiek*.

   Systeemintegriteitscontrole registreert de huidige verbinding van externe apparaten. Het programma begint het aansluiten en loskoppelen van externe apparaten te controleren nadat het onderdeel is ingeschakeld in de programma-instellingen. Vervolgens, wanneer een extern apparaat wordt aangesloten of losgekoppeld, genereert het programma een overeenkomstige gebeurtenis.

8. Bestands- en registerbewaking configureren:

   a. Selecteer het selectievakje **Bewaak bestanden en het register**.

   b. Klik op **Instellingen**.

   Dit opent de lijst met regels voor Systeemintegriteitscontrole.

   c. Klik op **Toevoegen**.

   U kunt ook regels importeren uit een andere bron.

   d. Configureer de regel voor systeemintegriteitscontrole (zie onderstaande tabel).

9. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Realtime systeemintegriteitscontrole inschakelen in de Webconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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** → **System Integrity Monitoring**.

5. Zet de schakelaar **System Integrity Monitoring ENABLED** aan.

6. Selecteer het tabblad **Windows**.

7. Onder **Real-Time System Integrity Monitoring**, selecteer een modus voor Realtime systeemintegriteitscontrole:

   - **Apply rules**. In deze modus blokkeert Systeemintegriteitscontrole acties met bestanden en registersleutels uit het bewakingsbereik en genereert het een overeenkomstige gebeurtenis.

   - **Test rules (Inform)**. In deze modus staat Systeemintegriteitscontrole acties toe met bestanden en registersleutels uit het bewakingsbereik en genereert het een overeenkomstige gebeurtenis.

8. Bestands- en registerbewaking configureren:

    a. Selecteer het selectievakje **Monitor files and the registry**.

    b. Klik op **Rules**.

    Dit opent de lijst met regels voor Systeemintegriteitscontrole.

    c. Klik op **Add**.

    U kunt ook regels importeren uit een andere bron.

    d. Configureer de regel voor systeemintegriteitscontrole (zie onderstaande tabel).

9. Externe apparaatbewaking configureren:

    a. Selecteer het selectievakje **Monitor devices**.

    b. In de **Event severity level** vervolgkeuzelijst, selecteer het belangniveau van externe apparaatbewakingsgebeurtenissen: *Informational*, *Warning*, *Critical*.

    Systeemintegriteitscontrole registreert de huidige verbinding van externe apparaten. Het programma begint het aansluiten en loskoppelen van externe apparaten te controleren nadat het onderdeel is ingeschakeld in de programma-instellingen. Vervolgens, wanneer een extern apparaat wordt aangesloten of losgekoppeld, genereert het programma een overeenkomstige gebeurtenis.

10. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Hoe Realtime systeemintegriteitscontrole in de interface van het programma in te schakelen?

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

2. Selecteer **Security Controls** → **Systeemintegriteitscontrole** in het venster met de programma-instellingen.

3. Zet de schakelaar **Systeemintegriteitscontrole** aan.

4. Onder **Uitvoermodus voor het blokkeren van regels**, selecteer een modus voor Realtime systeemintegriteitscontrole:

    - **Blokkeren**. In deze modus blokkeert Systeemintegriteitscontrole acties met bestanden en registersleutels uit het bewakingsbereik en genereert het een overeenkomstige gebeurtenis.

    - **Melden**. In deze modus staat Systeemintegriteitscontrole acties toe met bestanden en registersleutels uit het bewakingsbereik en genereert het een overeenkomstige gebeurtenis.

5. Schakel in het blok **Realtime Systeemintegriteitscontrole** het selectievakje **Realtime Systeemintegriteitscontrole** in.

6. Externe apparaatbewaking configureren:

    a. Selecteer het selectievakje **Bewaak apparaten**.

    b. In de **Ernstniveau van gebeurtenis** vervolgkeuzelijst, selecteer het belangniveau van externe apparaatbewakingsgebeurtenissen: *Informatief*, *Waarschuwing*, *Essentieel*.

Systeemintegriteitscontrole registreert de huidige verbinding van externe apparaten. Het programma begint het aansluiten en loskoppelen van externe apparaten te controleren nadat het onderdeel is ingeschakeld in de programma-instellingen. Vervolgens, wanneer een extern apparaat wordt aangesloten of losgekoppeld, genereert het programma een overeenkomstige gebeurtenis.

7. Bestands- en registerbewaking configureren:

   a. Selecteer het selectievakje **Bewaak bestanden en het register**.

   b. Klik op **Configureren**.

      Dit opent de lijst met regels voor Systeemintegriteitscontrole.

   c. Klik op **Toevoegen**.

      U kunt ook regels importeren uit een andere bron.

8. Configureer de regel voor systeemintegriteitscontrole (zie onderstaande tabel).

9. Sla uw wijzigingen op.

Realtime systeemintegriteitscontrole regelinstellingen

Parameter	Beschrijving
Regelnaam	Naam van de regel voor Realtime systeemintegriteitscontrole
Bewerkingen met bestanden en register	• **Toestaan**. Systeemintegriteitscontrole staat acties toe met bestanden en registersleutels uit de bewakingsbereik. • **Blokkeren**. Het gedrag van Systeemintegriteitscontrole hangt af van de geselecteerde modus. Als je de hebt geselecteerd *Systeembeveiligingsmodus*, Systeemintegriteitscontrole blokkeert acties met bestanden en registersleutels uit het bewakingsbereik, genereert een overeenkomstige gebeurtenis en wijzigt de status van het apparaat in de Kaspersky Security Center-console. Als je de hebt geselecteerd *Testmodus*, Systeemintegriteitscontrole staat acties toe met bestanden en registersleutels uit de bewakingsbereik.

Parameter	Beschrijving
Ernstniveau van gebeurtenis	Kaspersky Endpoint Security logt bestandswijzigingen wanneer een bestand of registersleutel in het bewakingsbereik wordt gewijzigd. De volgende ernstniveaus zijn beschikbaar voor gebeurtenissen: *Informatief*, *Waarschuwing*, *Essentieel*.

Bereik van bewaking	• **Bestand**. Lijst met bestanden en mappen die door het onderdeel worden bewaakt. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de `*` en `?`-tekens bij het invoeren van een masker. 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:\Folder\**\*.txt` omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen bevinden genest in de `Folder`, uitgezonderd de `Folder` 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:\Folder\???.txt` omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam `Folder` bevinden, die een TXT-extensie hebben en die een naam met drie tekens hebben.
	• **Register**. Lijst met registersleutels en -waarden die door het onderdeel worden bewaakt. Kaspersky Endpoint Security biedt geen ondersteuning voor de tekens `*` en `?` bij de invoer van een masker.

Uitzonderingen	• **Bestand**. Lijst van uitzonderingen van het bewakingsbereik. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de `*` en `?`-tekens bij het invoeren van een masker. Bijvoorbeeld `C:\Folder\Application\*.log`. Uitzonderingen hebben een hogere prioriteit dan bewakingsbereik. 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:\Folder\**\*.txt` omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen bevinden genest in de `Folder`, uitgezonderd de `Folder` 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:\Folder\???.txt` omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam `Folder` bevinden, die een TXT-extensie hebben en die een naam met drie tekens hebben.
	• **Register**. Lijst van uitzonderingen van het bewakingsbereik. Kaspersky Endpoint Security biedt geen ondersteuning voor de tekens `*` en `?` bij de invoer van een masker. Uitzonderingen hebben een hogere prioriteit dan bewakingsbereik.

Vertrouwde gebruikers en/of gebruikersgroepen	Een *vertrouwde gebruiker* is een gebruiker die acties mag uitvoeren met bestanden en registersleutels in de bewakingsbereik. Als Kaspersky Endpoint Security een actie detecteert die is uitgevoerd door een vertrouwde gebruiker, genereert Systeemintegriteitscontrole een *Informatief* evenement. U kunt gebruikers selecteren in Active Directory, in de lijst van accounts in Kaspersky Security Center, of door handmatig een lokale gebruikersnaam in te voeren. Kaspersky raadt aan om locale gebruikersaccounts alleen in speciale gevallen te gebruiken, wanneer het niet mogelijk is om domeingebruikersaccounts te gebruiken.
Markeringen voor bestandsbewerkingen / Bewaakte operaties	Markeringen die de actie karakteriseren met bestanden of registersleutels die het onderdeel zal controleren.
Hashing	Het berekenen van een bestandshash bij wijziging. Kaspersky Endpoint Security voegt informatie toe over de hash van het bestand wanneer een gebeurtenis wordt gegenereerd.

On-demand systeemintegriteitscontrole

On-demand systeemintegriteitscontrole is een taak die u handmatig of volgens een schema kunt uitvoeren. Bij het uitvoeren van de *Systeemintegriteitscheck* taak vergelijkt het programma de huidige staat van de objecten die zijn opgenomen in de bewakingsbereik met hun *basislijn* staat. In tegenstelling tot Realtime systeemintegriteitscontrole, *Systeemintegriteitscheck* taak helpt het aantal gebeurtenissen te beperken en stelt u in staat een algemeen rapport van wijzigingen in het besturingssysteem te genereren.

Om Systeemintegriteitscontrole te laten werken, moet u minimaal één regel toevoegen. een *Regel voor Systeemintegriteitscontrole* is een set criteria die de toegang van gebruikers tot bestanden en het register definiëren. Systeemintegriteitscontrole detecteert wijzigingen in de bestanden en het register binnen de opgegeven *bewakingsbereik*. Het bereik van de controle is een van de criteria van een regel voor Systeemintegriteitscontrole. U kunt regels configureren die worden gedeeld door Realtime systeemintegriteitscontrole en de *Systeemintegriteitscheck* taak of maak afzonderlijke regels voor de taak. Om een Basislijn te maken, past Kaspersky Endpoint Security het bewakingsbereik toe vanaf de *Systeemintegriteitscheck* taak aan de *Baseline update* taak.

Een basislijn maken en bijwerken

De *Systeemintegriteitscheck* taak heeft een basislijn nodig om te werken. Een *basislijn* is een geregistreerde staat van objecten in het systeem, die het programma als referentie gebruikt bij het vergelijken met de huidige staat. Als de huidige status van het systeem afwijkt van de status van het systeem zoals vastgelegd in de basislijn, genereert Kaspersky Endpoint Security de bijbehorende gebeurtenis. U kunt een basislijn maken of bijwerken met behulp van de *Baseline update* taak.

U kunt de basislijn bijwerken in de volgende modi:

- Volledige update.

  Het programma werkt alle objecten in het bewakingsbereik bij.

- Incrementele update.

  Het programma detecteert en actualiseert alleen gewijzigde of nieuwe objecten.

Een basislijn maken of bijwerken in de Beheerconsole (MMC)

1. Selecteer **Tasks** in de structuur van de Beheerconsole van Kaspersky Security Center.

   De lijst met taken wordt geopend.

2. Klik op **New task**.

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

Stap 1. Een taaktype selecteren

Selecteer **Kaspersky Endpoint Security voor Windows 14.1. → Baseline update**.

Stap 2. De basislijn-updatemodus selecteren

Selecteer een basislijn-updatemodus:

- **Volledige update**. Het programma werkt alle objecten in het bewakingsbereik bij.
- **Incrementele update**. Het programma detecteert en actualiseert alleen gewijzigde of nieuwe objecten.

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 *Basislijn 2024*.

Stap 5. Aanmaak van de taak voltooien

Verlaat de wizard verlaten. Schakel indien nodig het selectievakje **Run the task after the wizard finishes** in. U kunt de voortgang van de taak volgen in de taakeigenschappen.

Een basislijn maken of bijwerken in de Webconsole

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

   De lijst met taken wordt geopend.

2. Klik op **Add**.

   De wizard Taak wordt gestart.

3. Configureer de taakinstellingen:

   a. Selecteer in de vervolgkeuzelijst **Application** de optie **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. Selecteer in de vervolgkeuzelijst **Task type** de optie **Baseline update**.

c. Typ in het veld **Task name** een korte omschrijving, zoals *Basislijn 2024*.

d. Selecteer in het gedeelte **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. Ga naar de volgende stap.
5. Selecteer een account om de taak uit te voeren. Kaspersky Endpoint Security start de taak standaard met de rechten van een lokaal gebruikersaccount.
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. Selecteer een basislijn-updatemodus:
   - **Full update**. Het programma werkt alle objecten in het bewakingsbereik bij.
   - **Incremental update**. Het programma detecteert en actualiseert alleen gewijzigde of nieuwe objecten.
10. Sla uw wijzigingen op.
11. Schakel het selectievakje naast de taak in.
12. Klik op **Start**.

Het bewakingsbereik configureren voor de Systeemintegriteitscheck taak

Standaard is het bewakingsbereik van de *Systeemintegriteitscheck* taak hetzelfde als het bewakingsbereik van Realtime systeemintegriteitscontrole. U kunt een ander bewakingsbereik voor de taak configureren.

> Systeemintegriteitscontrole biedt geen ondersteuning voor het importeren van de sleutels `HKEY_CURRENT_USER` en `HKEY_CURRENT_CONFIG` voor de *Systeemintegriteitscheck*-taak. Als het bewakingsbereik van de taak deze sleutels bevat, maakt het programma de gebeurtenis *Bereik van bewaking bevat onjuiste objecten* aan.

Een ander bewakingsbereik configureren voor de Systeemintegriteitscheck taak in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Security Controls** → **Systeemintegriteitscontrole** in het beleidsvenster.
4. Selecteer het selectievakje **Systeemintegriteitscontrole**.
5. Onder **Systeemintegriteitscheck**, selecteer de modus taakconfiguratie: **Aangepaste instellingen**.

6. Externe apparaatbewaking configureren:

   a. Selecteer het selectievakje **Apparaten bewaken**.

   b. In de **Ernstniveau van gebeurtenis** vervolgkeuzelijst, selecteer het belangniveau van externe apparaatbewakingsgebeurtenissen: *Informatief* ⓘ, *Waarschuwing* ⚠, *Kritiek* ⓘ.

   Systeemintegriteitscontrole registreert informatie over aangesloten externe apparaten op het moment dat de basislijn wordt gemaakt. Wanneer vervolgens een extern apparaat wordt aangesloten, genereert het programma een overeenkomstige gebeurtenis. Bij het uitvoeren van de *Systeemintegriteitscheck* taak, controleert het programma het loskoppelen van externe apparaten niet.

7. Bestands- en registerbewaking configureren:

   a. Selecteer het selectievakje **Bewaak bestanden en het register**.

   b. Klik op **Instellingen**.

   Dit opent de lijst met regels voor Systeemintegriteitscontrole.

   c. Klik op **Toevoegen**.

   U kunt ook regels importeren uit een andere bron.

   d. Configureer de regel voor systeemintegriteitscontrole (zie onderstaande tabel).

8. Sla uw wijzigingen op.

Een ander bewakingsbereik configureren voor de System Integrity Check taak in de Webconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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** → **System Integrity Monitoring**.

5. Selecteer het tabblad **Windows**.

6. Zet de schakelaar **System Integrity Monitoring ENABLED** aan.

7. Onder **System Integrity Check**, selecteer de modus taakconfiguratie: **Custom settings**.

8. Externe apparaatbewaking configureren:

   a. Selecteer het selectievakje **Monitor devices**.

   b. In de **Event severity level** vervolgkeuzelijst, selecteer het belangniveau van externe apparaatbewakingsgebeurtenissen: *Informational* ⓘ, *Warning* ⚠, *Critical* ⓘ.

   Systeemintegriteitscontrole registreert informatie over aangesloten externe apparaten op het moment dat de basislijn wordt gemaakt. Wanneer vervolgens een extern apparaat wordt aangesloten, genereert het programma een overeenkomstige gebeurtenis. Bij het uitvoeren van de *Systeemintegriteitscheck* taak, controleert het programma het loskoppelen van externe apparaten niet.

9. Bestands- en registerbewaking configureren:

    a. Selecteer het selectievakje **Monitor files and the registry**.

    b. Klik op **Rules**.

    Dit opent de lijst met regels voor Systeemintegriteitscontrole.

    c. Klik op **Add**.

    U kunt ook regels importeren uit een andere bron.

    d. Configureer de regel voor systeemintegriteitscontrole (zie onderstaande tabel).

10. Sla uw wijzigingen op.

Een ander bewakingsbereik configureren voor de Systeemintegriteitscheck taak in het programma-interface

1. Klik in het hoofdvenster van het programma op de knop ⚙.
2. Selecteer **Security Controls** → **Systeemintegriteitscontrole** in het venster met de programma-instellingen.
3. Zet de schakelaar **Systeemintegriteitscontrole** aan.
4. Onder **Systeemintegriteitscheck**, selecteer de modus taakconfiguratie: **Aangepaste instellingen**.
5. Externe apparaatbewaking configureren:

    a. Selecteer het selectievakje **Bewaak apparaten**.

    b. In de **Ernstniveau van gebeurtenis** vervolgkeuzelijst, selecteer het belangniveau van externe apparaatbewakingsgebeurtenissen: *Informatief* ⓘ, *Waarschuwing* ⚠, *Essentieel* ⓘ.

    Systeemintegriteitscontrole registreert informatie over aangesloten externe apparaten op het moment dat de basislijn wordt gemaakt. Wanneer vervolgens een extern apparaat wordt aangesloten, genereert het programma een overeenkomstige gebeurtenis. Bij het uitvoeren van de *Systeemintegriteitscheck* taak, controleert het programma het loskoppelen van externe apparaten niet.

6. Bestands- en registerbewaking configureren:

    a. Selecteer het selectievakje **Bewaak bestanden en het register**.

    b. Klik op **Configureren**.

    Dit opent de lijst met regels voor Systeemintegriteitscontrole.

    c. Klik op **Toevoegen**.

    U kunt ook regels importeren uit een andere bron.

    d. Configureer de regel voor systeemintegriteitscontrole (zie onderstaande tabel).

7. Sla uw wijzigingen op.

Instellingen van a Systeemintegriteitscheck taakregel

Parameter	Beschrijving
Regelnaam	Naam van de *Systeemintegriteitscheck* taakregel.
Ernstniveau van gebeurtenis	Kaspersky Endpoint Security logt bestandswijzigingen wanneer een bestand of registersleutel in het bewakingsbereik wordt gewijzigd. De volgende ernstniveaus zijn beschikbaar voor gebeurtenissen: *Informatief*, *Waarschuwing*, *Essentieel*.

Bereik van bewaking	• **Bestand**. Lijst met bestanden en mappen die door het onderdeel worden bewaakt. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de `*` en `?`-tekens bij het invoeren van een masker.
	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:\Folder\**\*.txt` omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen bevinden genest in de `Folder`, uitgezonderd de `Folder` 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:\Folder\???.txt` omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam `Folder` bevinden, die een TXT-extensie hebben en die een naam met drie tekens hebben.
	• **Register**. Lijst met registersleutels en -waarden die door het onderdeel worden bewaakt. Kaspersky Endpoint Security biedt geen ondersteuning voor de tekens `*` en `?` bij de invoer van een masker.

Uitzonderingen	• **Bestand**. Lijst van uitzonderingen van het bewakingsbereik. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de `*` en `?`-tekens bij het invoeren van een masker. Bijvoorbeeld `C:\Folder\Application\*.log`. Uitzonderingen hebben een hogere prioriteit dan bewakingsbereik.
	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:\Folder\**\*.txt` omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen bevinden genest in de `Folder`, uitgezonderd de `Folder` 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:\Folder\???.txt` omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam `Folder` bevinden, die een TXT-extensie hebben en die een naam met drie tekens hebben.
	• **Register**. Lijst van uitzonderingen van het bewakingsbereik. Kaspersky Endpoint Security biedt geen ondersteuning voor de tekens `*` en `?` bij de invoer van een masker. Uitzonderingen hebben een hogere prioriteit dan bewakingsbereik.

Uitvoeren van de taak Systeemintegriteitscheck

De *Systeemintegriteitscheck* taak maakt het mogelijk om bestanden of registersleutels te controleren op wijzigingen en ook om de verbinding van externe apparaten te controleren. Om bestanden op wijzigingen te controleren, kunt u de *Systeemintegriteitscheck* taak in de volgende modi uitvoeren:

- Snelle scan.

  Bij het controleren van bestanden op wijzigingen, controleert het programma alleen bestandskenmerken. Het programma controleert de inhoud van bestanden niet.

- Volledige Scan.

  Bij het controleren van bestanden op wijzigingen controleert het programma alle bestandskenmerken en de inhoud van bestanden.

De modus waarin de taak wordt uitgevoerd, heeft geen invloed op de controle van het register of externe apparaten.

Systeemintegriteitscheck uitvoeren in de beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de beheerconsole **Tasks**.

   De lijst met taken wordt geopend.
3. Klik op **New task**.

   De wizard Taak wordt gestart. Volg de instructies van de wizard.
4. Selecteer **Kaspersky Endpoint Security → Baseline systeemintegriteitsmonitor**. Selecteer een modus voor Systeemintegriteitscontrole:

   - **Volledige Scan**. In deze modus controleert het programma alle kenmerken en hashes van bestanden.
   - **Snelle Scan**. In deze modus, controleert het programma alleen bestandskenmerken.
5. Selecteer de computers waarop de taak wordt uitgevoerd. De volgende opties zijn beschikbaar:

   - 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.
   - Geef de selectie van apparaten op waarvoor u de taak wilt uitvoeren.
   - Wijs de taak aan een beheergroep toe. In dit geval wordt de taak toegewezen aan computers uit een eerder gemaakte beheergroep.
6. Selecteer een account om de taak uit te voeren. Kaspersky Endpoint Security start de taak standaard met de rechten van een lokaal gebruikersaccount.
7. Configureer een schema voor het starten van een taak, bijvoorbeeld handmatig of op een specifieke dag van de week.
8. Voer een naam voor de taak in.
9. Verlaat de wizard verlaten. Schakel indien nodig het selectievakje **Run the task after the wizard finishes** in. U kunt de voortgang van de taak volgen in de taakeigenschappen.

Een taak System Integrity Check uitvoeren in de Webconsole

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

   De lijst met taken wordt geopend.
2. Klik op **Add**.

   De wizard Taak wordt gestart.

3. Configureer de taakinstellingen:

    a. Selecteer in de vervolgkeuzelijst **Application** de optie **Kaspersky Endpoint Security for Windows 14.1.0**.

    b. Selecteer in de vervolgkeuzelijst **Task type** de optie **System Integrity Check**.

    c. Typ in het veld **Task name** een korte omschrijving, zoals *Wekelijkse Systeemintegriteitscheck*.

    d. Selecteer in het gedeelte **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. Ga naar de volgende stap.

5. Selecteer een account om de taak uit te voeren. Kaspersky Endpoint Security start de taak standaard met de rechten van een lokaal gebruikersaccount.

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. Selecteer een modus voor Systeemintegriteitscheck:

    - **Quick Scan**. Het programma controleert alleen bestandskenmerken. Het programma controleert de inhoud van bestanden niet.

    - **Full Scan**. Het programma controleert alle bestandskenmerken van bestanden en hun inhoud.

10. Sla uw wijzigingen op.

11. Schakel het selectievakje naast de taak in.

12. Klik op **Start**.

Voor de *Systeemintegriteitscheck* taak succesvol af te ronden, de bewakingsbereik van de *Systeemintegriteitscheck* taak moet volledig overeenkomen met de basislijn. Als het bewakingsbereik anders is, eindigt de taak met een fout. Om bewakingsbereiken te synchroniseren, voert u de *Baseline update* taak met een nieuw bewakingsbereik.

Regels voor Systeemintegriteitscontrole exporteren en importeren

U kunt de lijst met regels voor Systeemintegriteitscontrole exporteren naar een XML-bestand. Vervolgens kunt u het bestand aanpassen om bijvoorbeeld een groot aantal records 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 Systeemintegriteitscontrole of om de lijst naar een andere server te migreren.

Systeemintegriteitscontrole biedt geen ondersteuning voor het importeren van de sleutels `HKEY_CURRENT_USER` en `HKEY_CURRENT_CONFIG` voor de *Systeemintegriteitscheck*-taak. Als het bewakingsbereik van de taak deze sleutels bevat, maakt het programma de gebeurtenis *Bereik van bewaking bevat onjuiste objecten* aan.

Een lijst met regels voor Systeemintegriteitscontrole exporteren en importeren in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Security Controls** → **Systeemintegriteitscontrole** in het beleidsvenster.
4. Exporteren of importeren *Realtime systeemintegriteitscontrole* regels:
   a. In het blok **Realtime systeemintegriteitscontrole**, klikt u op de knop **Instellingen**.
   b. Een lijst met regels voor Realtime systeemintegriteitscontrole exporteren:
      1. 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.
      2. Klik op de koppeling **Exporteren**.
      3. 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.
      4. Sla het bestand op.

         Kaspersky Endpoint Security exporteert de lijst met regels naar het XML-bestand.
   c. Een lijst met regels voor Realtime systeemintegriteitscontrole importeren:
      1. Klik op de koppeling **Importeren**.

         Selecteer in het geopende venster het XML-bestand waaruit u de lijst met regels wilt importeren.
      2. 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.

5. Exporteren of importeren *Systeemintegriteitscheck* regels:

   a. Selecteer in het blok **Systeemintegriteitscheck Aangepaste instellingen**.

   b. Klik op **Instellingen**.

   c. De lijst met regels voor Systeemintegriteitscheck exporteren:

      1. 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.

      2. Klik op de koppeling **Exporteren**.

      3. 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.

      4. Sla het bestand op.

      Kaspersky Endpoint Security exporteert de lijst met regels naar het XML-bestand.

   d. Een lijst met regels voor Systeemintegriteitscheck importeren:

      1. Klik op de koppeling **Importeren**.

         Selecteer in het geopende venster het XML-bestand waaruit u de lijst met regels wilt importeren.

      2. 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.

6. Sla uw wijzigingen op.

Een lijst met regels voor Systeemintegriteitscontrole exporteren en importeren in de Webconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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** → **System Integrity Monitoring**.

5. Selecteer het tabblad **Windows**.

6. Exporteren of importeren *Realtime systeemintegriteitscontrole* regels:

   a. Klik in het blok **Real-Time System Integrity Monitoring** op de koppeling **Rules**.

   b. Een lijst met regels voor Realtime systeemintegriteitscontrole exporteren:

      1. Selecteer de regels die u wilt exporteren.

      2. Klik op de knop → **Export**.

         Kaspersky Endpoint Security exporteert de lijst met regels naar een JSON-bestand in de standaard downloadmap.

   c. Een lijst met regels voor Realtime systeemintegriteitscontrole importeren:

      1. Klik op de knop → **Import**.

         Selecteer in het geopende venster het JSON-bestand waaruit u de lijst met vertrouwde adressen wilt importeren.

      2. 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 JSON-bestand.

7. Exporteren of importeren *Systeemintegriteitscheck* regels:

   a. Selecteer in het blok **On-Demand System Integrity Check Custom settings**.

   b. Klik op de koppeling **Rules**.

   c. De lijst met regels voor Systeemintegriteitscheck exporteren:

      1. Selecteer de regels die u wilt exporteren.

      2. Klik op de knop → **Export**.

         Kaspersky Endpoint Security exporteert de lijst met regels naar een JSON-bestand in de standaard downloadmap.

   d. Een lijst met regels voor Systeemintegriteitscheck importeren:

      1. Klik op de knop → **Import**.

         Selecteer in het geopende venster het JSON-bestand waaruit u de lijst met vertrouwde adressen wilt importeren.

      2. 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 JSON-bestand.

8. Sla uw wijzigingen op.

Rapporten over Systeemintegriteitscontrole bekijken

Om de prestaties van regels voor systeemintegriteitscontrole te analyseren, kunt u rapporten en gebeurtenissen bekijken die door het programma zijn gegenereerd. Kaspersky Endpoint Security genereert de volgende rapporten over het onderdeel:

- In het programma-interface:
  - Het rapport Systeemintegriteitscontrole
  - Het rapport Systeemintegriteitscheck
  - Het Basislijn-updaterapport

  De rapporten Systeemintegriteitscontrole-gebeurtenissen.
- In de Kaspersky Security Center-console:
  - Rapport over computers waarop controleregels het vaakst zijn geactiveerd
  - Rapporteren over de meest geactiveerde controleregels

  Standaard wordt er een rapport gemaakt voor de afgelopen 30 dagen, inclusief de datum waarop het rapport is gemaakt.

  Rapporten van Systeemintegriteitscontrole bekijken in de Beheerconsole (MMC)

  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 **New report template**.

     De wizard Nieuwe rapportsjabloon wordt gestart.
  4. Volg de instructies van de wizard Sjabloon voor rapport. Bij de **Selecting the report template type** stap, selecteer het rapport Systeemintegriteitscontrole (de **Other** sectie):
     - **Top 10 devices with File Integrity Monitor / System Integrity Monitoring rules most frequently triggered**.
     - **Top 10 rules of File Integrity Monitor / System Integrity Monitoring that were triggered on devices most frequently**.

     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.

Rapporten over systeemintegriteitscontrole bekijken in de Webconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Monitoring** → **Reports**.
2. Klik op **Add**.

   De wizard Nieuwe rapportsjabloon wordt gestart.
3. Onder **Template type**, in het gedeelte **Other**, selecteer een rapport Systeemintegriteitsconrole:

   - **Top 10 devices with File Integrity Monitor / System Integrity monitoring rules most frequently triggered**.
   - **Top 10 rules of File Integrity Monitor / System Integrity Monitoring that were triggered on devices most frequently**.

   Wanneer u de wizard Nieuwe rapportsjabloon hebt voltooid, verschijnt de nieuwe rapportsjabloon in de tabel.
4. Selecteer en voer het rapport uit.

Het rapport wordt gemaakt. Het rapport wordt in een nieuw venster weergegeven.

Om gebeurtenissen te bekijken die door het programma zijn gegenereerd, kunt u ook gebeurtenisselecties gebruiken in de Kaspersky Security Center-console.

Reset status van Systeemintegriteit

Computers in de Kaspersky Security Center-console hebben een van de volgende statussen: *OK*🖥️, *Warning*🖥️, of *Critical*🖥️. Als Systeemintegriteitscontrole wijziging van bestanden of registersleutels in het bewakingsbereik detecteert, verandert de status van de computer in: *Warning* of *Critical*. De status die wordt toegewezen door Systeemintegriteitscontrole heet de *systeemintegriteitsstatus*. U kunt de systeemintegriteitsstatus resetten, bijvoorbeeld als analyse u ervan heeft overtuigd dat de gedetecteerde wijziging van objecten geen invloed heeft op de beveiliging van de computer.

De systeemintegriteitsstatus resetten in de Beheerconsole (MMC)

1. Selecteer **Tasks** in de structuur van de Beheerconsole van Kaspersky Security Center.

   De lijst met taken wordt geopend.
2. Klik op **New task**.

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

Stap 1. Een taaktype selecteren

Selecteer **Kaspersky Endpoint Security voor Windows 14.1.** → **Reset van de systeemintegriteitsstatus**.

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 het taakschema bijvoorbeeld handmatig.

Stap 4. Taaknaam definiëren

Voer de naam van de taak in, bijvoorbeeld *De status resetten na het wijzigen van de bewakingsbereik*.

Stap 5. Aanmaak van de taak voltooien

Verlaat de wizard verlaten. Schakel indien nodig het selectievakje **Run the task after the wizard finishes** in. U kunt de voortgang van de taak volgen in de taakeigenschappen.

De systeemintegriteitsstatus resetten in de Webconsole

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

   De lijst met taken wordt geopend.

2. Klik op **Add**.

   De wizard Taak wordt gestart.

3. Configureer de taakinstellingen:

   a. Selecteer in de vervolgkeuzelijst **Application** de optie **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. Selecteer in de vervolgkeuzelijst **Task type** de optie **System integrity status reset**.

   c. In de **Task name** voer een korte beschrijving in, bijvoorbeeld *De status resetten na het wijzigen van de bewakingsbereik*.

   d. Selecteer in het gedeelte **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. Ga naar de volgende stap.
5. Selecteer een account om de taak uit te voeren. Kaspersky Endpoint Security start de taak standaard met de rechten van een lokaal gebruikersaccount.
6. Verlaat de wizard verlaten.

   U ziet een nieuwe taak in de lijst met taken.
7. Schakel het selectievakje naast de taak in.
8. Klik op **Start**.

Als gevolg hiervan, als de status van de computer werd gewijzigd in: *Warning* of *Critical* vanwege Systeemintegriteitscontrole-gebeurtenissen wordt de status van de computer gereset naar: *OK*. Als de status van de computer ook is gewijzigd vanwege andere gebeurtenissen, blijft de status van de computer ongewijzigd.

Cloud Discovery

Cloud Discovery beheert gebruikerstoegang tot cloudservices. Cloudservices omvatten bijvoorbeeld Microsoft Teams, Salesforce en Microsoft Office 365. Cloudservices zijn gegroepeerd in categorieën, bijvoorbeeld *Bestandsdeling*, *Messengers*, *E-mail*. Kaspersky-experts updaten regelmatig de Cloud Discovery-categorieën en cloudservices die in de categorieën zijn ingedeeld. Kaspersky Endpoint Security updatet de reeks categorieën en cloudservices met de programmadatabases. Dit betekent dat Cloud Discovery het Kaspersky Security Network niet gebruikt voor het categoriseren van cloudservices.

Cloud Discovery biedt de volgende functionaliteit:

- Monitoren van het gebruik van cloudservices
- Gebruikerstoegang tot cloudservices blokkeren

Systeem vereisten

Cloud Discovery is beschikbaar als aan de volgende voorwaarden wordt voldaan:

- Het programma wordt geïnstalleerd op een computer met Windows voor werkstations.

  Het onderdeel is niet beschikbaar voor servers.
- Kaspersky Security Center versie 15.1 of hoger.

  Het onderdeel is niet beschikbaar in de Beheerconsole (MMC). U kunt Cloud Discovery configureren in Kaspersky Security Center Web Console en Kaspersky Security Center Cloud Console.
- Kaspersky Next-licentie.

Schakel de functie van het programma in die vereist is voor het onderdeel Cloud Discovery:

1. **Geëncrypte verbindingen scannen**. Dit is nodig voor het bewaken van HTTPS-verkeer. U kunt deze functie beheren in het gedeelte **Netwerkinstellingen**.

2. **Injecteer script in internetverkeer voor interactie met webpagina's**. Het script maakt de registratie van Cloud Discovery gebeurtenissen mogelijk. Het script biedt ook volledige blokkering van de toegang tot cloudservices. Zonder het script blokkeert het programma alleen de domeinen toegang van de cloudservices. U kunt deze functie beheren in het gedeelte **Netwerkinstellingen**.

U kunt ook de functie **Registreer het openen van toegestane pagina's** inschakelen. De functionaliteit bevat het groeperen van gebeurtenissen wanneer een gebruiker webpagina's bezoekt die tot hetzelfde domein behoren. Op deze manier registreert Cloud Discovery, wanneer een gebruiker een cloudservice gebruikt, slechts één gebeurtenis in plaats van meerdere gebeurtenissen voor elke webpagina. U kunt deze functie beheren in het gedeelte **Webcontrole**.

Monitoren van cloudservices

Wanneer een gebruiker een cloudservice begint te gebruiken, registreert Kaspersky Endpoint Security die gebeurtenis en maakt een item in het rapport. Cloud Discovery regelt het gebruik van cloudservices in de browser en in bijbehorende programma's. Cloud Discovery beheert het gebruik van cloudservices via HTTP en HTTPS.

Schakel monitoring van cloudservices in Cloud Console in

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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 **Communication & Web Protection** → **Cloud Discovery**.

5. Zet de schakelaar **Cloud Discovery ENABLED** aan.

6. Sla uw wijzigingen op.

Als resultaat stuurt het programma informatie over de gebruikte cloudservices door naar Kaspersky Security Center. U kunt gebruiksinformatie van de cloudservice bekijken in rapporten. Indien nodig kunt u de toegang tot cloudservices blokkeren.

Toegang tot cloudservices blokkeren

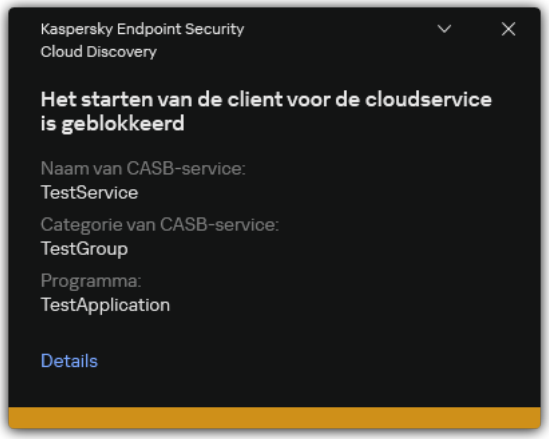
Het blokkeren van de toegang tot cloudservices is alleen beschikbaar voor de Kaspersky Next EDR Optimum-licentie en XDR Expert-licentie. Deze functie is niet beschikbaar voor de Kaspersky Next EDR Foundations-licentie. Vergelijking van de programmafunctionaliteit afhankelijk van het Kaspersky Next-licentietype, zie Kaspersky Next Help.

De beheerder kan de gebruikerstoegang beperken tot Cloud Discovery-categorieën of individuele cloudservices. Op deze manier kan de beheerder alleen veilige cloudservices toestaan en datalekken voorkomen. *Informatie over het risiconiveau* wordt voor elke cloudservice weergegeven in Cloud Discovery. Het risiconiveau helpt bij het detecteren van diensten die niet voldoen aan de beveiligingseisen van de organisatie.

Het risiconiveau is een schatting en impliceert geen uitspraken over de kwaliteit van de cloudservices of de leverancier ervan. Het risiconiveau is slechts een aanbeveling van Kaspersky-experts.

Risiconiveaus van cloudservices worden weergegeven in de sectie **Cloud Discovery** van het beleid in de lijst met alle gecontroleerde cloudservices.

Andere Kaspersky Endpoint Security-onderdelen bieden bescherming tegen bedreigingen en volgen verdachte gebruikersactiviteiten bij het gebruik van cloudservices.



Cloud Discovery melding

Cloud Discovery blokkeert geen cloudapplicaties die vóór Kaspersky Endpoint Security zijn gestart.

Blokkeer de toegang tot cloudservices in Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Communication & Web Protection** → **Cloud Discovery**.
5. Zet de schakelaar **Cloud Discovery ENABLED** aan.

   Een lijst met alle cloudservices wordt weergegeven. Cloudservices zijn gegroepeerd in categorieën, zoals *File sharing*, *Messengers*, *Email*. Kaspersky-experts updaten regelmatig de Cloud Discovery-categorieën en cloudservices die in de categorieën zijn ingedeeld. Kaspersky Endpoint Security updatet de reeks categorieën en cloudservices met de programmadatabases.
6. Gebruik de schakelaar in de **Access**-kolom om de toegang tot cloudservices te configureren.
7. Sla uw wijzigingen op.

Als resultaat regelt het programma het gebruik van de cloudservice in de browser en in de bijbehorende programma's.

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 uitzonderingen en vertrouwde programma's maken naast de algemene vertrouwde zone in een beleid.

Vanaf Kaspersky Endpoint Security 12.5 voor Windows kunt u EDR-telemetrie toevoegen aan de vertrouwde zone. Hierdoor kunnen de gegevens worden geoptimaliseerd die het programma naar de Telemetrieverzamelingsserver verzendt voor de Kaspersky Anti Targeted Attack Platform (EDR)-oplossing.

Beginnend met Kaspersky Endpoint Security 12.6 voor Windows, uitzonderingen scannen en vertrouwde programma's worden toegevoegd aan de vertrouwde zone. Vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's helpen bij het snel configureren van Kaspersky Endpoint Security op SQL-servers, Microsoft Exchange-servers en System Center Configuration Manager. Dit betekent dat u niet handmatig een vertrouwde zone voor het programma op servers hoeft in te stellen.

Vanaf Kaspersky Endpoint Security 12.8 voor Windows kun je het programma in Light Agent-modus installeren om virtuele omgevingen te beschermen. Met voorgedefinieerde uitzonderingen van scans en vertrouwde programma's kunt u Kaspersky Endpoint Security snel configureren in Citrix- en VMware-virtuele omgevingen.

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 een 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 inbrekers kunnen gebruiken om uw 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
- *Malware-scan*-taak

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.

Het wijzigen van de lijst met uitzonderingen voor scans wordt mogelijk geblokkeerd door de eigenschappen van het bovenliggende beleid. Om de lijst te wijzigen, moet u toestaan dat de instellingen van vertrouwde zone in de Webconsole (het "hangslot" moet ontgrendeld zijn).

Vertrouwde zones zijn verschillend gegroepeerd in de Beheerconsole (MMC) en de Webconsole. Ook de manier waarop wijziging in de parameters voor de vertrouwde zone worden voorkomen, verschilt (verschillende "hangsloten"). We raden aan dat u alleen de Webconsole gebruikt om het programma te beheren. Als u de vertrouwde zone in verschillende consoles configureert, kan de beheerplug-in het "hangslot" terugzetten naar de standaardstatus.

Een scanuitzondering maken in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Algemene instellingen** → **Uitzonderingen en objecttypen** in het beleidsvenster.
4. In het blok **Scanuitzonderingen en vertrouwde programma's** → **Scanuitzonderingen**, klikt u op de knop **Instellingen**.

   Met een klik op deze koppeling opent u een venster waarin u een lijst met uitzonderingen vindt.
5. Schakel het selectievakje **Waarden samenvoegen bij overname** 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.

6. Schakel het selectievakje **Gebruik van lokale uitzonderingen toestaan** 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. En, wanneer dit selectievakje uitgeschakeld is, verbergt Kaspersky Endpoint Security de geconsolideerde lijst met scanuitzonderingen in de gebruikersinterface van het programma.

7. Klik **Toevoegen** en selecteer een actie:

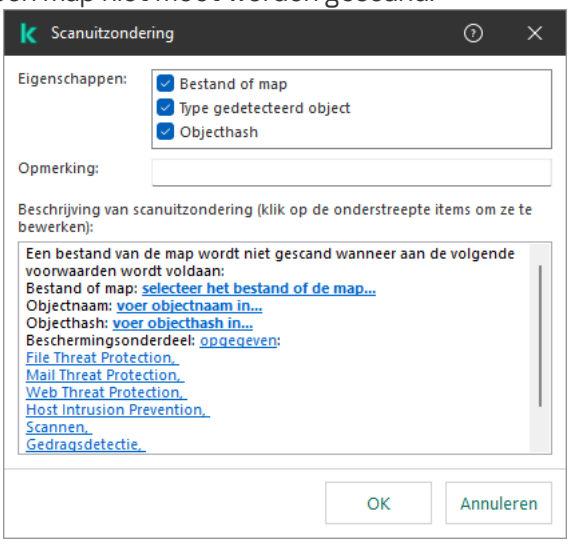
   - **Categorie**. U kunt scanuitzonderingen groeperen in afzonderlijke categorieën. Om een nieuwe categorie te maken, voer de naam van de categorie in en voeg ten minste één scanuitzonderingen toe aan de categorie.

   - **Nieuwe uitzondering**. Kaspersky Endpoint Security voegt een nieuwe scanuitzondering toe aan de hoofdmap van de lijst.

   - **Selecteer uitzonderingen uit lijst**. Om Kaspersky Endpoint Security snel te configureren op SQL-servers, Microsoft Exchange-servers en System Center Configuration Manager, bevat het programma: *vooraf gedefinieerde scanuitzonderingen*. Er zijn ook vooraf gedefinieerde scanuitzonderingen toegevoegd om de installatie van progromma's in virtuele Citrix- en VMware-omgevingen te ondersteunen. U moet vooraf gedefinieerde scanuitzonderingen selecteren, afhankelijk van het doel van de beveiligde server.

   - **Nieuwe uitzonderingen in geselecteerde categorie**. Als u een nieuwe scanuitzondering aan een specifieke categorie wilt toevoegen, selecteer een categorie.

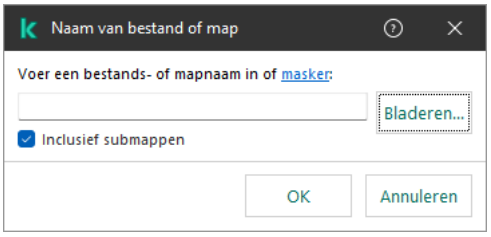
8. Zo stelt u in dat een bestand of een map niet moet worden gescand:



Instellingen voor uitzonderingen

a. Schakel in het blok **Eigenschappen** het selectievakje **Bestand of map** in.

b. Klik op de link in het onderstaande blok om het venster **Naam van bestand of map** te openen.



Bestand of map selecteren

a. 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:\Folder\**\*.txt` omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen bevinden genest in de `Folder`, uitgezonderd de `Folder` 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:\Folder\???.txt` omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam `Folder` bevinden, die een TXT-extensie hebben en die een naam met drie tekens hebben.

U kunt maskers gebruiken aan het begin, in het midden of aan het einde van het bestandspad. Als u bijvoorbeeld een map voor alle gebruikers aan uitzonderingen wilt toevoegen, voert u het masker `?:\Users\*\Folder\` in.

Kaspersky Endpoint Security ondersteunt omgevingsvariabelen

U kunt netwerkmappen uitsluiten. Voer hiervoor het pad naar de netwerkmap handmatig in (bijvoorbeeld, `\\Network Share\*`).

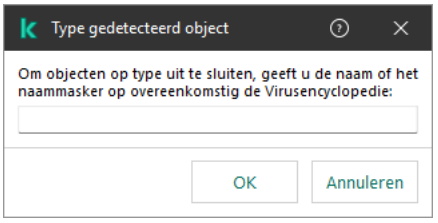
> Kaspersky Endpoint Security ondersteunt de omgevingsvariabele `%userprofile%` niet bij het genereren van een lijst met uitzonderingen op de Kaspersky Security Center-console. Om dit toe te passen op alle gebruikersaccounts, kunt u het teken `*` gebruiken (bijvoorbeeld, `C:\Users\*\Documents\File.exe`). Telkens wanneer u een nieuwe omgevingsvariabele toevoegt, moet u het programma opnieuw starten.

b. Sla uw wijzigingen op.

9. Zo stelt u in dat objecten met een specifieke naam niet moeten worden gescand:

a. Schakel in het blok **Eigenschappen** het selectievakje **Type gedetecteerd object** in.

b. Klik op de link in het onderstaande blok om het venster **Type gedetecteerd object** te openen.



Object selecteren

a. Voer de naam van het object 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.

b. Sla uw wijzigingen op.

10. Als u een afzonderlijk bestand van scans wilt uitsluiten:

    a. Schakel in het blok **Eigenschappen** het selectievakje **Objecthash** in.

    b. Klik op de link in het onderstaande blok om het venster **Objecthash** te openen.



Bestand selecteren

    a. Voer de bestandshash in of selecteer het bestand door op de knop **Bladeren** te klikken.

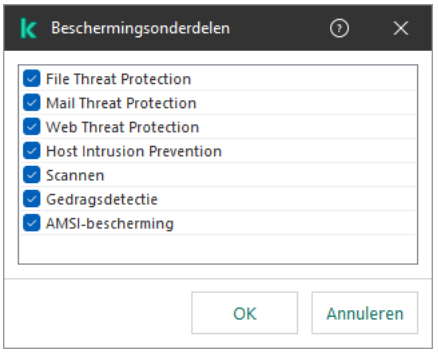
    Als het bestand is gewijzigd, wordt de bestandshash van het bestand ook gewijzigd. Als dit gebeurt, wordt het gewijzigde bestand niet toegevoegd aan uitzonderingen.

    b. Sla uw wijzigingen op.

11. Typ indien nodig in het veld **Opmerking** een korte opmerking over de scanuitzondering die u maakt.

12. Geef de onderdelen van Kaspersky Endpoint Security op die de scanuitzondering moeten gebruiken:

    a. Klik op de link in het onderstaande blok om het venster **Beschermingsonderdelen** te openen.



Beschermingsonderdelen selecteren

    a. Schakel de selectievakjes naast de onderdelen in die de scanuitzondering moeten gebruiken.

    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.

13. Klik op **OK**.

    De nieuwe uitzondering wordt aan de lijst toegevoegd. U kunt de uitzondering op elk moment uitschakelen met behulp van het selectievakje.

14. Sla uw wijzigingen op.

Een scanuitzondering maken in de webconsole en de cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 het gedeelte **Trusted Zone**.
5. Klik in het venster op de link **Malware 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 exclusions** 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. En, wanneer dit selectievakje uitgeschakeld is, verbergt Kaspersky Endpoint Security de geconsolideerde lijst met scanuitzonderingen in de gebruikersinterface van het programma.
8. Klik **Add** en selecteer een actie:

   - **Category**. U kunt scanuitzonderingen groeperen in afzonderlijke categorieën. Om een nieuwe categorie te maken, voer de naam van de categorie in en voeg ten minste één scanuitzonderingen toe aan de categorie.
   - **New exclusion**. Kaspersky Endpoint Security voegt een nieuwe scanuitzondering toe aan de hoofdmap van de lijst.
   - **Select exclusion from list**. Om Kaspersky Endpoint Security snel te configureren op SQL-servers, Microsoft Exchange-servers en System Center Configuration Manager, bevat het programma: *vooraf gedefinieerde scanuitzonderingen*. Er zijn ook vooraf gedefinieerde scanuitzonderingen toegevoegd om de installatie van progromma's in virtuele Citrix- en VMware-omgevingen te ondersteunen. U moet vooraf gedefinieerde scanuitzonderingen selecteren, afhankelijk van het doel van de beveiligde server.

   Om een nieuwe scanuitzonderingen aan een specifieke categorie toe te voegen, schakel het selectievakje naast die categorie in en selecteer de optie **New exclusion**.
9. Selecteer hoe u de uitzondering wil toevoegen: **Path to the file or folder**, **Object type** of **Object hash**.

10. Voer het pad handmatig in om een bestand of map uit te sluiten van de scan. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de `*` en `?`-tekens bij het invoeren 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:\Folder\**\*.txt` omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen bevinden genest in de `Folder`, uitgezonderd de `Folder` 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:\Folder\???.txt` omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam `Folder` bevinden, die een TXT-extensie hebben en die een naam met drie tekens hebben.

      U kunt maskers gebruiken aan het begin, in het midden of aan het einde van het bestandspad. Als u bijvoorbeeld een map voor alle gebruikers aan uitzonderingen wilt toevoegen, voert u het masker `?:\Users\*\Folder\` in.

      U kunt netwerkmappen uitsluiten. Voer hiervoor het pad naar de netwerkmap handmatig in (bijvoorbeeld, `\\Network Share\*`).

11. Als u een bepaald type object van scans wilt uitsluiten, voert u in het veld **Object type** 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 uitzonderingen.

13. Selecteer in het blok **Apply exclusion to** 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. Klik op **OK**.

    De nieuwe uitzondering wordt aan de lijst toegevoegd. U kunt de schakelaar gebruiken om een uitzondering op elk moment te stoppen.

16. Sla uw wijzigingen op.

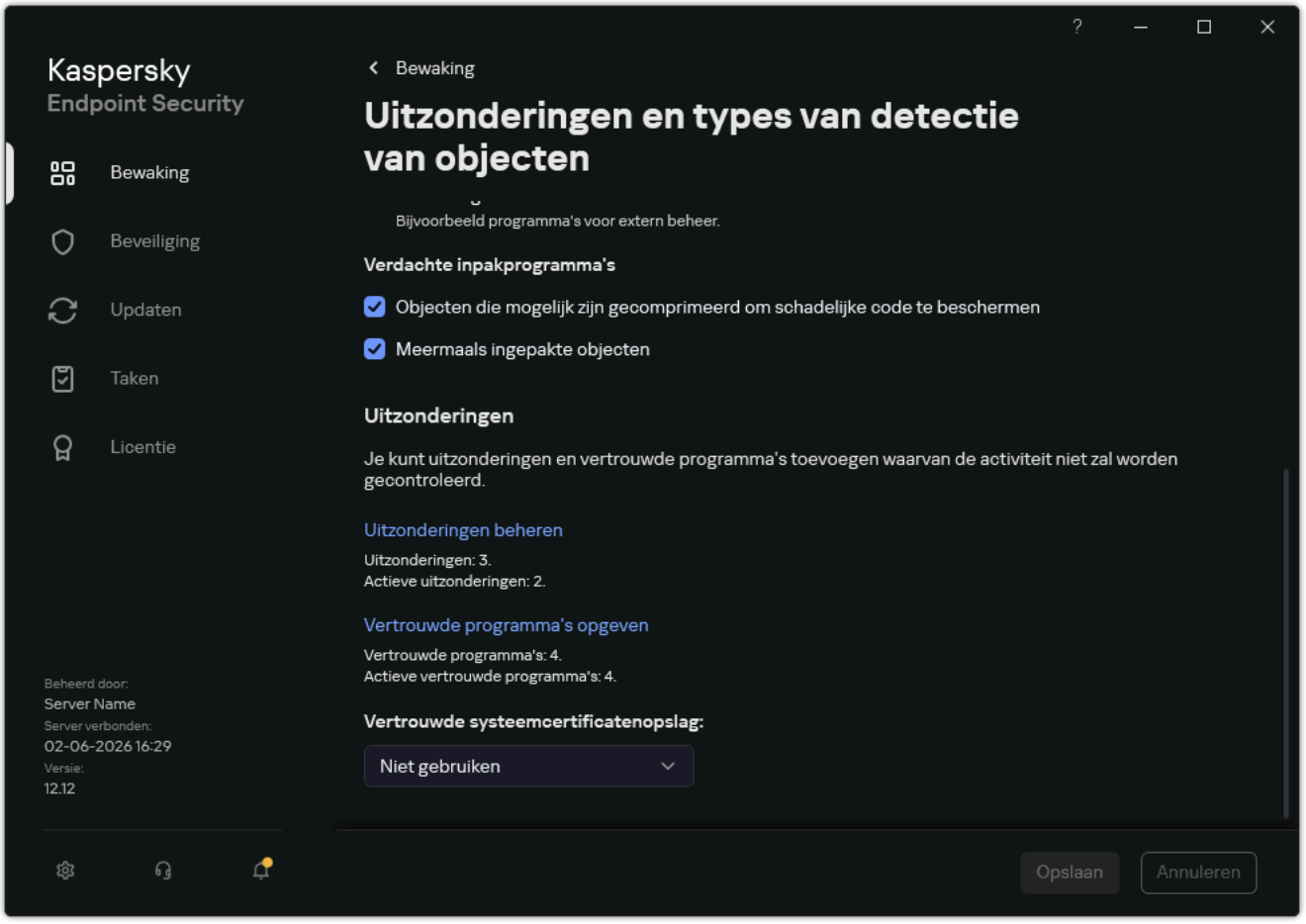
Een scanuitzondering maken in de programma-interface

1. Klik in het hoofdvenster van het programma op de knop ⚙.

2. Selecteer **Algemene instellingen → Uitzonderingen en types van detectie van objecten** in het venster met de programma-instellingen.

3. Klik in het blok **Uitzonderingen** op de koppeling **Uitzonderingen beheren**.

Kaspersky Endpoint Security verbergt de lijst met scanuitzonderingen in de gebruikersinterface van het programma als het instellen van scanuitzonderingen geblokkeerd is door de beheerder in de console ("gesloten slot"-symbool) en lokale scanuitzonderingen zijn verboden (het selectievakje **Gebruik van lokale uitzonderingen toestaan** is uitgeschakeld).



Instellingen van uitzonderingen

4. Klik **Toevoegen** en selecteer een actie:

   - **Categorie**. U kunt scanuitzonderingen groeperen in afzonderlijke categorieën. Om een nieuwe categorie te maken, voer de naam van de categorie in en voeg ten minste één scanuitzonderingen toe aan de categorie.

   - **Nieuwe uitzondering**. Kaspersky Endpoint Security voegt een nieuwe scanuitzondering toe aan de hoofdmap van de lijst.

   - **Selecteer uitzonderingen uit lijst**. Om Kaspersky Endpoint Security snel te configureren op SQL-servers, Microsoft Exchange-servers en System Center Configuration Manager, bevat het programma: *vooraf gedefinieerde scanuitzonderingen*. Er zijn ook vooraf gedefinieerde scanuitzonderingen toegevoegd om de installatie van progromma's in virtuele Citrix- en VMware-omgevingen te ondersteunen. U moet vooraf gedefinieerde scanuitzonderingen selecteren, afhankelijk van het doel van de beveiligde server.

   Om een nieuwe scanuitzonderingen aan een specifieke categorie toe te voegen, schakel het selectievakje naast die categorie in en selecteer de optie **Nieuwe uitzondering**.

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 verwijderen. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de `*` en `?`-tekens bij het invoeren 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:\Folder\**\*.txt` omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen bevinden genest in de `Folder`, uitgezonderd de `Folder` 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:\Folder\???.txt` omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam `Folder` bevinden, die een TXT-extensie hebben en die een naam met drie tekens hebben.

  U kunt maskers gebruiken aan het begin, in het midden of aan het einde van het bestandspad. Als u bijvoorbeeld een map voor alle gebruikers aan uitzonderingen wilt toevoegen, voert u het masker `?:\Users\*\Folder\` in.

  U kunt netwerkmappen uitsluiten. Voer hiervoor het pad naar de netwerkmap handmatig in (bijvoorbeeld, `\\Network Share\*`).

6. Als u een bepaald type object van scans wilt uitsluiten, voert u in het veld **Soorten gedetecteerde objecten** 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 uitzonderingen.

8. Selecteer in het blok **Beschermingsonderdelen** de componenten waarop u de scanuitzondering wilt toepassen.

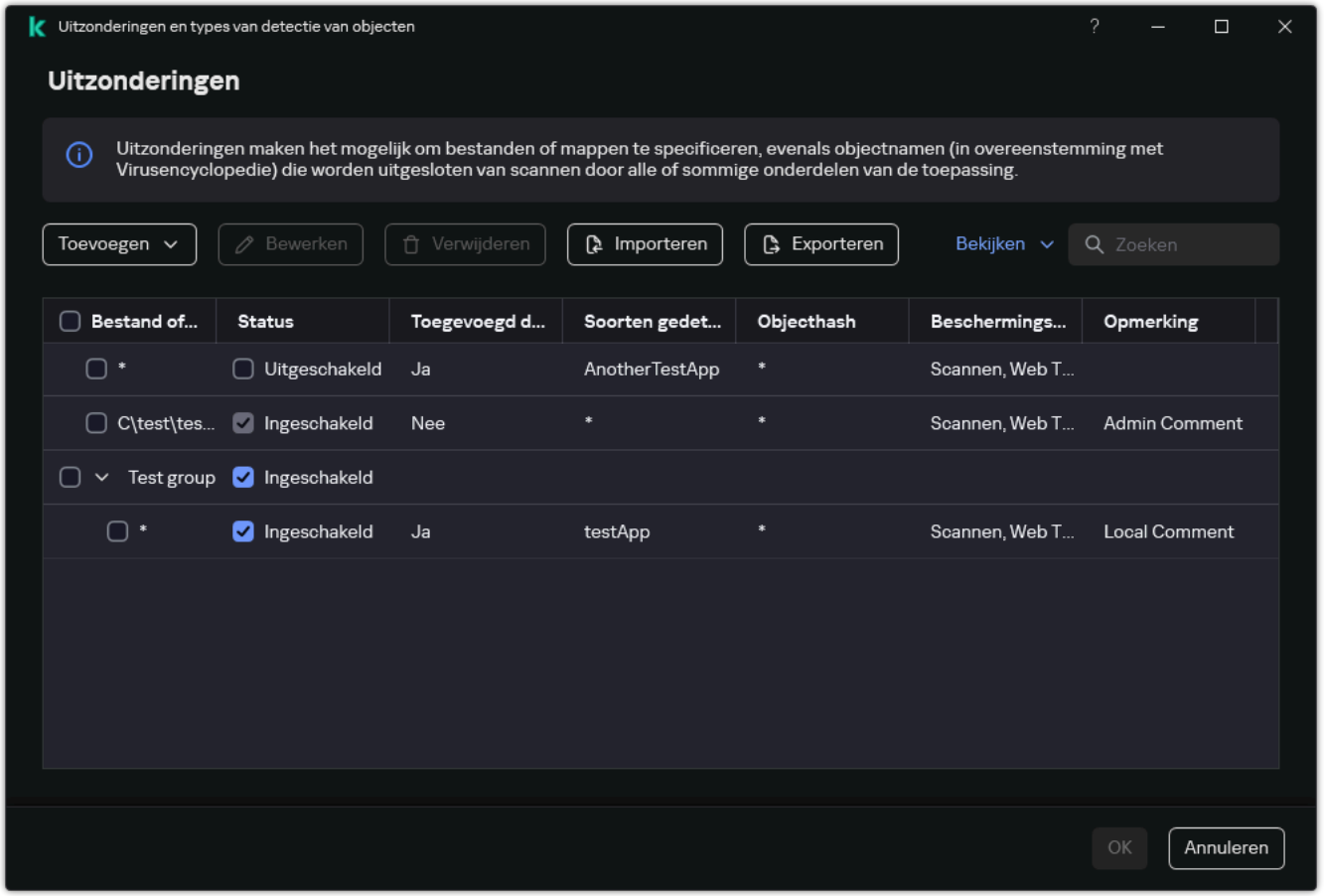
9. Typ indien nodig in het veld **Opmerking** een korte opmerking over de scanuitzondering die u maakt.

10. Selecteer de status **Actief** voor de uitzondering.

11. Klik op **Toevoegen**.

    De nieuwe uitzondering wordt aan de lijst toegevoegd. U kunt de uitzondering op elk moment stoppen met behulp van het selectievakje in de kolom **Status**.

12. Sla uw wijzigingen op.



Lijst met uitzonderingen

Voorbeelden padmasker:

We raden aan dat u relatieve paden opgeeft in plaats van absolute paden. Hierdoor kunt u niet alleen bestandssysteemobjecten uitsluiten, maar ook objecten zonder bestanden. Bijvoorbeeld `*\Program Files (x86)\Folder\Subfolder`.

Paden naar bestanden in een willekeurige map:

- Het masker `*.exe` omvat alle paden naar bestanden met de EXE-extensie.
- Het masker `example*` omvat alle paden naar bestanden met de naam EXAMPLE.

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.
- 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\`.
- Het masker `C:\dir1\*\dir3\` omvat alle paden naar bestanden in dir3-submappen één niveau in de map `C:\dir1\`.
- Het masker `C:\dir1\**\dirN\` bevat alle paden naar bestanden in dirN-submappen in de map `C:\dir1\` op elk niveau.

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 uitzondering maken op type gedetecteerde objecten

Kaspersky Endpoint Security classificeert gedetecteerde objecten als volgt:

- **Virussen en wormen**

  Subcategorie: Virussen en wormen (Viruses_and_Worms)

  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. *Overwriting* 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. *Parasitic* virussen wijzigen bestanden waardoor ze volledig of deels functioneel blijven. *Companion* 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: *Link virussen*, *OBJ-virussen*, *LIB-virussen*, *broncode* virussen 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. 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.
IRC-Worm	Online chat wormen	Deze verspreiden zich via Internet Relay Chats, servicesystemen waarmee mensen met elkaar kunnen communiceren in real time via het internet. 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.
Net-worm	Netwerkwormen	Deze wormen verspreiden zich via computernetwerken. 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.
P2P-worm	Netwerkwormen voor bestandsdeling	Deze verspreiden zich via peer-to-peernetwerken voor bestandsdeling. 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. 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.

Type	Naam	Beschrijving
Worm	Andere soorten wormen	Enkele andere soorten wormen zijn: • 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. • 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.

  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
Trojan-ArcBomb	Trojans – "archiefbommen"	Tijdens het uitpakken worden deze archieven zo groot dat de werking van de computer wordt beïnvloed. 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.
Backdoor	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.
Trojan	Trojans	Deze omvatten de volgende schadelijke programma's: • **Klassieke Trojans**. 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. • **Veelzijdige Trojans**. Deze programma's hebben geavanceerde functies die kenmerken zijn voor diverse soorten Trojans.
Trojan-Ransom	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.
Trojan-Clicker	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.

Type	Naam	Beschrijving
Trojan-Downloader	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.
Trojan-Dropper	Trojan droppers	Deze bevatten andere Trojans die ze op de harde schijf plaatsen en vervolgens installeren. Indringers kunnen programma's van het type Trojan Dropper gebruiken voor het volgende: • 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. • De detectie van een ander schadelijk programma voorkomen: niet alle antivirussoftware kan een schadelijk programma in een programma van het type Trojan Dropper detecteren.
Trojan-Notifier	Trojan notifiers	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. 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.
Trojan-Proxy	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.
Trojan-PSW	Software voor het stelen van wachtwoorden	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. 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).
Trojan-Spy	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.
Trojan-DDoS	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. 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.
Trojan-IM	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.
Rootkit	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.
Trojan-SMS	Trojans in de vorm van sms-berichten	Deze infecteren mobiele telefoons door sms-berichten naar betalende telefoonnummers te versturen.
Trojan-GameThief	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.
Trojan-Banker	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.
Trojan-Mailfinder	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
Constructeur	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.
Dos	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).
Exploit	Exploits	Een *exploit* 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. 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. Net-Worms verspreiden zich via netwerken door middel van exploits. Nuker exploits zijn netwerkpakketten die computers uitschakelen.
FileCryptor	Encryptors	Deze encrypten andere schadelijke programma's om ze te verbergen voor het antivirusprogramma.
Flooder	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).
HackTool	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.
Hoax	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.
Spoofer	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.
VirTool	Tools die schadelijke programma's aanpassen	Deze kunnen worden gebruikt om malware aan te passen en ze te verbergen voor antivirusprogramma's.
Email-Flooder	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.

Type	Naam	Beschrijving
IM-Flooder	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.
SMS-Flooder	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: Automatische inbelprogramma's (Inbeller).

  Veiligheidsrisico: Gemiddeld

  Automatische inbelprogramma's kunnen heimelijk telefoonverbindingen tot stand brengenvia een modem.

- **Legitieme software die hackers kunnen gebruiken om de computer of persoonlijke gegevens te beschadigen**

  Subcategorie: Legitieme software die inbrekers 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 internetservers 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
Client-IRC	Online chatprogramma's	Gebruikers installeren deze programma's om met personen in Internet Relay Chats te spreken. Indringers gebruiken ze om malware te verspreiden.
Downloader	Programma's voor downloads	Deze kunnen bestanden vanaf webpagina's downloaden in een verborgen modus.

Type	Naam	Beschrijving
Monitor	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).
PSWTool	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.
RemoteAdmin	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. 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.
Server-FTP	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.
Server-Proxy	Proxyservers	Deze werken als proxyservers. Indringers plaatsen ze op de computer van de gebruiker om spam onder de naam van de gebruiker te versturen.
Server-Telnet	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.
Server-Web	Webservers	Deze werken als webservers. Indringers plaatsen ze op de computer van de gebruiker om er op afstand toegang tot te krijgen via HTTP.
RiskTool	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.
NetTool	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.
Client-P2P	P2P-netwerkprogramma's	Deze hebben functies voor peer-to-peernetwerken. Ze kunnen door indringers worden gebruikt om malware te verspreiden.
Client-SMTP	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.
WebToolbar	Online werkbalken	Deze voegen werkbalken aan de interface van andere programma's toe om zoekmachines te gebruiken.
FraudTool	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**

  subcategorie: Ingepakte bestanden die schade kunnen veroorzaken.

  Veiligheidsrisico: Gemiddeld.

  Het bestand wordt ingepakt met een speciale packer die wordt gebruikt voor het verpakken van malware: virussen, wormen, Trojans. Kaspersky Endpoint Security scant de decompressiemodule in SFX-archieven (zelfuitpakkende archieven).

  Om malware te verbergen voor detectie door een antivirusprogramma, pakken hackers het in met speciale packers. Kaspersky-experts hebben de compressieprogramma's geïdentificeerd die hackers het meest gebruiken.

- **Meermaals ingepakte objecten**

  subcategorie: Meerdere verpakte bestanden.

  Veiligheidsrisico: Gemiddeld.

Het bestand is drie of meer keer ingepakt met een of meer packers.

Om te voorkomen dat malware door een antivirusprogramma wordt gedetecteerd, kunnen hackers een bestand meerdere keren inpakken. Kaspersky Endpoint Security scant ingepakte bestanden.

Standaard detecteert Kaspersky Endpoint Security alle soorten objecten. We raden aan om de detectie van alle soorten objecten ingeschakeld te laten om de beveiliging van de computer te verbeteren. Als u interne hulpprogramma's gebruikt die door het programma als kwaadaardig worden gedetecteerd, voeg deze hulpprogramma's toe aan een lijst met uitzonderingen, maar schakel de detectie van het hele type objecten niet uit.

Selecteer de typen detecteerbare objecten in de Beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de beheerconsole **Policies**.
3. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
4. Selecteer **Algemene instellingen** → **Uitzonderingen en objecttypen** in het beleidsvenster.
5. In het blok **Soorten gedetecteerde objecten**, klikt u op de knop **Instellingen**.
6. Schakel in het venster dat wordt geopend de selectievakjes aan naast de soorten objecten die u door Kaspersky Endpoint Security wilt laten detecteren.
7. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Selecteer soorten detecteerbare objecten in de Webconsole en de Cloudconsole

1. Selecteer in het hoofdvenster van de Webconsole het tabblad **Asset management** → **Policies**.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.

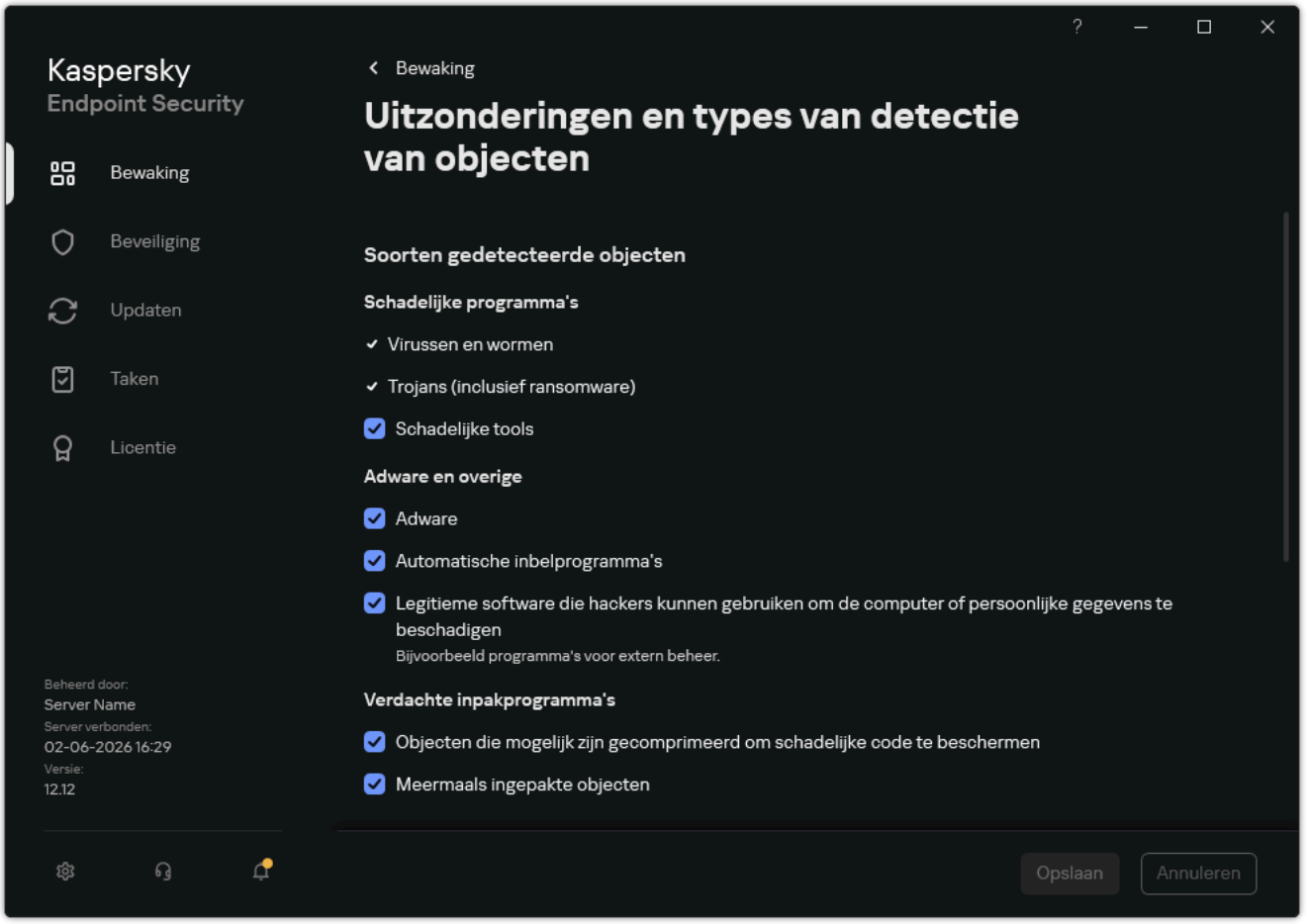
   U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **General Settings** → **Detection Settings**.
5. Schakel in het gedeelte **Detection of other types of objects** de selectievakjes in naast de soorten objecten die Kaspersky Endpoint Security moet detecteren.
6. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Selecteer de typen detecteerbare objecten in de programma-interface

1. Klik in het hoofdvenster van het programma op de knop .
2. Selecteer **Algemene instellingen** → **Uitzonderingen en types van detectie van objecten** 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.

4. Sla uw wijzigingen op.



Soorten detecteerbare objecten

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 bewaakt 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. Nadat een programma is toegevoegd aan de lijst met vertrouwde programma's, stopt Kaspersky Endpoint Security met het monitoren van de activiteit van het programma.

Het verschil tussen scanuitzonderingen en vertrouwde programma's is dat Kaspersky Endpoint Security voor uitzonderingen geen bestanden scant, terwijl het voor vertrouwde programma's geen controle heeft over de gestarte processen. Als een vertrouwd programma een kwaadaardig bestand maakt in een map die niet is opgenomen in scanuitzonderingen, zal Kaspersky Endpoint Security het bestand detecteren en de dreiging elimineren. Als de map wordt toegevoegd aan uitzonderingen, slaat Kaspersky Endpoint Security dit bestand over.

Als u bijvoorbeeld objecten die door het standaard Microsoft Windows-programma Kladblok worden gebruikt als veilig beschouwt, omdat u dit programma vertrouwt, kunt u Microsoft Windows-programma Kladblok toevoegen aan de lijst met vertrouwde programma's, zodat de objecten die door dit programma worden gebruikt, niet bewaakt. Dit zal de computerprestaties verbeteren, wat vooral belangrijk is bij het gebruik van servertoepassingen.

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.

Vertrouwde programma's helpen compatibiliteitsproblemen tussen Kaspersky Endpoint Security en andere programma's te voorkomen (bijvoorbeeld het probleem van het dubbel scannen van het netwerkverkeer van een computer van derden door Kaspersky Endpoint Security en door een ander antivirusprogramma).

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.

Het wijzigen van de lijst met vertrouwde programma's wordt mogelijk geblokkeerd door de eigenschappen van het bovenliggende beleid. Om de lijst te wijzigen, moet u toestaan dat de instellingen van vertrouwde zone in de Webconsole (het "hangslot" moet ontgrendeld zijn).

Vertrouwde zones zijn verschillend gegroepeerd in de Beheerconsole (MMC) en de Webconsole. Ook de manier waarop wijziging in de parameters voor de vertrouwde zone worden voorkomen, verschilt (verschillende "hangsloten"). We raden aan dat u alleen de Webconsole gebruikt om het programma te beheren. Als u de vertrouwde zone in verschillende consoles configureert, kan de beheerplug-in het "hangslot" terugzetten naar de standaardstatus.

Een programma toevoegen aan de vertrouwde lijst in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Algemene instellingen** → **Uitzonderingen en objecttypen** in het beleidsvenster.
4. In het blok **Scanuitzonderingen en vertrouwde programma's** → **Vertrouwde programma's**, klikt u op de knop **Instellingen**.

   Dit opent een venster met een lijst met vertrouwde programma's.
5. 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.
6. 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. En, wanneer dit selectievakje uitgeschakeld is, verbergt Kaspersky Endpoint Security de geconsolideerde lijst met vertrouwde programma's in de gebruikersinterface van het programma.

7. Klik **Toevoegen** en selecteer een actie:

- **Categorie**. U kunt vertrouwde programma's in afzonderlijke categorieën groeperen. Om een nieuwe categorie aan te maken, voer de naam van de categorie in en voeg ten minste één vertrouwd programma toe aan de categorie.

- **Nieuwe uitzondering**. Kaspersky Endpoint Security voegt een nieuw vertrouwd programma toe aan de hoofdmap van de lijst.

- **Selecteer uitzonderingen uit lijst**. Om Kaspersky Endpoint Security snel te configureren op SQL-servers, Microsoft Exchange-servers en System Center Configuration Manager, bevat het programma: *vooraf gedefinieerde vertrouwde programma's*. Er zijn ook vooraf gedefinieerde vertrouwde programma's toegevoegd om de installatie van progromma's in virtuele Citrix- en VMware-omgevingen te ondersteunen. Afhankelijk van het doel van de beveiligde server moet u vooraf gedefinieerde vertrouwde programma's selecteren.

- **Nieuwe uitzonderingen in geselecteerde categorie**. Als u een nieuw vertrouwd programma aan een specifieke categorie wilt toevoegen, selecteer een categorie.

8. Selecteer de vertrouwenscriteria:

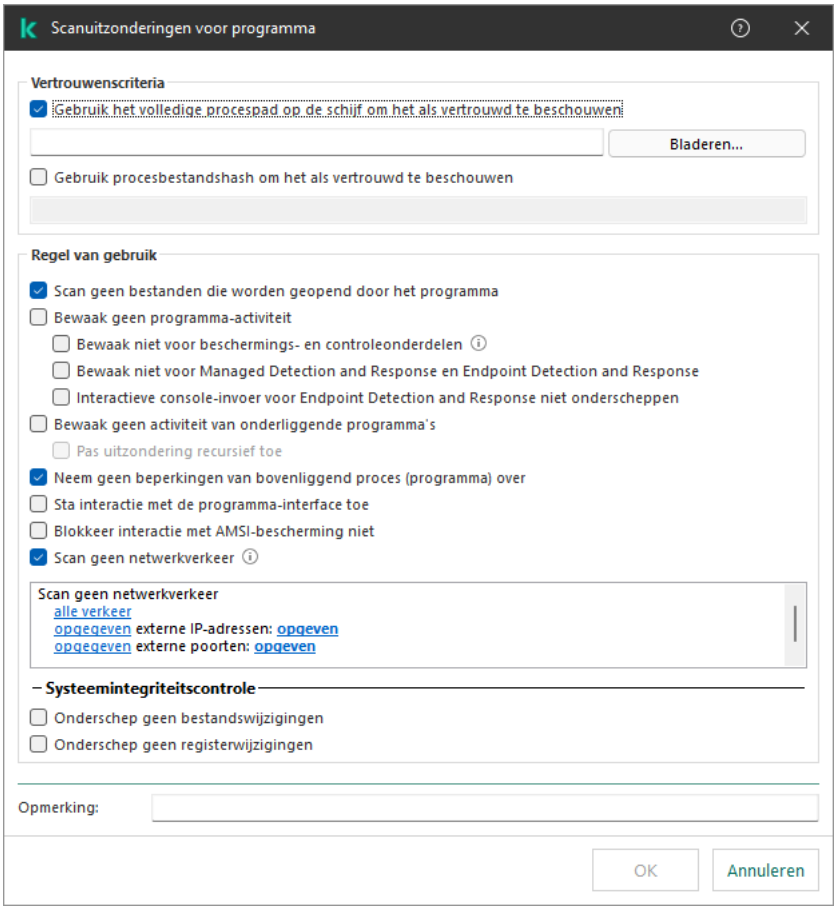
- **Gebruik het volledige procespad op de schijf om het als vertrouwd te beschouwen**. Voer het pad naar het uitvoerbare bestand van het vertrouwde programma in.

  Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de `*` en `?`-tekens bij het invoeren van een masker.

  Kaspersky Endpoint Security behandelt de bestandsnaam van een vertrouwd programma als hoofdlettergevoelig. Als de bestandsnaam die u invoert de verkeerde naam heeft, herkent Kaspersky Endpoint Security het vertrouwde programma niet.

- **Gebruik procesbestandshash om het als vertrouwd te beschouwen**.

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.

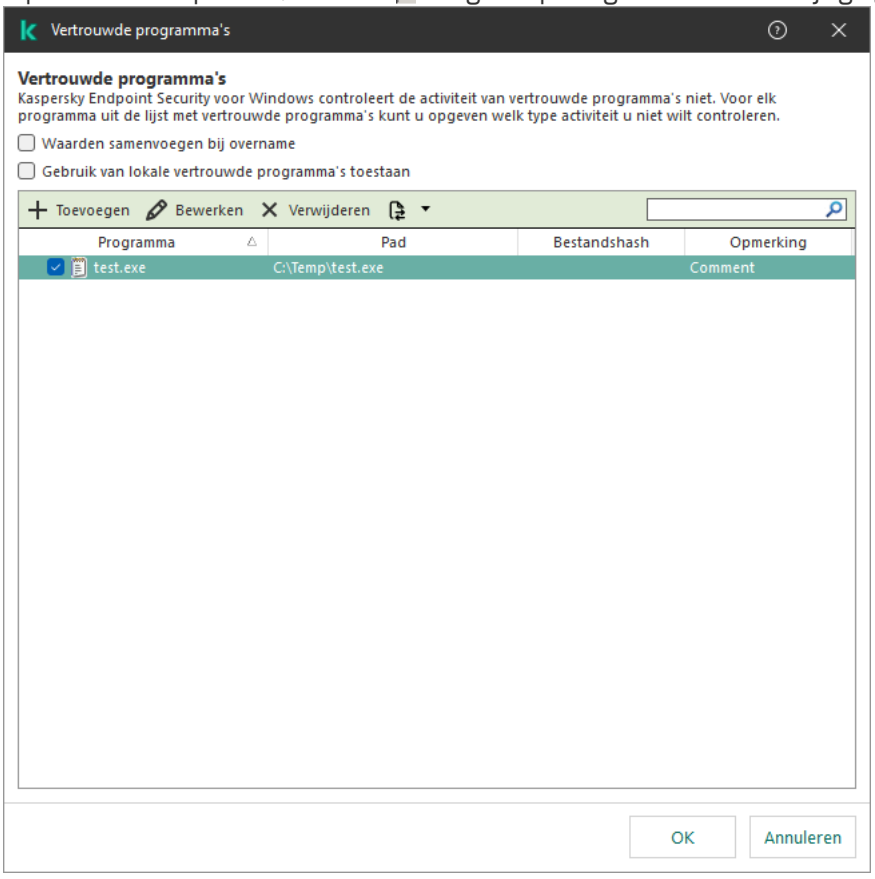


Instellingen vertrouwde programma's

9. Configureer de geavanceerde instellingen voor het vertrouwde programma (zie onderstaande tabel).
10. Klik op **OK**.

    De nieuwe vertrouwde programma wordt aan de lijst toegevoegd. U kunt op elk moment een programma uitsluiten van de vertrouwde zone met behulp van het selectievakje naast het object.

11. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.



Lijst met vertrouwde programma's

Een applicatie toevoegen aan de vertrouwde lijst in de webconsole en cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 het gedeelte **Trusted Zone**.
5. Klik in het venster op de link **Applications**.

   Dit opent een venster met een lijst met vertrouwde programma's.
6. Schakel het selectievakje **Merge values when inheriting** 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 **Allow use of local exclusions** 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. En, wanneer dit selectievakje uitgeschakeld is, verbergt Kaspersky Endpoint Security de geconsolideerde lijst met vertrouwde programma's in de gebruikersinterface van het programma.

8. Klik **Add** en selecteer een actie:

   - **Category**. U kunt vertrouwde programma's in afzonderlijke categorieën groeperen. Om een nieuwe categorie aan te maken, voer de naam van de categorie in en voeg ten minste één vertrouwd programma toe aan de categorie.
   - **New exclusion**. Kaspersky Endpoint Security voegt een nieuw vertrouwd programma toe aan de hoofdmap van de lijst.
   - **Select exclusion from list**. Om Kaspersky Endpoint Security snel te configureren op SQL-servers, Microsoft Exchange-servers en System Center Configuration Manager, bevat het programma: *vooraf gedefinieerde vertrouwde programma's*. Er zijn ook vooraf gedefinieerde vertrouwde programma's toegevoegd om de installatie van progromma's in virtuele Citrix- en VMware-omgevingen te ondersteunen. Afhankelijk van het doel van de beveiligde server moet u vooraf gedefinieerde vertrouwde programma's selecteren.

   Als u een nieuwe vertrouwd programma aan een specifieke categorie wilt toevoegen, schakel het selectievakje naast die categorie in en selecteer de optie **New exclusion**.

9. Selecteer de vertrouwenscriteria:

   - **Path to the file or folder**. Voer het pad naar het uitvoerbare bestand van het vertrouwde programma in.

     Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de `*` en `?`-tekens bij het invoeren van een masker.

     Kaspersky Endpoint Security behandelt de bestandsnaam van een vertrouwd programma als hoofdlettergevoelig. Als de bestandsnaam die u invoert de verkeerde naam heeft, herkent Kaspersky Endpoint Security het vertrouwde programma niet.

   - **Application hash**.

   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. Klik op **OK**.

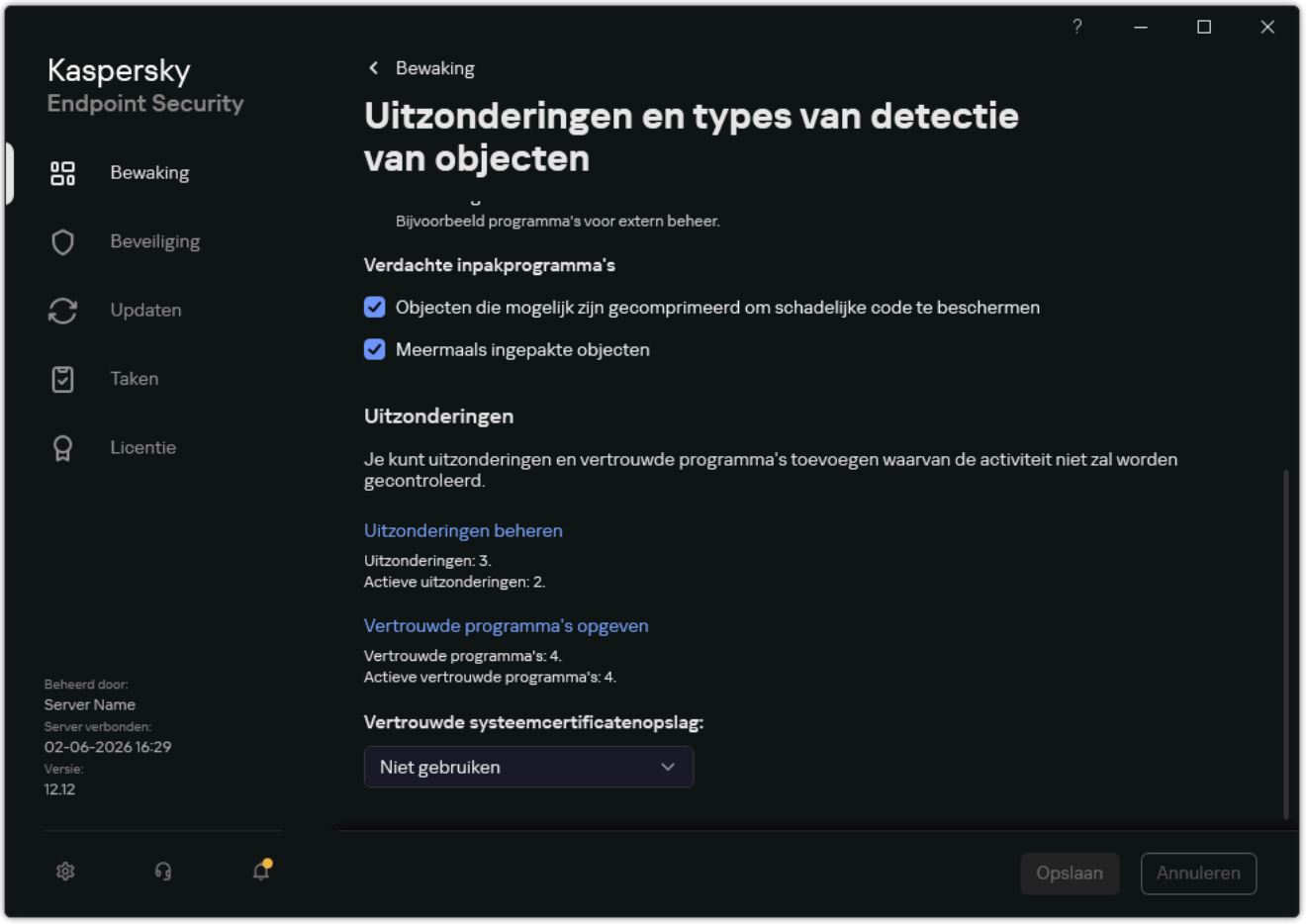
    De nieuwe vertrouwde programma wordt aan de lijst toegevoegd. U kunt op elk moment een programma uitsluiten van de vertrouwde zone met behulp van het selectievakje in de kolom **Status**.

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** → **Uitzonderingen en types van detectie van objecten** in het venster met de programma-instellingen.
3. Klik in het blok **Uitzonderingen** op de koppeling **Vertrouwde programma's opgeven**.

Kaspersky Endpoint Security verbergt de geconsolideerde lijst met vertrouwde programma's in de gebruikersinterface van het programma als het instellen van vertrouwde programma's geblokkeerd is door de beheerder in de console ("gesloten slot"-symbool) en lokale vertrouwde programma's zijn verboden (het selectievakje **Gebruik van lokale vertrouwde programma's toestaan** is uitgeschakeld).



Instellingen van uitzonderingen

4. Klik **Toevoegen** en selecteer een actie:

   - **Categorie**. U kunt vertrouwde programma's in afzonderlijke categorieën groeperen. Om een nieuwe categorie aan te maken, voer de naam van de categorie in en voeg ten minste één vertrouwd programma toe aan de categorie.

   - **Nieuwe uitzondering**. Kaspersky Endpoint Security voegt een nieuw vertrouwd programma toe aan de hoofdmap van de lijst.

   - **Selecteer uitzonderingen uit lijst**. Om Kaspersky Endpoint Security snel te configureren op SQL-servers, Microsoft Exchange-servers en System Center Configuration Manager, bevat het programma: *vooraf gedefinieerde vertrouwde programma's*. Er zijn ook vooraf gedefinieerde vertrouwde programma's toegevoegd om de installatie van progromma's in virtuele Citrix- en VMware-omgevingen te ondersteunen. Afhankelijk van het doel van de beveiligde server moet u vooraf gedefinieerde vertrouwde programma's selecteren.

   Als u een nieuwe vertrouwd programma aan een specifieke categorie wilt toevoegen, schakel het selectievakje naast die categorie in en selecteer de optie **Nieuwe uitzondering**.

5. Selecteer de vertrouwenscriteria:

   - **Gebruik het volledige procespad op de schijf om het als vertrouwd te beschouwen**. Voer het pad naar het uitvoerbare bestand van het vertrouwde programma in.

     Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de `*` en `?`-tekens bij het invoeren van een masker.

     Kaspersky Endpoint Security behandelt de bestandsnaam van een vertrouwd programma als hoofdlettergevoelig. Als de bestandsnaam die u invoert de verkeerde naam heeft, herkent Kaspersky Endpoint Security het vertrouwde programma niet.

   - **Gebruik procesbestandshash om het als vertrouwd te beschouwen**.

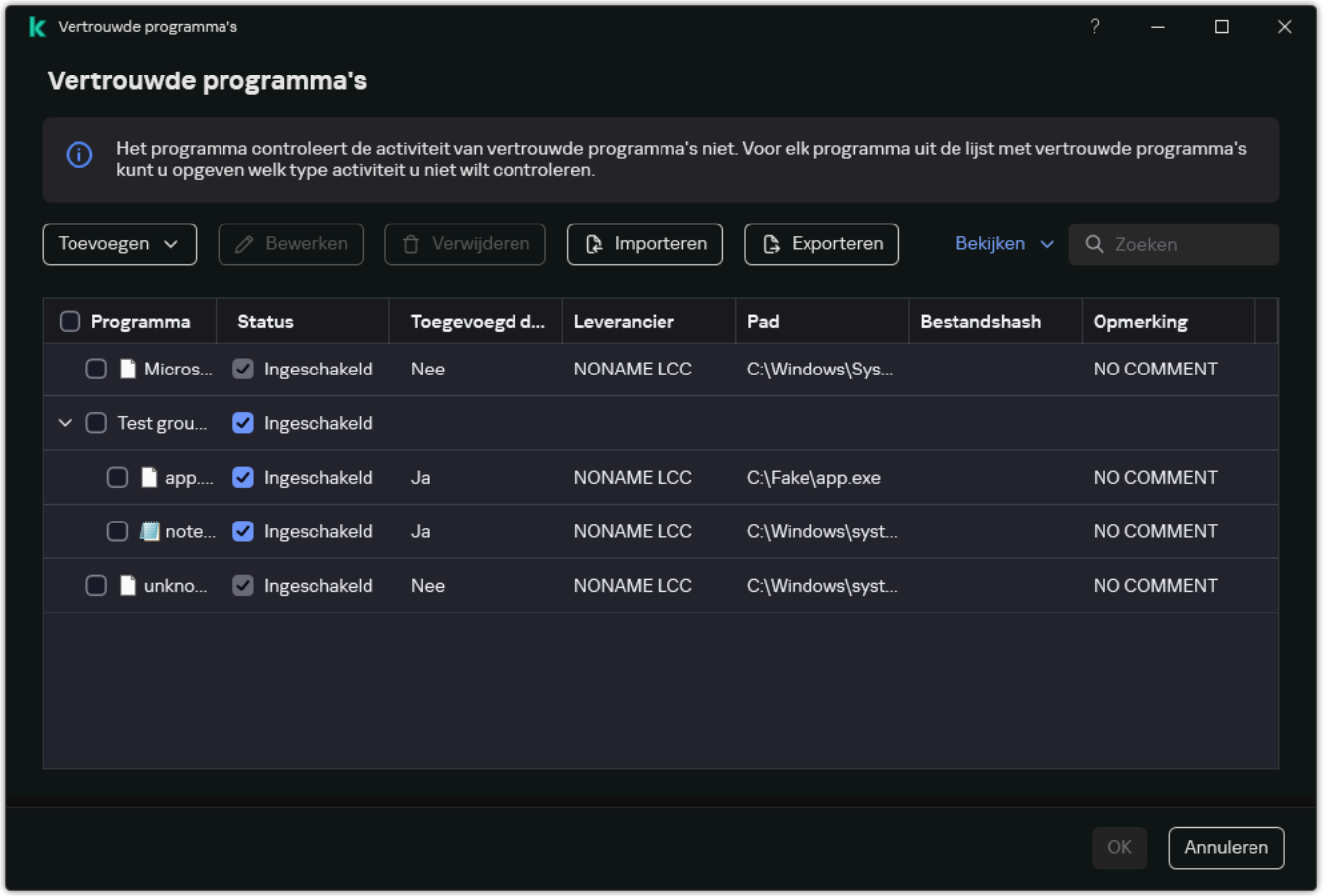
   Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en converteert het pad in de lokale interface van het programma. Als u met andere woorden het bestandspad `%userprofile%\Documents\File.exe` opent, wordt een record `C:\Users\Fred123\Documents\File.exe` toegevoegd aan lokale interface van het 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.

7. Klik op **OK**.

   De nieuwe vertrouwde programma wordt aan de lijst toegevoegd. U kunt op elk moment een programma uitsluiten van de vertrouwde zone met behulp van het selectievakje in de kolom **Status**.

8. Sla uw wijzigingen op.



Lijst met vertrouwde programma's

Instellingen vertrouwde programma's

Parameter	Beschrijving
Scan geen bestanden die door het programma worden geopend	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.
Bewaak geen programma-activiteit	Kaspersky Endpoint Security controleert de bestands- en netwerkactiviteit van het programma in het besturingssysteem niet. U kunt het monitoren van programma-activiteit configureren voor verschillende onderdelen van Kaspersky Endpoint Security: • **Bewaak niet voor beschermings- en controleonderdelen**. De programma/activiteit wordt gecontroleerd door de volgende componenten: Gedragsdetectie, Exploit-preventie, Host Intrusion Prevention, Remediation Engine en Firewall. • **Bewaak niet voor Managed Detection and Response en Endpoint Detection and Response**. De programma/activiteit wordt gecontroleerd door ingebouwde MDR agent en ingebouwde EDR (KATA) agent. • **Interactieve console-invoer voor Endpoint Detection and Response niet onderscheppen**. Kaspersky Endpoint Security verzendt geen telemetriegegevens over het beheer van het programma op de console. Telemetriegegevens worden gebruikt door Kaspersky Anti Targeted Attack Platform (EDR).
Bewaak geen activiteit van onderliggende programma's	Kaspersky Endpoint Security bewaakt de bestands- of netwerkactiviteit van programma's die worden gestart door het programma niet. U kunt de uitzondering recursief toepassen. Zodat het programma niet de activiteit van de hele keten van onderliggende programma's bewaakt.
Neem geen beperkingen van bovenliggend proces (programma) over	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 programmamachtigingen (Host Intrusion Prevention) en netwerkregels voor programma's (Firewall) zijn geconfigureerd.
Bewaak geen activiteit van onderliggende programma's	Kaspersky Endpoint Security bewaakt de bestands- of netwerkactiviteit van programma's die worden gestart door het programma niet. U kunt de uitzondering recursief toepassen. Zodat het programma niet de activiteit van de hele keten van onderliggende programma's bewaakt.
Sta interactie met de programma-interface toe	Kaspersky Endpoint Security Self-Defense 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.

Parameter	Beschrijving
Blokkeer interactie met AMSI-bescherming niet	Kaspersky Endpoint Security controleert de verzoeken van het vertrouwde programma voor objecten die moeten worden gescand door de AMSI bescherming niet.
Scan geen netwerkverkeer	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. Kaspersky Endpoint Security versie 14.0 of ouder ondersteunt het uitsluiten van netwerkverkeer als een hash is opgegeven voor een vertrouwd programma in plaats van een pad niet.
Onderschep geen bestandswijzigingen *(alleen beschikbaar in de Kaspersky Security Center-console)*	Kaspersky Endpoint Security bewaakt geen wijzigingen in bestanden vanaf de Systeemintegriteitscontrole bewakingsbereik. Het programma past de uitzondering toe op alle modi van Systeemintegriteitscontrole: Realtime systeemintegriteitscontrole en On-demand systeemintegriteitscontrole.
Onderschep geen registerwijzigingen *(alleen beschikbaar in de Kaspersky Security Center-console)*	Kaspersky Endpoint Security bewaakt geen wijzigingen in registersleutels vanaf de Systeemintegriteitscontrole bewakingsbereik. Het programma past de uitzondering toe op alle modi van Systeemintegriteitscontrole: Realtime systeemintegriteitscontrole en On-demand systeemintegriteitscontrole.
Opmerking	Indien nodig kunt u een korte opmerking plaatsen voor de vertrouwde toepassing. Opmerkingen helpen het zoeken en sorteren van vertrouwde applicaties te vereenvoudigen.
Status	Status van de vertrouwde applicatie: • De status **Actief** betekent dat het programma in de vertrouwde zone zit. • **Inactief** status betekent dat de applicatie is uitgesloten van de vertrouwde zone.

Een lokale vertrouwde zone creëren

De gebruiker kan nu zijn eigen lokale vertrouwde zone voor een specifieke computer creëren. Op deze manier kan de gebruiker zijn eigen lokale lijsten met scanuitsluitingen 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 in de beleidsinstellingen. Gebruik hiervoor de **Gebruik van lokale uitzonderingen toestaan** en **Gebruik van lokale vertrouwde programma's toestaan** selectievakjes in de **Uitzonderingen** gedeelte van het beleid.

Als het maken van een lokale vertrouwde zone is toegestaan door een beheerder, kan de gebruiker zijn eigen scanuitzonderingen en vertrouwde programma's toevoegen in de gebruikersinterface van het programma. Tegelijkertijd heeft de gebruiker geen machtigingen om objecten te wijzigen of te verwijderen uit de vertrouwde zone die in het beleid is geconfigureerd. De beheerder kan ook lijstitems bekijken, toevoegen, wijzigen of verwijderen in de Kaspersky Security Center-console als er uitzonderingen moeten worden toegevoegd voor een individuele computer.

Kaspersky Endpoint Security verbergt de lijst met scanuitzonderingen en vertrouwde programma's in de gebruikersinterface van het programma als het instellen van de vertrouwde zone geblokkeerd is door de beheerder in de console ("gesloten slot"-symbool) en lokale scanuitzonderingen en vertrouwde programma's zijn verboden.

Een object toevoegen aan de lokale vertrouwde zone 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.

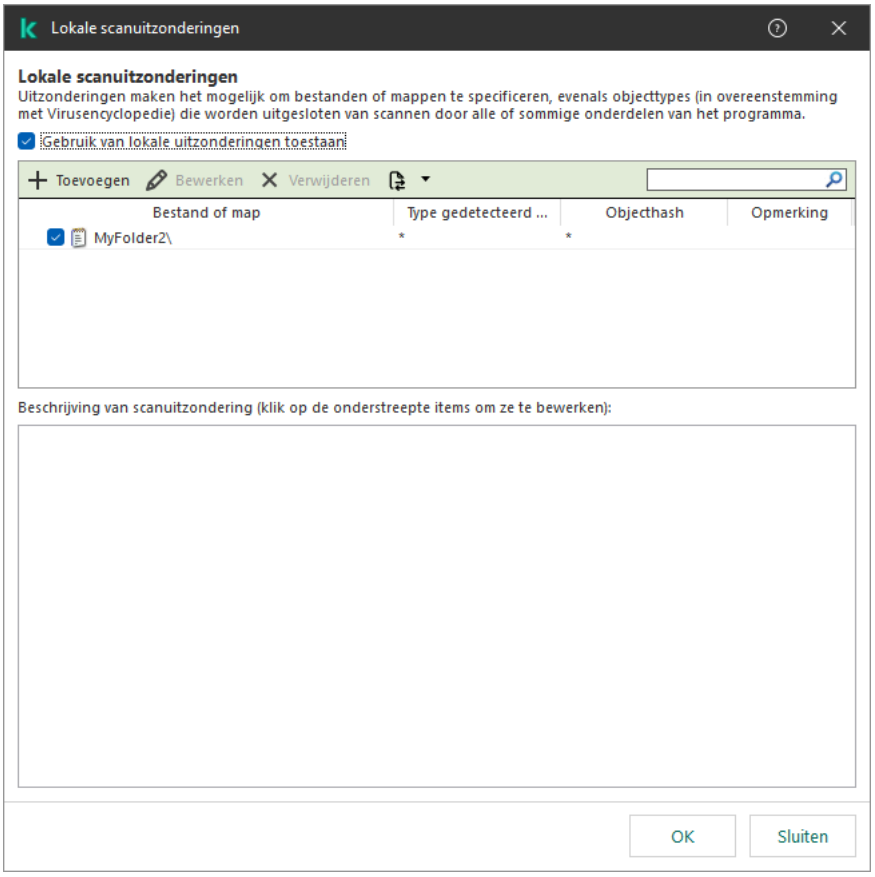
5. Selecteer het gedeelte **Applications** in het venster met computereigenschappen.

6. Selecteer **Kaspersky Endpoint Security voor Windows (14.1)** in de lijst met Kaspersky-programma's die op de computer zijn geïnstalleerd en dubbelklik om de eigenschappen van het programma te openen.

7. Selecteer **Algemene instellingen** → **Uitzonderingen en objecttypen** in het venster met de programma-instellingen.

8. In het blok **Scanuitzonderingen en vertrouwde programma's** → **Lokale scanuitzonderingen**, klikt u op de knop **Instellingen**.

   Met een klik op deze koppeling opent u een venster waarin u een lijst met lokale uitzonderingen vindt.



Instellingen vertrouwde zone

9. Maak een lijst met lokale scanuitzonderingen.

   De regels voor het maken van lokale scanuitzonderingen zijn dezelfde als voor algemene uitzonderingen. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de * en ?-tekens bij het invoeren van een masker.

10. In het blok **Scanuitzonderingen en vertrouwde programma's** → **Lokale vertrouwde programma's**, klikt u op de knop **Instellingen**.

    Dit opent een venster met een lijst met lokale vertrouwde programma's.

11. Maak een lijst met lokale vertrouwde programma's.

    Regels voor het toevoegen van programma's aan de lijst met lokale vertrouwde programma's zijn dezelfde als de regels voor het toevoegen ervan aan de algemene lijst. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de * en ?-tekens bij het invoeren van een masker.

12. Sla uw wijzigingen op.

Een object toevoegen aan de lokale vertrouwde zone in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Assets (Devices)**.
2. Klik op de naam van de computer waarop u een gebruiker een geblokkeerde actie wilt laten uitvoeren.
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. Selecteer **General settings** → **Exclusions and types of detected objects** in het venster met de programma-instellingen.
7. Klik in het blok **Scan exclusions and trusted applications** op de koppeling **Local scan exclusions**.
8. Maak een lijst met lokale scanuitzonderingen.

   Regels voor het maken van lokale uitzonderingen zijn dezelfde als de regels voor het maken van algemene uitzonderingen. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de * en ?-tekens bij het invoeren van een masker.

9. Klik in het blok **Scan exclusions and trusted applications** op de koppeling **Local trusted applications**.
10. Maak een lijst met lokale vertrouwde programma's.

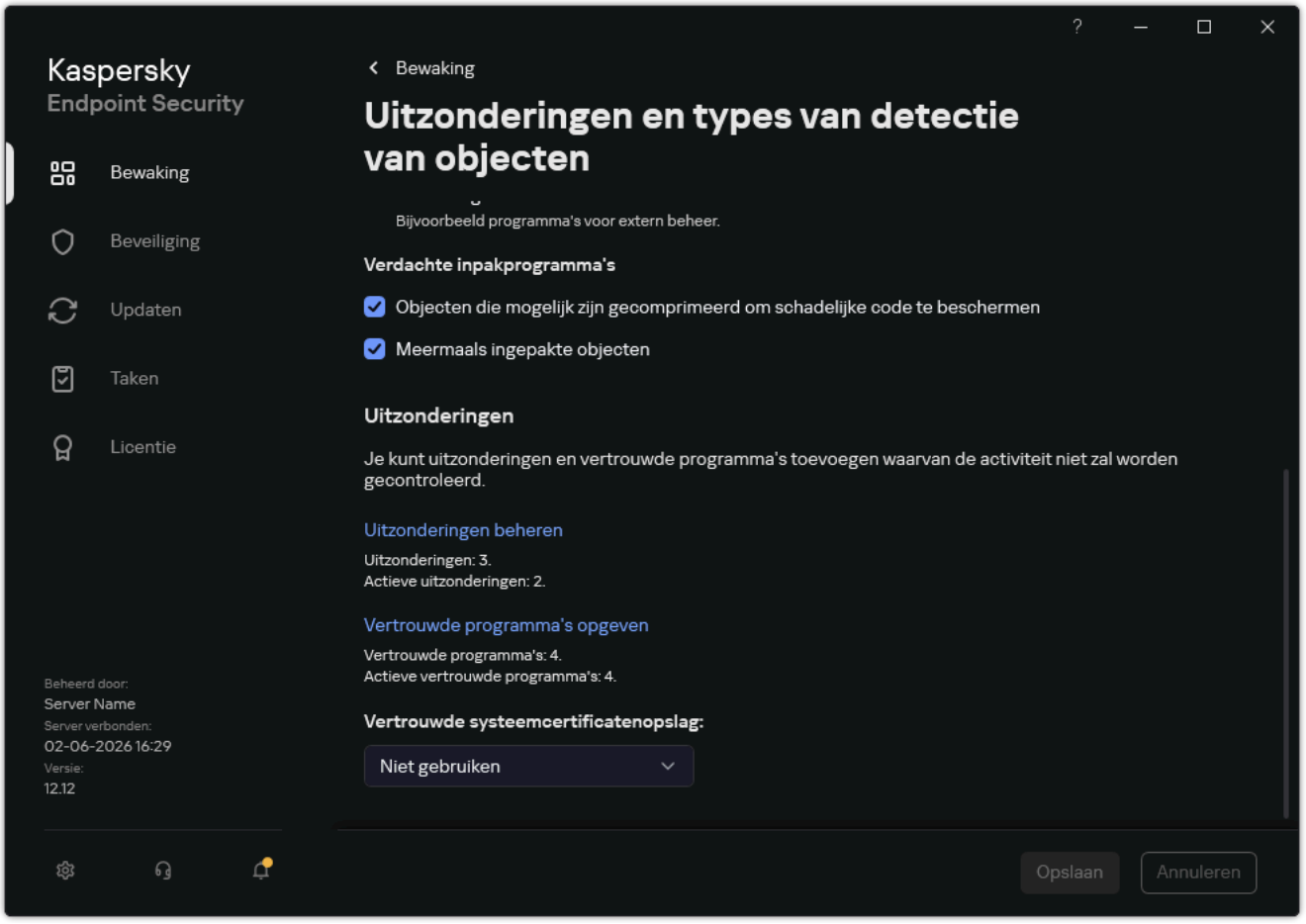
    Regels voor het toevoegen van programma's aan de lijst met lokale vertrouwde programma's zijn dezelfde als de regels voor het toevoegen ervan aan de algemene lijst. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de * en ?-tekens bij het invoeren van een masker.

11. Sla uw wijzigingen op.

Een lokale scanuitzondering maken in de programma-interface

1. Klik in het hoofdvenster van het programma op de knop ⚙.
2. Selecteer **Algemene instellingen** → **Uitzonderingen en types van detectie van objecten** in het venster met de programma-instellingen.
3. Klik in het blok **Uitzonderingen** op de koppeling **Uitzonderingen beheren**.

Kaspersky Endpoint Security verbergt de lijst met scanuitzonderingen in de gebruikersinterface van het programma als het instellen van scanuitzonderingen geblokkeerd is door de beheerder in de console ("gesloten slot"-symbool) en lokale scanuitzonderingen zijn verboden (het selectievakje **Gebruik van lokale uitzonderingen toestaan** is uitgeschakeld).



Instellingen van uitzonderingen

4. Klik **Toevoegen** en selecteer een actie:

   - **Categorie**. U kunt scanuitzonderingen groeperen in afzonderlijke categorieën. Om een nieuwe categorie te maken, voer de naam van de categorie in en voeg ten minste één scanuitzonderingen toe aan de categorie.

   - **Nieuwe uitzondering**. Kaspersky Endpoint Security voegt een nieuwe scanuitzondering toe aan de hoofdmap van de lijst.

   - **Selecteer uitzonderingen uit lijst**. Om Kaspersky Endpoint Security snel te configureren op SQL-servers, Microsoft Exchange-servers en System Center Configuration Manager, bevat het programma: *vooraf gedefinieerde scanuitzonderingen*. Er zijn ook vooraf gedefinieerde scanuitzonderingen toegevoegd om de installatie van progromma's in virtuele Citrix- en VMware-omgevingen te ondersteunen. U moet vooraf gedefinieerde scanuitzonderingen selecteren, afhankelijk van het doel van de beveiligde server.

   Om een nieuwe scanuitzonderingen aan een specifieke categorie toe te voegen, schakel het selectievakje naast die categorie in en selecteer de optie **Nieuwe uitzondering**.

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 verwijderen. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de `*` en `?`-tekens bij het invoeren 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:\Folder\**\*.txt` omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen bevinden genest in de `Folder`, uitgezonderd de `Folder` 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:\Folder\???.txt` omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam `Folder` bevinden, die een TXT-extensie hebben en die een naam met drie tekens hebben.

  U kunt maskers gebruiken aan het begin, in het midden of aan het einde van het bestandspad. Als u bijvoorbeeld een map voor alle gebruikers aan uitzonderingen wilt toevoegen, voert u het masker `?:\Users\*\Folder\` in.

  U kunt netwerkmappen uitsluiten. Voer hiervoor het pad naar de netwerkmap handmatig in (bijvoorbeeld, `\\Network Share\*`).

6. Als u een bepaald type object van scans wilt uitsluiten, voert u in het veld **Soorten gedetecteerde objecten** 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 uitzonderingen.

8. Selecteer in het blok **Beschermingsonderdelen** de componenten waarop u de scanuitzondering wilt toepassen.

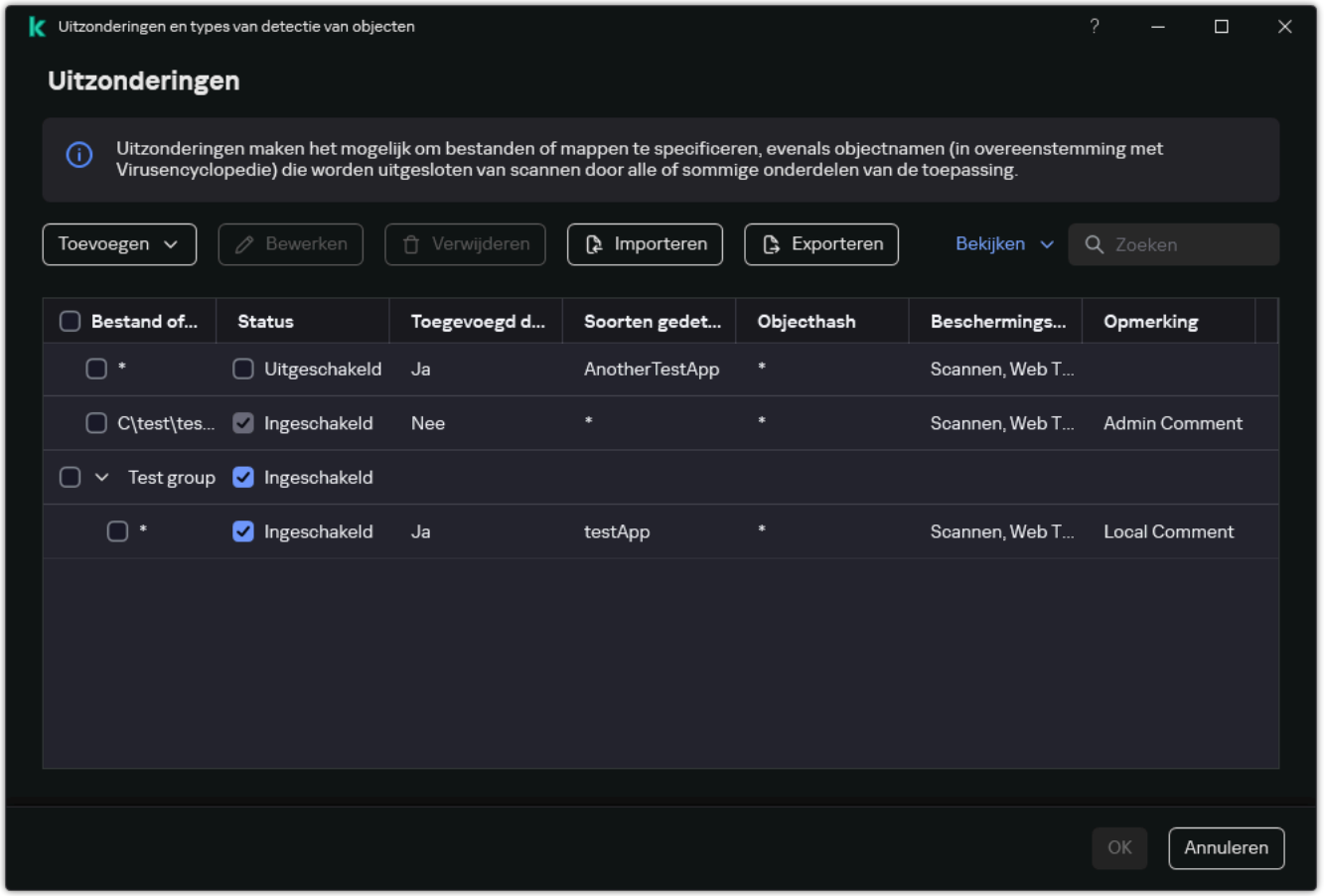
9. Typ indien nodig in het veld **Opmerking** een korte opmerking over de scanuitzondering die u maakt.

10. Selecteer de status **Actief** voor de uitzondering.

11. Klik op **Toevoegen**.

    De nieuwe uitzondering wordt aan de lijst toegevoegd. U kunt de uitzondering op elk moment stoppen met behulp van het selectievakje in de kolom **Status**.

12. Sla uw wijzigingen op.



Lijst met uitzonderingen

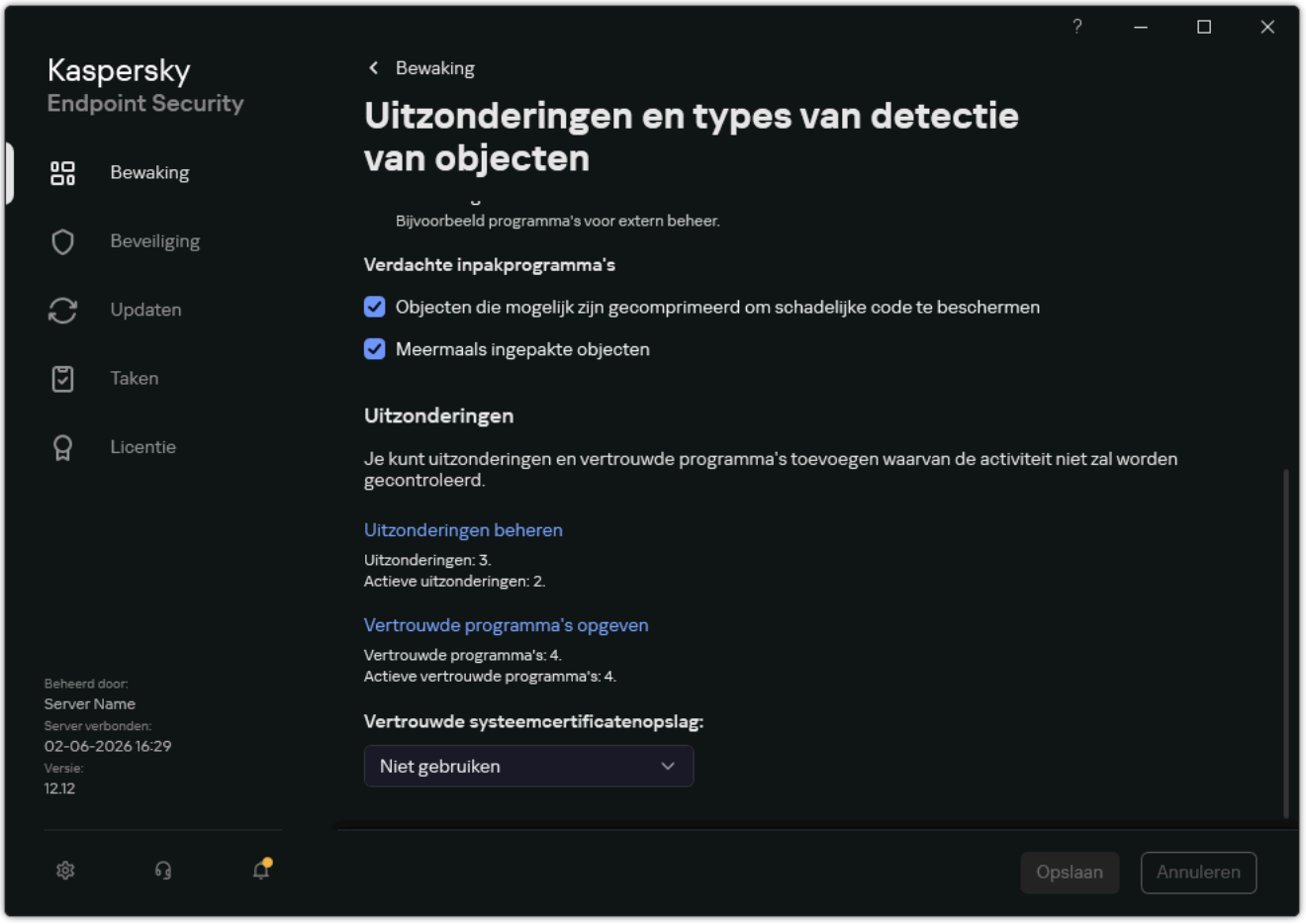
Een programma toevoegen aan de lijst met lokale vertrouwde programma's in het programma-interface

1. Klik in het hoofdvenster van het programma op de knop ⚙.

2. Selecteer **Algemene instellingen** → **Uitzonderingen en types van detectie van objecten** in het venster met de programma-instellingen.

3. Klik in het blok **Uitzonderingen** op de koppeling **Vertrouwde programma's opgeven**.

Kaspersky Endpoint Security verbergt de geconsolideerde lijst met vertrouwde programma's in de gebruikersinterface van het programma als het instellen van vertrouwde programma's geblokkeerd is door de beheerder in de console ("gesloten slot"-symbool) en lokale vertrouwde programma's zijn verboden (het selectievakje **Gebruik van lokale vertrouwde programma's toestaan** is uitgeschakeld).



Instellingen van uitzonderingen

4. Klik **Toevoegen** en selecteer een actie:

- **Categorie**. U kunt vertrouwde programma's in afzonderlijke categorieën groeperen. Om een nieuwe categorie aan te maken, voer de naam van de categorie in en voeg ten minste één vertrouwd programma toe aan de categorie.
- **Nieuwe uitzondering**. Kaspersky Endpoint Security voegt een nieuw vertrouwd programma toe aan de hoofdmap van de lijst.
- **Selecteer uitzonderingen uit lijst**. Om Kaspersky Endpoint Security snel te configureren op SQL-servers, Microsoft Exchange-servers en System Center Configuration Manager, bevat het programma: *vooraf gedefinieerde vertrouwde programma's*. Er zijn ook vooraf gedefinieerde vertrouwde programma's toegevoegd om de installatie van progromma's in virtuele Citrix- en VMware-omgevingen te ondersteunen. Afhankelijk van het doel van de beveiligde server moet u vooraf gedefinieerde vertrouwde programma's selecteren.

Als u een nieuwe vertrouwd programma aan een specifieke categorie wilt toevoegen, schakel het selectievakje naast die categorie in en selecteer de optie **Nieuwe uitzondering**.

5. Selecteer de vertrouwenscriteria:

- **Gebruik het volledige procespad op de schijf om het als vertrouwd te beschouwen**. Voer het pad naar het uitvoerbare bestand van het vertrouwde programma in.

  Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de `*` en `?`-tekens bij het invoeren van een masker.

  Kaspersky Endpoint Security behandelt de bestandsnaam van een vertrouwd programma als hoofdlettergevoelig. Als de bestandsnaam die u invoert de verkeerde naam heeft, herkent Kaspersky Endpoint Security het vertrouwde programma niet.

- **Gebruik procesbestandshash om het als vertrouwd te beschouwen**.

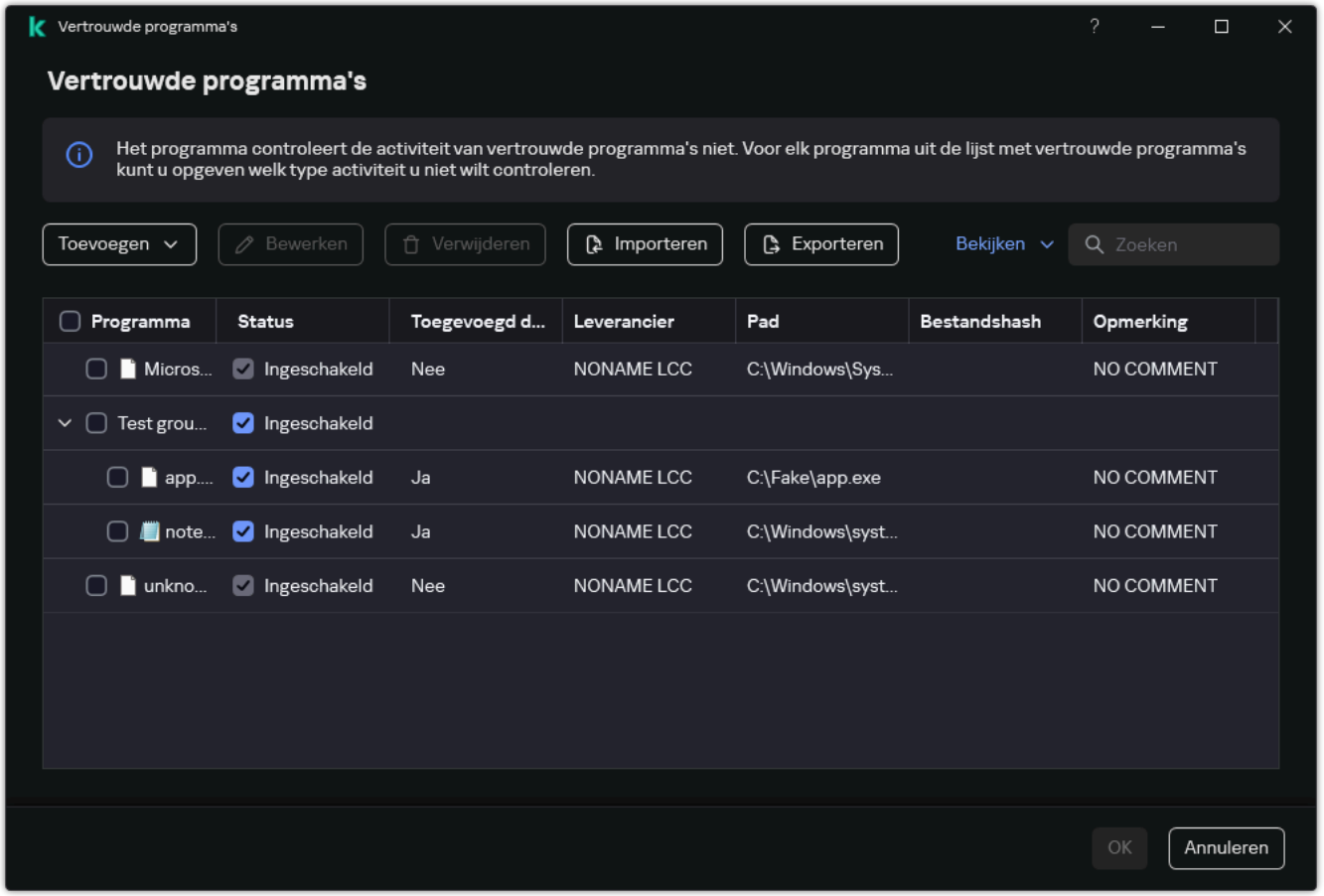
> Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en converteert het pad in de lokale interface van het programma. Als u met andere woorden het bestandspad `%userprofile%\Documents\File.exe` opent, wordt een record `C:\Users\Fred123\Documents\File.exe` toegevoegd aan lokale interface van 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.

7. Klik op **OK**.

   De nieuwe vertrouwde programma wordt aan de lijst toegevoegd. U kunt op elk moment een programma uitsluiten van de vertrouwde zone met behulp van het selectievakje in de kolom **Status**.

8. Sla uw wijzigingen op.



Lijst met vertrouwde programma's

De vertrouwde zone importeren en exporteren

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 vertrouwde zone bestaat uit de volgende lijsten: *scanuitzonderingen* en *vertrouwde programma's*. U kunt deze lijsten exporteren naar XML-bestanden en andere indelingen. 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 en de lijst met vertrouwde programma's of om de lijst naar een andere server te migreren.

Het programma gebruikt de volgende indelingen voor het exporteren en importeren van de *lijst met uitzonderingen*:

- XML is beschikbaar in de Beheerconsole (MMC), Webconsole en Cloudconsole.
- DAT is alleen beschikbaar voor import in de Beheerconsole (MMC). Het doel van deze indeling is het behouden van compatibiliteit met oudere versies van het programma. U kunt een DAT-bestand converteren naar XML in mmc (Beheerconsole) om lijsten met uitzonderingen naar de Webconsole te migreren.
- CSV is alleen beschikbaar op de lokale interface van het programma.

Kaspersky Endpoint Security gebruikt de XML-indeling voor het exporteren en importeren van de *lijst met vertrouwde programma's*.

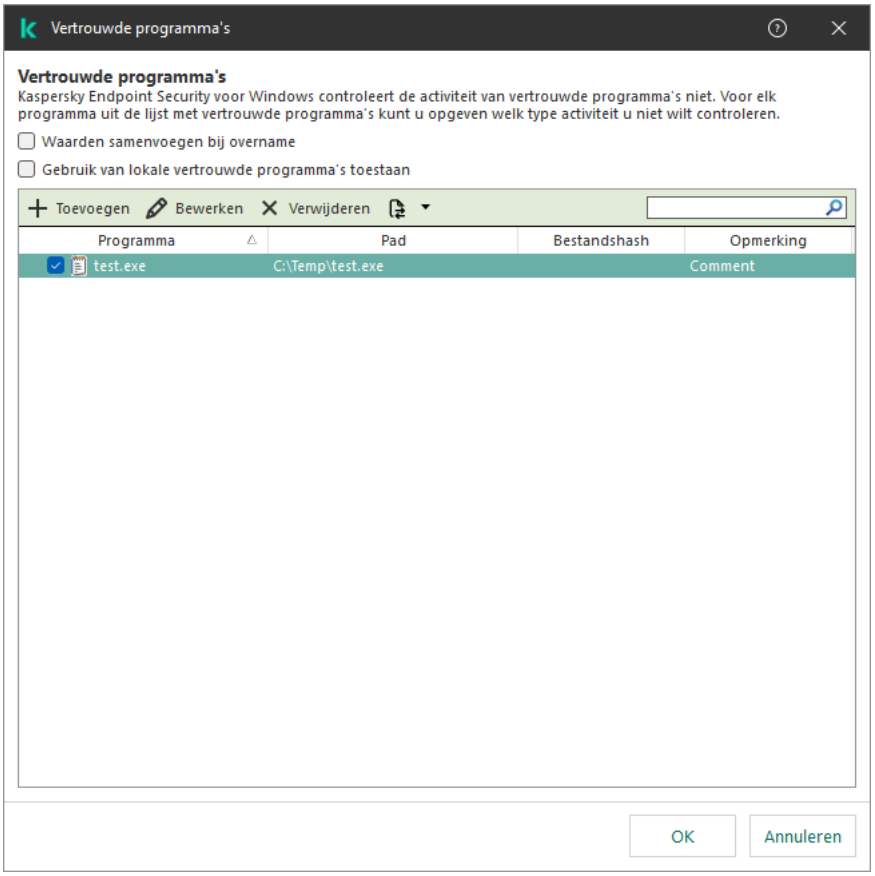
De vertrouwde zone exporteren en importeren in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Algemene instellingen** → **Uitzonderingen en objecttypen** in het beleidsvenster.
4. Onder **Scanuitzonderingen en vertrouwde programma's**, selecteer het onderdeel van de vertrouwde zone dat u wilt exporteren of importeren: **Scanuitzonderingen** of **Vertrouwde programma's**.
5. Klik op **Instellingen**.
6. 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 knop → **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. Kaspersky Endpoint Security ondersteunt ook het exporteren van de lijst met regels naar een DAT-bestand.



Lijst met vertrouwde programma's

7. De lijst met uitzonderingen importeren:

   a. Klik op de knop → **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. Kaspersky Endpoint Security ondersteunt ook het importeren van een lijst met uitzonderingen uit een DAT-bestand.

8. Sla uw wijzigingen op.

De vertrouwde zone exporteren en importeren in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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 het gedeelte **Trusted Zone**.

5. De lijst met regels exporteren:

   a. Klik op de koppeling **Malware Scan exclusions**.

   b. Selecteer de uitzonderingen die u wilt exporteren.

   c. Klik op de knop → **Export**.

      Kaspersky Endpoint Security exporteert de lijst met uitzonderingen naar een JSON-bestand in de standaard downloadmap.

6. Zo exporteert u de lijst met vertrouwde programma's:

   a. Selecteer de vertrouwde programma's in de lijst die u wilt exporteren.

   b. Klik op de knop → **Export**.

      Kaspersky Endpoint Security exporteert de lijst met vertrouwde programma's naar een JSON-bestand in de standaard downloadmap.

7. De lijst met uitzonderingen importeren:

   a. Klik op de koppeling **Malware Scan exclusions**.

   b. Klik op de knop → **Import**.

      Selecteer in het geopende venster het JSON-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 JSON-bestand.

8. Een lijst met vertrouwde programma's importeren:

   a. Klik op de koppeling **Applications**.

   b. Klik op de knop → **Import**.

      Dit opent een venster; Selecteer in dat venster het JSON-bestand waaruit u de lijst met vertrouwde programma's wilt importeren.

   c. Open het bestand.

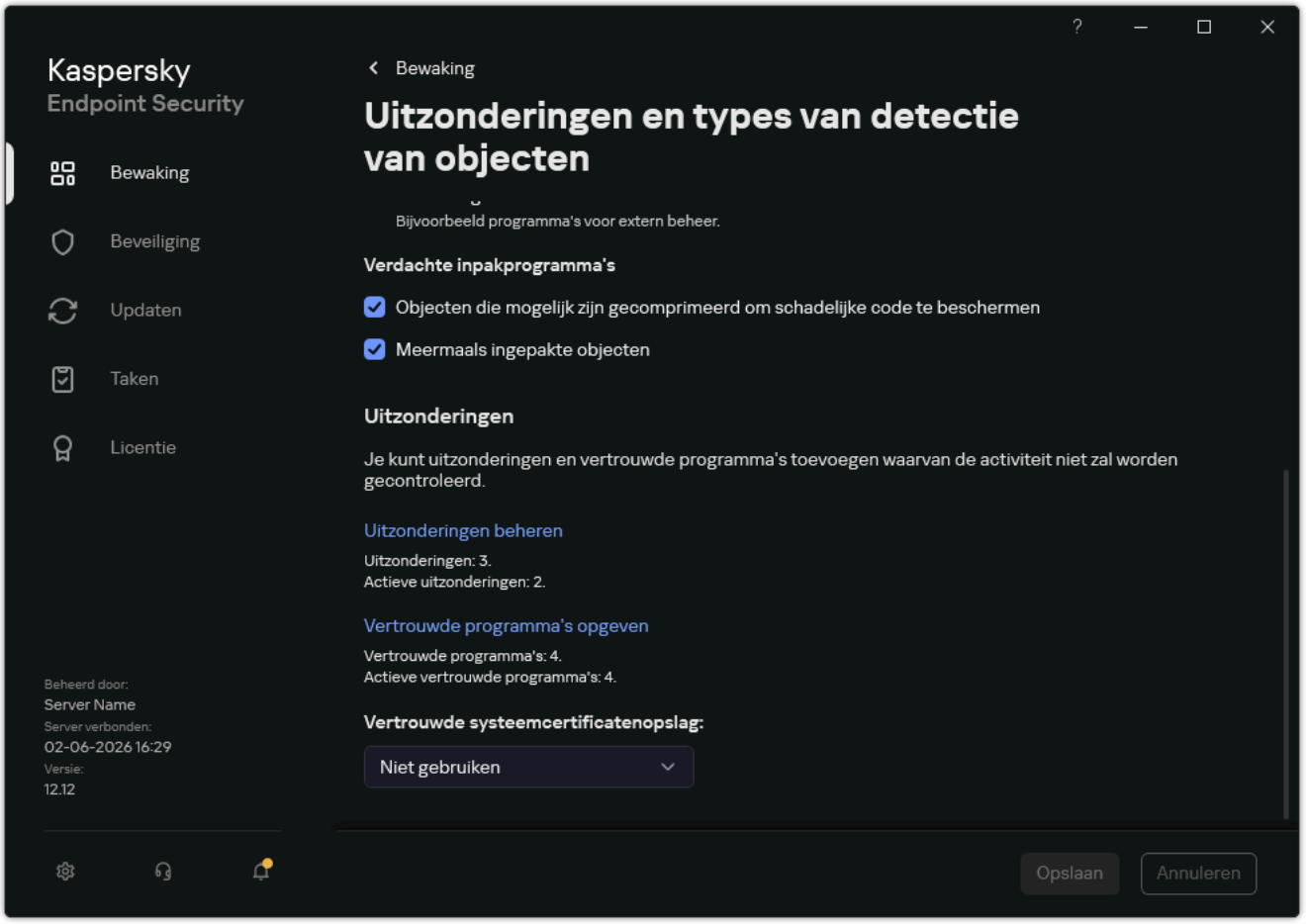
      Als de computer al een lijst met vertrouwde programma's heeft, vraagt Kaspersky Endpoint Security u of u de bestaande lijst wilt verwijderen of u er nieuwe items aan wilt toevoegen vanuit het JSON-bestand.

9. Sla uw wijzigingen op.

De vertrouwde zone exporteren of importeren in de programma-interface

1. Klik in het hoofdvenster van het programma op de knop ⚙.

2. Selecteer **Algemene instellingen** → **Uitzonderingen en types van detectie van objecten** in het venster met de programma-instellingen.



Instellingen van uitzonderingen

3. De lijst met regels exporteren:

   a. Klik in het blok **Uitzonderingen** op de koppeling **Uitzonderingen beheren**.

   b. Selecteer de uitzonderingen die u wilt exporteren.

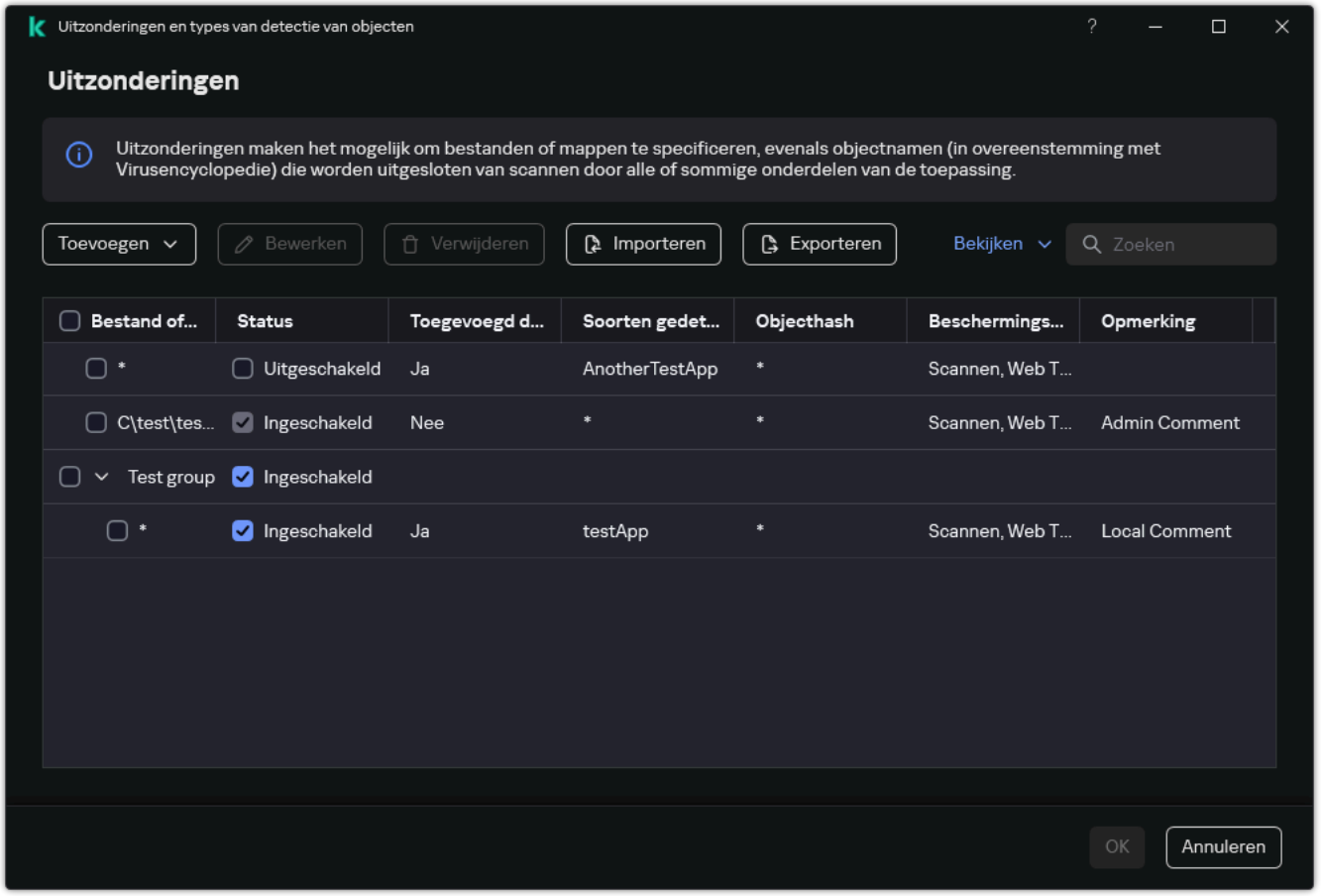
   c. Klik op **Exporteren**.

d. Bevestig dat u alleen de geselecteerde uitzonderingen wilt exporteren of de volledige lijst met uitzonderingen wilt exporteren.

e. Geef in het geopende venster de naam van het CSV-bestand op waarnaar u de lijst met uitzonderingen 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 uitzonderingen naar het CSV-bestand.



Lijst met uitzonderingen

4. Zo exporteert u de lijst met vertrouwde programma's:

a. Klik in het blok **Uitzonderingen** op de koppeling **Vertrouwde programma's opgeven**.

b. Selecteer de vertrouwde programma's in de lijst die u wilt exporteren.

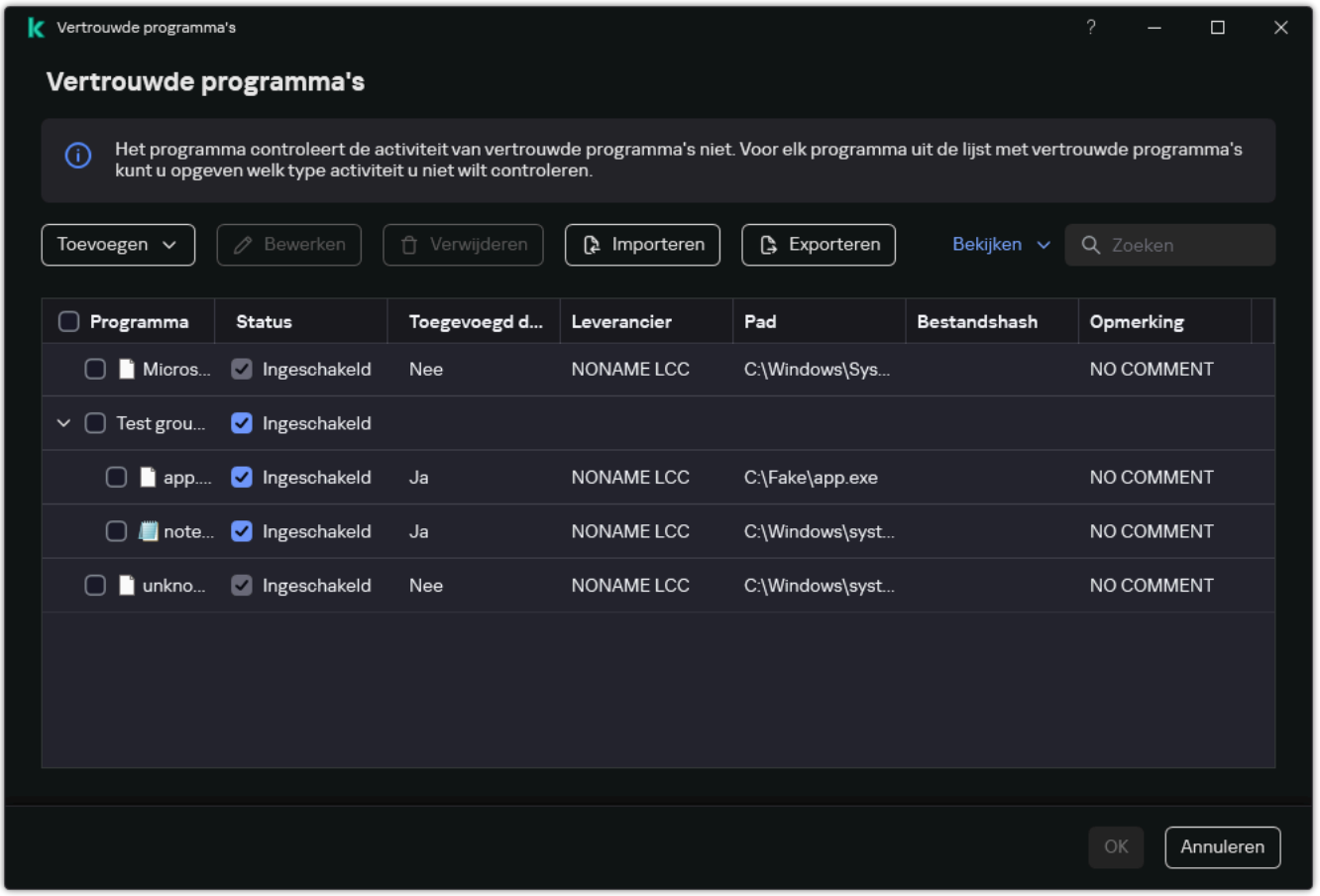
c. Klik op **Exporteren**.

d. Bevestig dat u alleen de geselecteerde vertrouwde programma's wilt exporteren of de volledige lijst wilt exporteren.

e. Dit opent een venster; Voer in het venster dat opent de naam in van het XML-bestand waarnaar u de lijst met vertrouwde programma's 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 vertrouwde programma's naar het XML-bestand.



Lijst met vertrouwde programma's

5. De lijst met uitzonderingen importeren:

a. Klik in het blok **Uitzonderingen** op de koppeling **Uitzonderingen beheren**.

b. Klik op **Importeren**.

c. Selecteer in het geopende venster het CSV-bestand waaruit u de lijst met uitzonderingen wil importeren.

d. 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 CSV-bestand.

6. Een lijst met vertrouwde programma's importeren:

a. Klik in het blok **Uitzonderingen** op de koppeling **Vertrouwde programma's opgeven**.

b. Klik op **Importeren**.

c. Dit opent een venster; Selecteer in dat venster het XML-bestand waaruit u de lijst met vertrouwde programma's wilt importeren.

d. Open het bestand.

Als de computer al een lijst met vertrouwde programma's heeft, vraagt Kaspersky Endpoint Security u of u de bestaande lijst wilt verwijderen of u er nieuwe items aan wilt toevoegen vanuit het XML-bestand.

7. Sla uw wijzigingen op.

Programma's met een vertrouwde digitale handtekening 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*.

Het gebruik van een vertrouwde opslag van systeemcertificaten in de Beheerconsole (MMC) starten

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Algemene instellingen** → **Uitzonderingen en objecttypen** in het beleidsvenster.
4. Schakel in het blok **Vertrouwde systeemcertificatenopslag** het selectievakje **Vertrouwde systeemcertificatenopslag gebruiken** in.
5. Selecteer in de vervolgkeuzelijst welke systeemopslag moet worden beschouwd als vertrouwd door Kaspersky Endpoint Security.
6. Sla uw wijzigingen op.

Het gebruik van een vertrouwde opslag van systeemcertificaten in de Webconsole en Cloudconsole starten

1. Selecteer in het hoofdvenster van de Webconsole het tabblad **Asset management** → **Policies**.
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 het gedeelte **Trusted Zone**.
5. Klik in het venster op de link **Root certificates**.
6. Selecteer in het venster dat opent het selectievakje **Use trusted system certificate store**.
7. Selecteer welke systeemopslag moet worden beschouwd als vertrouwd door Kaspersky Endpoint Security.
8. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Het gebruik van een vertrouwde opslag van systeemcertificaten in de programma-interface starten

1. Klik in het hoofdvenster van het programma op de knop ⚙.
2. Selecteer **Algemene instellingen** → **Uitzonderingen en types van detectie van objecten** 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.

Appendix. Vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's

Beginnend met Kaspersky Endpoint Security 12.6 voor Windows, uitzonderingen scannen en vertrouwde programma's worden toegevoegd aan de vertrouwde zone. Vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's helpen bij het snel configureren van Kaspersky Endpoint Security op SQL-servers, Microsoft Exchange-servers en System Center Configuration Manager. Dit betekent dat u niet handmatig een vertrouwde zone voor het programma op servers hoeft in te stellen. Vanaf Kaspersky Endpoint Security 12.8 voor Windows kun je het programma in Light Agent-modus installeren om virtuele omgevingen te beschermen. Met voorgedefinieerde uitzonderingen van scans en vertrouwde programma's kunt u Kaspersky Endpoint Security snel configureren in Citrix- en VMware-virtuele omgevingen.

U kunt op de volgende manieren vooraf gedefinieerde uitzonderingen en vertrouwde programma selecteren:

- Het programma installeren.
  - Het programma lokaal met de wizard installeren
  - Eigenschappen van installatiepakket
- Het beleid bepalen.
  - Nieuwe beleidswizard
  - Beleidseigenschappen: scanuitzonderingen en vertrouwde programma's

SQL-server

Wanneer u Kaspersky Endpoint Security op een SQL-server installeert, moet u een vertrouwde zone maken van vooraf gedefinieerde uitzonderingen en vertrouwde programma's om ervoor te zorgen dat de werking van de server niet wordt verstoord.

Vooraf gedefinieerde scanuitzonderingen

Pad	SQL-versie
%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.mdf	2012 2014 2016 2017 2019 2022
%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?*\Data*.mdf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.mdf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.ldf	2012 2014 2016 2017 2019 2022
%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL??.*\MSSQL\DATA*.mdf	2012 2014 2016 2017 2019 2022
%ProgramFiles%\Microsoft SQL Server\MSSQL??.**\MSSQL\DATA*.ldf	2012 2014 2016 2017 2019 2022

Microsoft Exchange-server

Wanneer u Kaspersky Endpoint Security op een Microsoft Exchange-server installeert, moet u een vertrouwde zone maken van vooraf gedefinieerde uitzonderingen en vertrouwde programma's om ervoor te zorgen dat de werking van de server niet wordt verstoord.

Vooraf gedefinieerde scanuitzonderingen

Pad	Microsoft Exchange-versie
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Chk	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Edb	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Jrs	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.log	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Que	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.jsl	2013 2016 2019

Pad	Microsoft Exchange-versie
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Chk	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Edb	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Jrs	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.log	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Que	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.jsl	2013 2016 2019

Vooraf gedefinieerde vertrouwde programma's

Pad	Microsoft Exchange-versie
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\EdgeTransport.exe	2013 2016 2019
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\MSExchangeFrontendTransport.exe	2013 2016 2019

System Center Configuration Manager

Vooraf gedefinieerde scanuitzonderingen

Pad	System Center Configuration Manager-versie
%ProgramFiles%\Microsoft Configuration Manager\Inboxes	2012 2012 R2

Citrix

Wanneer u Kaspersky Endpoint Security in een virtuele Citrix-omgeving, moet u een vertrouwde zone maken van vooraf gedefinieerde uitzonderingen en vertrouwde programma's om ervoor te zorgen dat de werking van de server niet wordt verstoord.

Vooraf gedefinieerde scanuitzonderingen

Pad
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName_log.ldf

Pad
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName_log.ldf
%ProgramData%\Citrix\Broker\Cache
%SystemRoot%\System32\drivers\CtxUvi.sys
%ProgramFiles%\Citrix\HDX\bin\CitrixLogonCsp.dll
mcsdif.vhdx
%Temp%\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%Temp%\Citrix\HDXRTConnector**.txt
%SystemDrive%\Users*\AppData\Local\Temp\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%ProgramFiles(x86)%\Citrix\ICA Client\epclient32.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epclient64.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epinject.sys
%ProgramFiles(x86)%\Citrix\ICA Client\EntryProtect.dll
*.vhd
*.avhd
*.vhdx
*.avhdx
*.pvp
*.lok
%SystemRoot%\System32\drivers\CVhdMp.sys (Windows Server 2012 R2)
%SystemRoot%\System32\drivers\CfsDep2.sys
%ProgramData%\Citrix\Provisioning Services\Tftpboot\ARDBP32.BIN
.vdiskcache
vdiskdif.vhdx
%SystemRoot%\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore**\PersistentDictionary.edb

Pad	Citrix-oplossing
%ProgramFiles%\Citrix\Broker\Service\BrokerService.exe	Virtual Apps and Desktops
%ProgramFiles%\Microsoft SQL Server\150\LocalDB\Binn\sqlservr.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\Broker\Service\HighAvailabilityService.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\ConfigSync\ConfigSyncService.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\User Profile Manager\UserProfileManager.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\Virtual Desktop Agent\BrokerAgent.exe	Virtual Apps and Desktops
%SystemRoot%\System32\drivers\CVhdFilter.sys	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\ICAService\CtxSvcHost.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\System32\ctxgfx.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\ICAService\picaSvc2.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\ICAService\CpSvc.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\CtxSvcHost.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\picaSvc2.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\CpSvc.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\System32\WebSocketService.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\ICAService\WebSocketService.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\HDX\bin\WebSocketService.exe	Virtual Apps and Desktops

Pad	Citrix-oplossing
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\AudioTranscoder.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngine.Net.Service.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngineService.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\ICA Client\MediaEngineService.exe	Werkruimte app
%ProgramFiles(x86)%\Citrix\ICA Client\CDViewer.exe	Werkruimte app
%ProgramFiles(x86)%\Citrix\ICA Client\concentr.exe	Werkruimte app
%ProgramFiles(x86)%\Citrix\ICA Client\wfica32.exe	Werkruimte app
%ProgramFiles(x86)%\Citrix\ICA Client\bgblursvc.exe	Werkruimte app
%ProgramFiles(x86)%\Citrix\ICA Client\AuthManager\AuthManSvr.exe	Werkruimte app
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfService.exe	Werkruimte app
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfServicePlugin.exe	Werkruimte app
%ProgramFiles(x86)%\Citrix\ICA Client\HdxRtcEngine.exe	Werkruimte app
%ProgramFiles(x86)%\Citrix\ICA Client\HdxTeams.exe	Werkruimte app
%ProgramFiles%\Citrix\Provisioning Services\BNTFTP.EXE	Voorziening
%ProgramFiles%\Citrix\Provisioning Services\PVSTSB.EXE	Voorziening
%ProgramFiles%\Citrix\Provisioning Services\StreamService.exe	Voorziening
%ProgramFiles%\Citrix\Provisioning Services\StreamProcess.exe	Voorziening
%ProgramFiles%\Citrix\Provisioning Services\soapserver.exe	Voorziening
%ProgramFiles%\Citrix\Provisioning Services\Inventory.exe	Voorziening
%ProgramFiles%\Citrix\Provisioning Services\Notifier.exe	Voorziening
%ProgramFiles%\Citrix\Provisioning Services\MgmtDaemon.exe	Voorziening
%ProgramFiles%\Citrix\Provisioning Services\BNPXE.exe	Voorziening
%ProgramFiles%\Citrix\Provisioning Services\CdfSvc.exe	Voorziening
%ProgramFiles%\Citrix\Provisioning Services\BNAbsService.exe	Voorziening
%SystemRoot%\System32\drivers\bnistack6.sys	Voorziening
%SystemRoot%\System32\drivers\CfsDep2.sys	Voorziening
%SystemRoot%\System32\drivers\cnicteam.sys	Voorziening
%ProgramFiles%\Citrix\Provisioning Services\BNDevice.exe	Voorziening
%ProgramFiles%\Citrix\Provisioning Services\drivers\BNIstack6.sys	Voorziening
%ProgramFiles%\Citrix\Provisioning Services\drivers\CNicTeam.sys	Voorziening
%ProgramFiles%\Citrix\Provisioning Services\drivers\CFsDep2.sys	Voorziening

Pad	Citrix-oplossing
%ProgramFiles%\Citrix\Provisioning Services\drivers\CVhdMp.sys	Voorziening
%ProgramFiles%\Citrix\Receiver StoreFront\Services\SubscriptionsStoreService\Citrix.DeliveryServices.SubscriptionsStore.ServiceHost.exe	StoreFront
%ProgramFiles%\Citrix\Receiver StoreFront\Services\CredentialWallet\Citrix.DeliveryServices.CredentialWallet.ServiceHost.exe	StoreFront

VMware

Wanneer u Kaspersky Endpoint Security in een virtuele VMware-omgeving, moet u een vertrouwde zone maken van vooraf gedefinieerde vertrouwde programma's om ervoor te zorgen dat de werking van de server niet wordt verstoord.

Vooraf gedefinieerde vertrouwde programma's

Pad	VMware-oplossing
C:\Program Files\VMware\VMware View\Agent\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\wsnm_jms.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\ws_scripthost.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastS.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastW.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\SecurityGateway.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\x64\pcoip_server_win32.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\pcoip_server_win32.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\Scanner.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\tsdrvdisvc.dll	Horizon
C:\Program Files\VMware\VMware View\Server\appblastgateway\nssm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\SecurityGateway.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_TunnelService.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_SecurityServer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmUpdateLauncher.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-appstub.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-view.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-helper.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-previewer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-redir-client.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-remotemks.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-view-usbloader.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\ClientService\horizon_client_service.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\DCT\ws_diag.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\cef\HTML5VideoPlayer.exe	Horizon

Pad	VMware-oplossing
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib64.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib64.exe	Horizon
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlping.exe	Horizon
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlsv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\diagutil.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\ftscanmgrhv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\scan.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\scan64.exe	Horizon
C:\Program Files\Common Files\VMware\SerialPortRedirection\Client\vmwsprrdpwks.exe	Horizon

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.14.1\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. Klik in het venster met de programma-instellingen onder **Algemene instellingen** op de tegel **Rapporten en Opslag**.



Back-upinstellingen

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. Klik in het venster met de programma-instellingen onder **Algemene instellingen** op de tegel **Rapporten en Opslag**.



Back-upinstellingen

3. Schakel in het blok **Back-up** het selectievakje **Beperk de grootte van Back-up tot N MB** in. Als het selectievakje is ingeschakeld, is de maximale opslaggrootte beperkt tot de opgegeven waarde. De maximale grootte is standaard 1024 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.

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 *Niet gedesinfecteerd* eraan toe, plaatst het een kopie ervan in Back-up en probeert 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 verwijderd 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 het besturingssysteem (raadpleeg de Help-bestanden van Microsoft Windows voor informatie over het herstel van een programma uit de Windows Store).

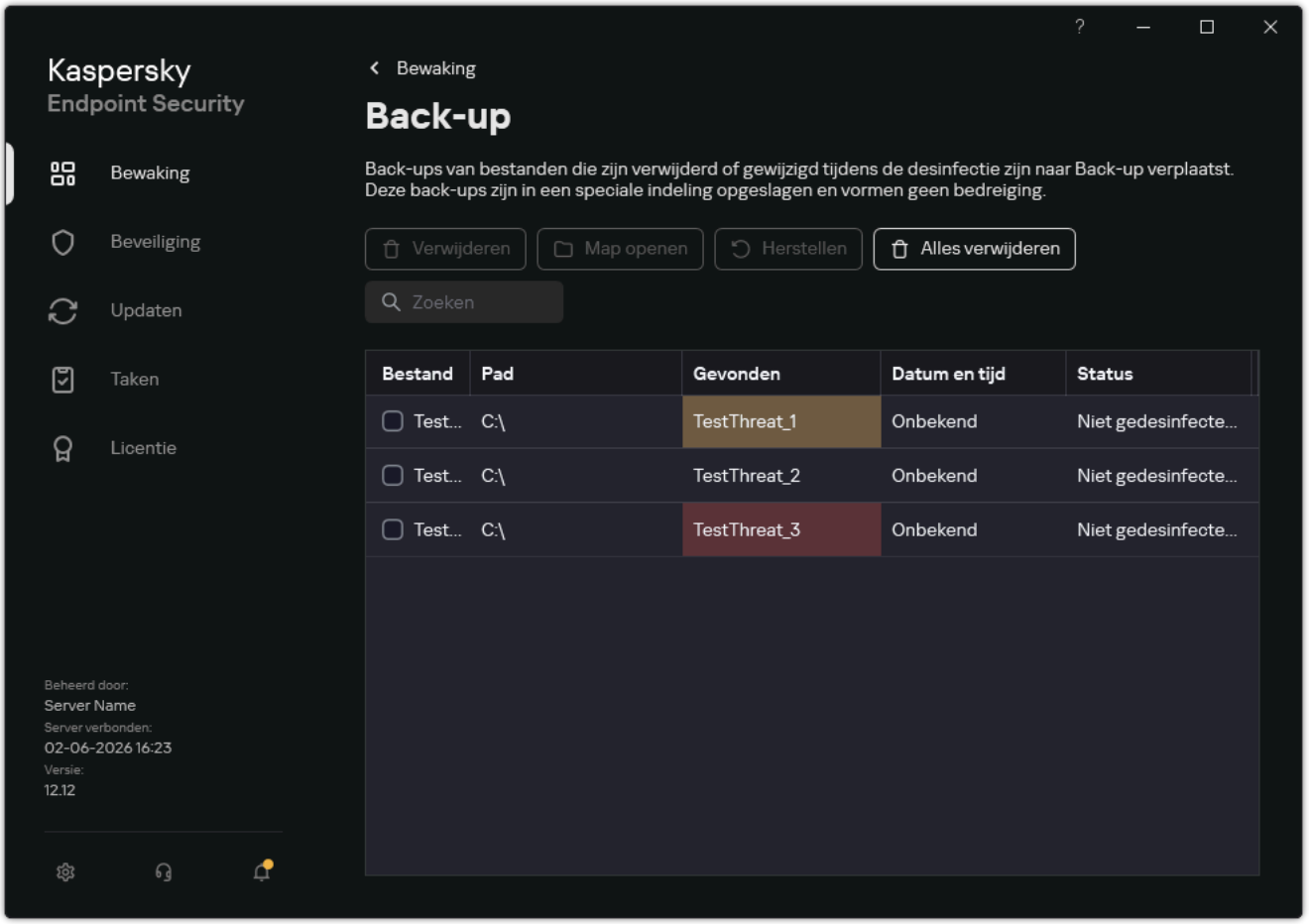
De back-ups van bestanden worden als een tabel voorgesteld. Voor een back-up van een bestand wordt het pad naar de oorspronkelijke map van het bestand weergegeven. Het pad naar de oorspronkelijke map van het bestand bevat mogelijk persoonlijke gegevens.

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 in het hoofdvenster van het programma naar **Bewaking** 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-up

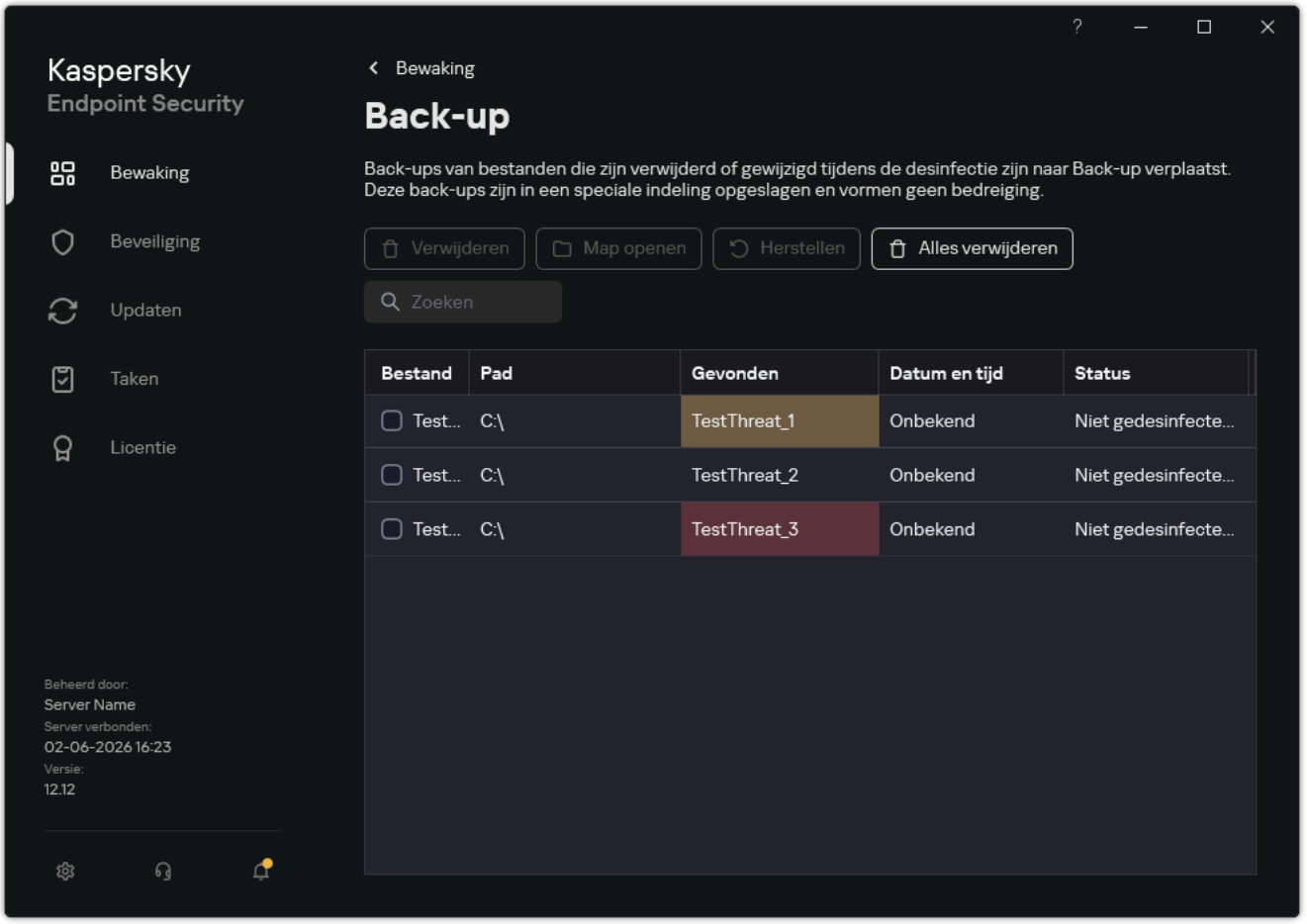
Back-ups van bestanden uit Back-up verwijderen

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 in het hoofdvenster van het programma naar **Bewaking** 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.



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.
- Sorteer gebeurtenissen van de service voor meldingen.
- Wijzig de volgorde en de reeks kolommen die in de lijst met gebeurtenissen van de service voor meldingen worden weergegeven.

Instellingen voor gebeurtenislogboeken configureren

Zo configureert u instellingen voor gebeurtenislogboeken:

1. 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 **Meldingen configureren**.

   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 `Application` 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 **Meldingen configureren**.

   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 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 **E-mailmeldingen configureren**.

   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.

   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 **Event selections** de optie **User requests**.

4. Selecteer het bericht dat u naar de beheerder hebt verstuurd.

5. Klik op de knop **Open event properties window** 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.14.1\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 **Systeemaudit**. Dit bevat informatie over gebeurtenissen tijdens de interactie tussen de gebruiker en het programma en tijdens de algemene werking van het programma die niets te maken hebben een specifieke onderdelen of taken van Kaspersky Endpoint Security.
- 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.
- Sorteer 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.

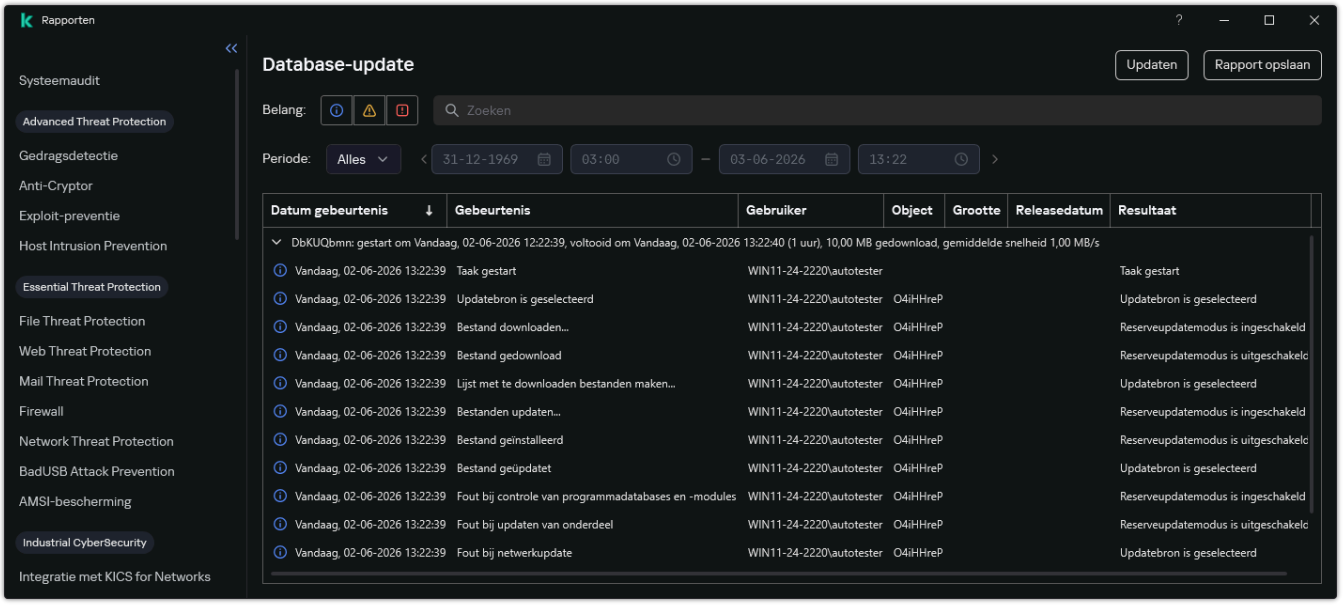
Als Kaspersky Endpoint Security wordt uitgevoerd onder beheer van Kaspersky Security Center, kan informatie over gebeurtenissen worden doorgestuurd naar de Kaspersky Security Center Administration Server (raadpleeg de Help van Kaspersky Security Center voor meer informatie).

Rapporten bekijken

Als een gebruiker rapporten kan bekijken, kan de gebruiker ook alle gebeurtenissen in de rapporten bekijken.

Zo bekijkt u rapporten:

1. Ga in het hoofdvenster van het programma naar **Bewaking** en klik op de tegel **Rapporten**.



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. Klik in het venster met de programma-instellingen onder **Algemene instellingen** op de tegel **Rapporten en Opslag**.



Rapportinstellingen

3. Als u de opslagduur van rapporten wilt beperken, schakelt u in het blok **Rapporten** het selectievakje **Bewaar rapporten niet langer dan N dagen** in. Definieer de maximale opslagduur voor rapporten.

4. Sla uw wijzigingen op.

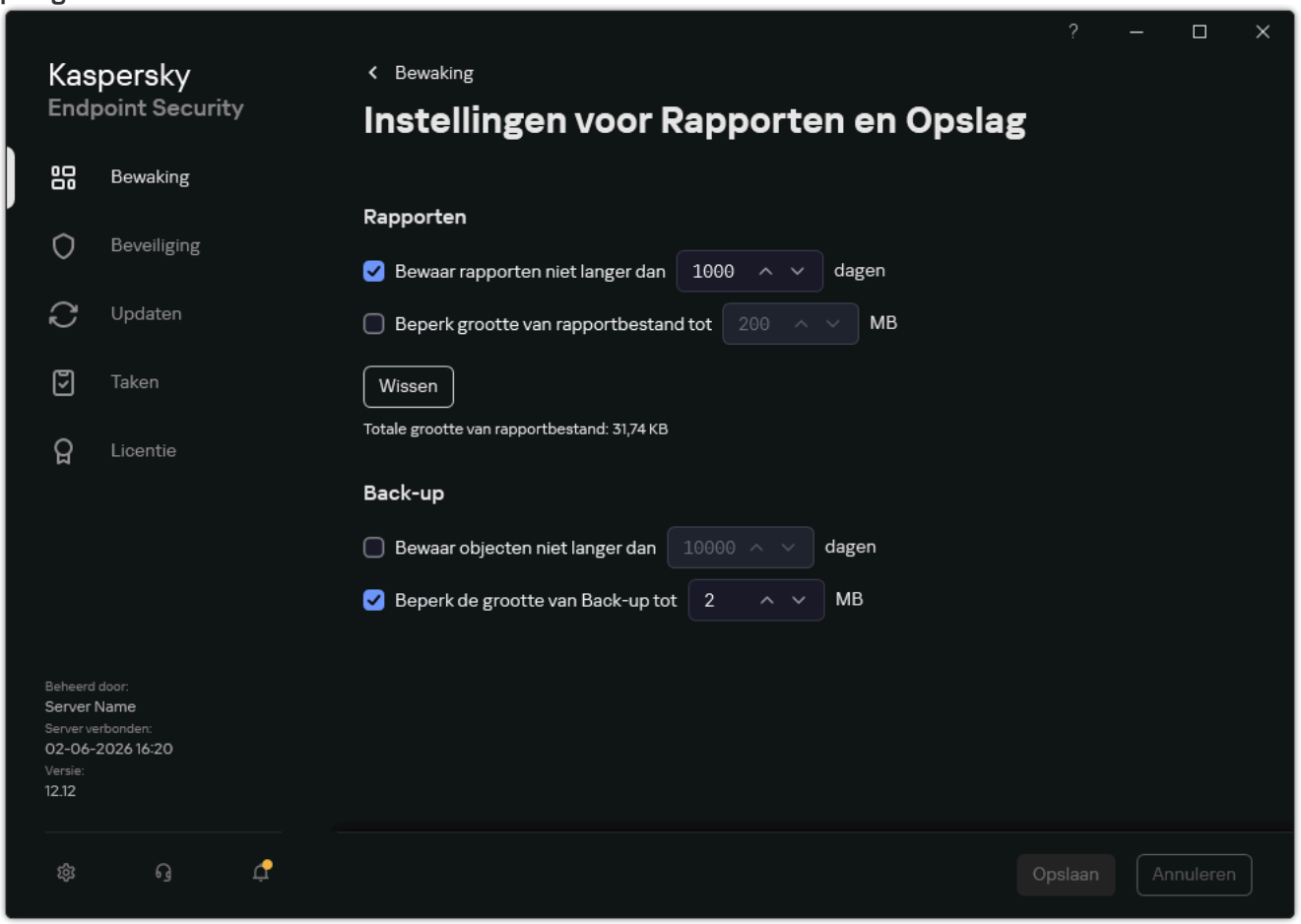
Maximale grootte van het rapportbestand configureren

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. Klik in het venster met de programma-instellingen onder **Algemene instellingen** op de tegel **Rapporten en Opslag**.



Rapportinstellingen

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

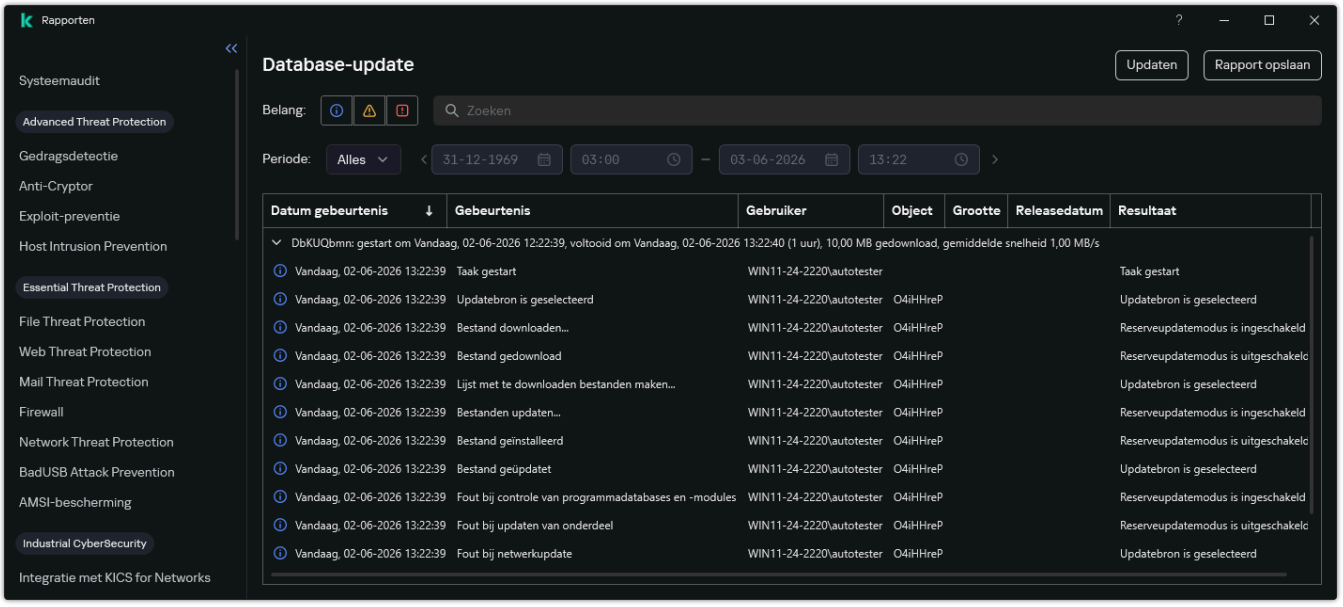
De gebruiker is persoonlijk verantwoordelijk voor het veilig houden van informatie dat vanuit een rapport is opgeslagen in een bestand, en in het bijzonder voor de controle en beperking van de toegang tot deze informatie.

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 in het hoofdvenster van het programma naar **Bewaking** en klik op de tegel **Rapporten**.



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. Klik in het venster met de programma-instellingen onder **Algemene instellingen** op de tegel **Rapporten en Opslag**.



Rapportinstellingen

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). Zelfbescherming omvat ook wachtwoordbeveiliging en Administration Server-verbindingsbeveiliging.

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).

Administration Server verbindingsbeveiliging voorkomt ongeoorloofde herverbinding van de computer met een niet-vertrouwde server.

Zelfbeschermingstechnologieën van Kaspersky Endpoint Security

Technologie	Beschrijving	x86 computer	x64 computer
Zelfbeschermingsmechanisme	De technologie blokkeert de toegang tot de volgende programmacomponenten: • bestanden in de Kaspersky Endpoint Security-installatiemap en andere bestanden van het programma; • registersleutels met records die bij het programma horen; • processen die het programma uitvoert.	✓	✓
AM-PPL (Antimalware Protected Process Light)	De technologie beschermt Kaspersky Endpoint Security-processen tegen schadelijke acties. Voor meer informatie over AM-PPL-technologie gaat u naar de website van Microsoft. AM-PPL-technologie is beschikbaar voor de besturingssystemen Windows 10 versie 1703 (RS2) of hoger en Windows Server 2019.	✓	✓
Verdedigingsmechanisme voor extern beheer	Deze technologie voorkomt dat andere programma's (bijvoorbeeld TeamViewer of RemotelyAnywhere) toegang krijgen tot Kaspersky Endpoint Security.	✓	– (behalve voor Windows 7)

Zelfbescherming inschakelen en uitschakelen

Kaspersky Endpoint Security voorkomt de wijziging of verwijdering van programmabestanden op de harde schijf, processen in het geheugen en vermeldingen in het systeemregister.

De technologie blokkeert de toegang tot de volgende programmacomponenten:

- bestanden in de Kaspersky Endpoint Security-installatiemap en andere bestanden van het programma;
- registersleutels met records die bij het programma horen;
- processen die het programma uitvoert.

Het mechanisme Zelfbescherming van Kaspersky Endpoint Security is standaard ingeschakeld.

Zelfbescherming in- of uitschakelen in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Algemene instellingen** → **Programma-instellingen** in het beleidsvenster.
4. Gebruik het selectievakje **Zelfbescherming inschakelen** om het zelfbeschermingsmechanisme in of uit te schakelen.
5. Sla uw wijzigingen op.

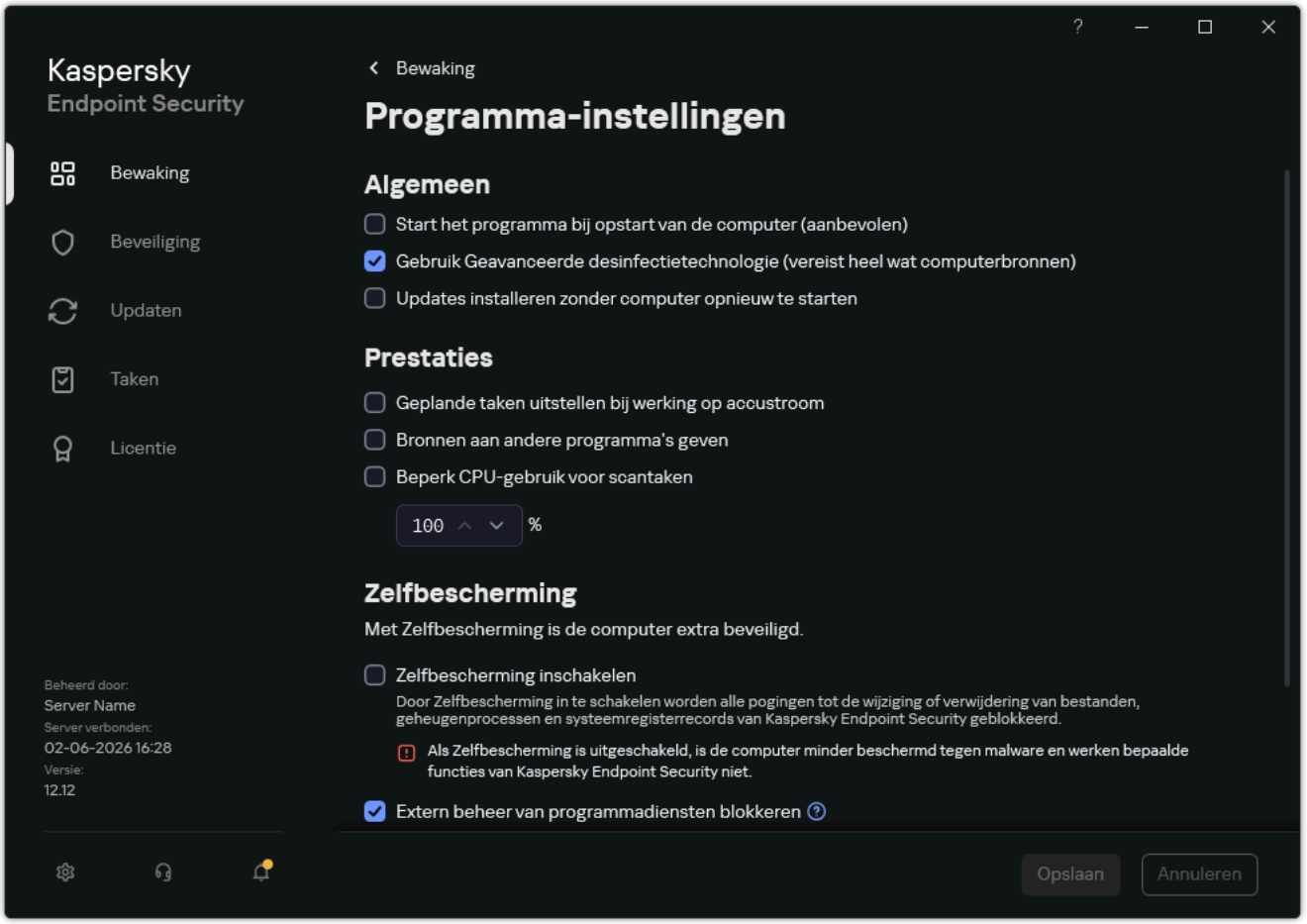
Hoe Zelfbescherming in- of uit te schakelen in de webconsole en cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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** → **Self-Defense**.
5. Gebruik de schakelaar **Self-Defense ENABLED** om het zelfbeschermingsmechanisme in of uit te schakelen.
6. Sla uw wijzigingen op.

Het onderdeel Zelfbescherming 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.



Instellingen Kaspersky Endpoint Security voor Windows

3. Gebruik het selectievakje **Zelfbescherming inschakelen** 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.

Gebruik de AM-PPL-technologie continu. AM-PPL is een belangrijk onderdeel van de bescherming van het besturingssysteem. Als u AM-PPL-ondersteuning uitschakelt, kunnen sommige functies van Kaspersky Endpoint Security falen (bijvoorbeeld de integratie van het programma met het Windows Security Center). Het uitschakelen van AM-PPL-ondersteuning is alleen toegestaan in een aparte testomgeving voor het oplossen van problemen.

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.

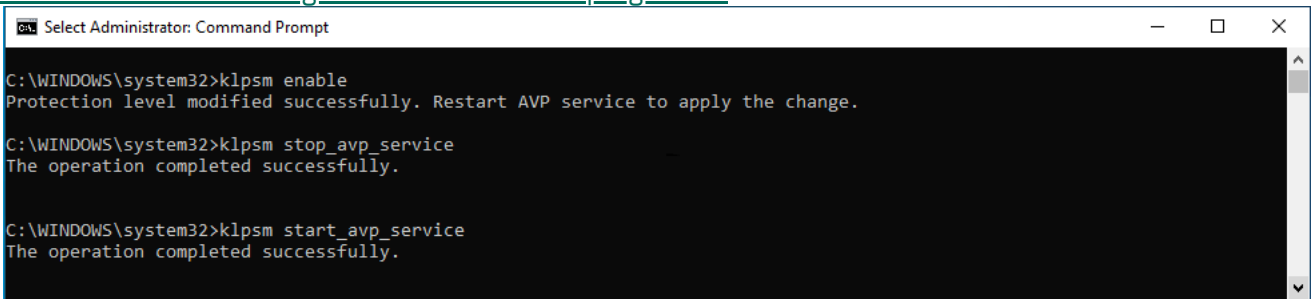
   U kunt het pad naar het uitvoerbare bestand toevoegen aan de systeemvariabele %PATH% tijdens programma installatie.

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.



Ondersteuning voor AM-PPL-technologie inschakelen

Bescherming van programmaservices tegen extern beheer

Bescherming van programmaservices tegen extern beheer blokkeert pogingen van gebruikers en andere programma's om Kaspersky Endpoint Security-services te stoppen. Bescherming verzekert de werking van de volgende diensten:

- Kaspersky Endpoint Security Service (AVP.KES.14.1)
- Kaspersky Seamless Update Service service (AVPSUS.KES.14.1)

Schakel de bescherming van Kaspersky Endpoint Security-services tegen extern beheer uit om het programma via de opdrachtregel af te sluiten.

U kunt extern beheer van programmaservices alleen toestaan op computers die de AM-PPL-technologie niet ondersteunen of op computers waarop de technologie is uitgeschakeld.

Bescherming van programmaservices tegen extern beheer in- of uitschakelen in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Algemene instellingen** → **Programma-instellingen** in het beleidsvenster.
4. Gebruik het **Extern beheer van programmadiensten blokkeren** om de bescherming van Kaspersky Endpoint Security-services tegen extern beheer in of uit te schakelen.
5. Sla uw wijzigingen op.

Hoe de bescherming van programmaservices tegen extern beheer in- of uitschakelen in de Webconsole en Cloudconsole

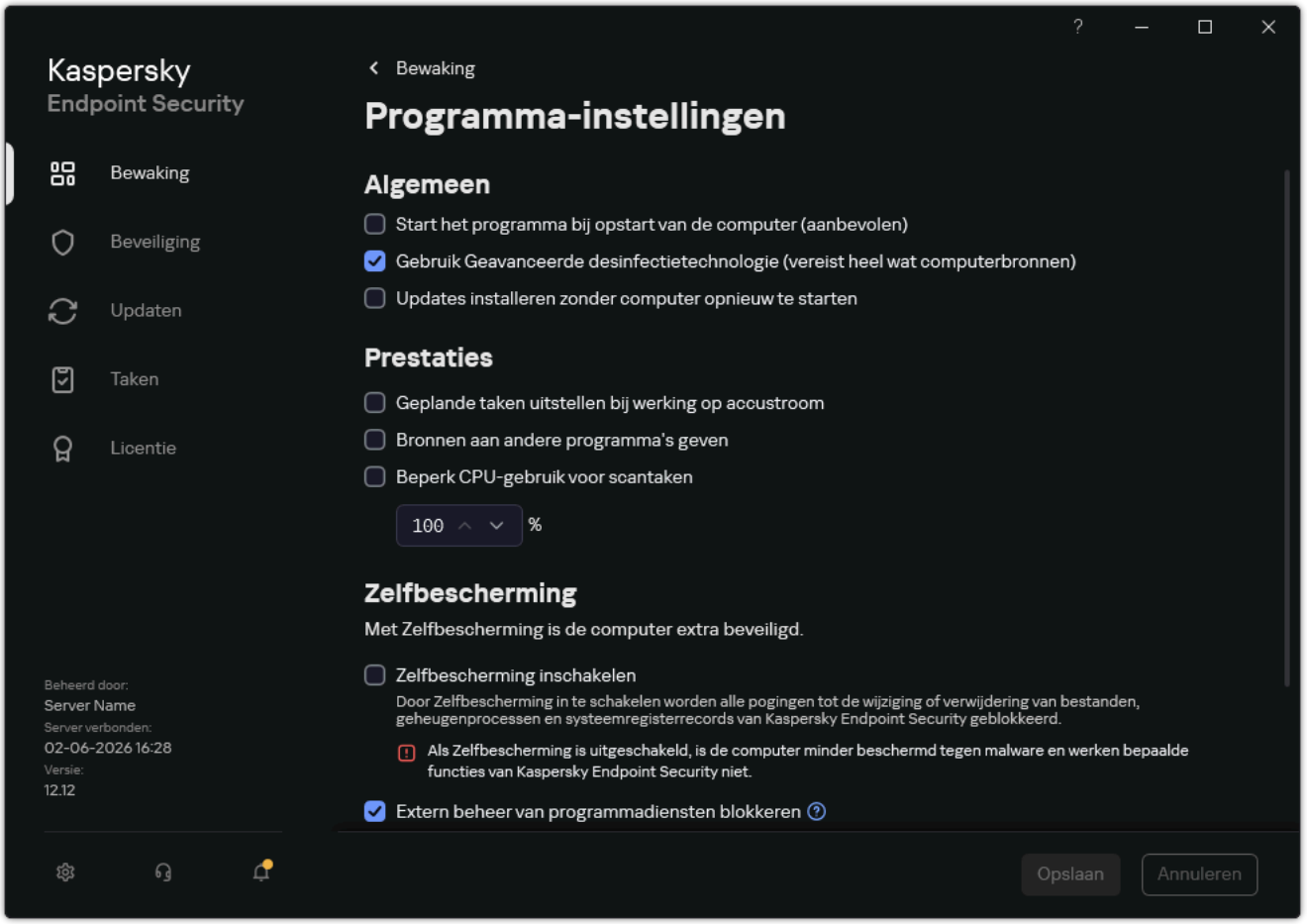
1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.

   U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **General Settings** → **Self-Defense**.
5. Gebruik het **Block external management of application services** om de bescherming van Kaspersky Endpoint Security-services tegen extern beheer in of uit te schakelen.
6. Sla uw wijzigingen op.

Bescherming van programmaservices tegen extern beheer in- of uitschakelen 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.

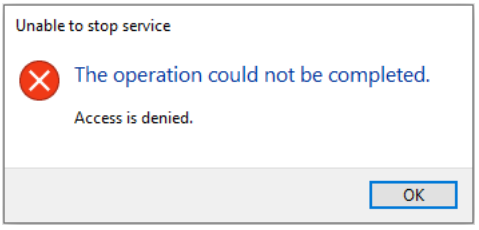


Instellingen Kaspersky Endpoint Security voor Windows

3. Gebruik het **Extern beheer van programmadiensten blokkeren** om de bescherming van Kaspersky Endpoint Security-services tegen extern beheer in of uit te schakelen.

4. Sla uw wijzigingen op.

Als gevolg hiervan verschijnt er een systeemvenster met een foutmelding wanneer een gebruiker programmaservices probeert te stoppen. De gebruiker kan alleen programmaservices beheren vanuit de Kaspersky Endpoint Security-interface.



Programmaservices toegangsfout

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** → **Uitzonderingen en types van detectie van objecten** in het venster met de programma-instellingen.
3. Klik in het blok **Uitzonderingen** op de koppeling **Vertrouwde programma's opgeven**.
4. Klik in het venster op de knop **Toevoegen**.
5. Selecteer het uitvoerbare bestand van de toepassing voor beheer op afstand.

   U kunt het pad ook handmatig verwijderen. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de `*` en `?`-tekens bij het invoeren van een masker.
6. Selecteer het selectievakje **Sta interactie met de interface van Kaspersky Endpoint Security toe**.
7. 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 of een handmatig toegevoegde account.

- 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.



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. 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.

- **Account handmatig toegevoegd**. Een account buiten het Active Directory-domein. U kunt dit service-account gebruiken in plaats van KLAdmin als u het beheerderswachtwoord niet wilt delen. U kunt elke gebruikersnaam en wachtwoord instellen en individuele machtigingen configureren.

- **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.

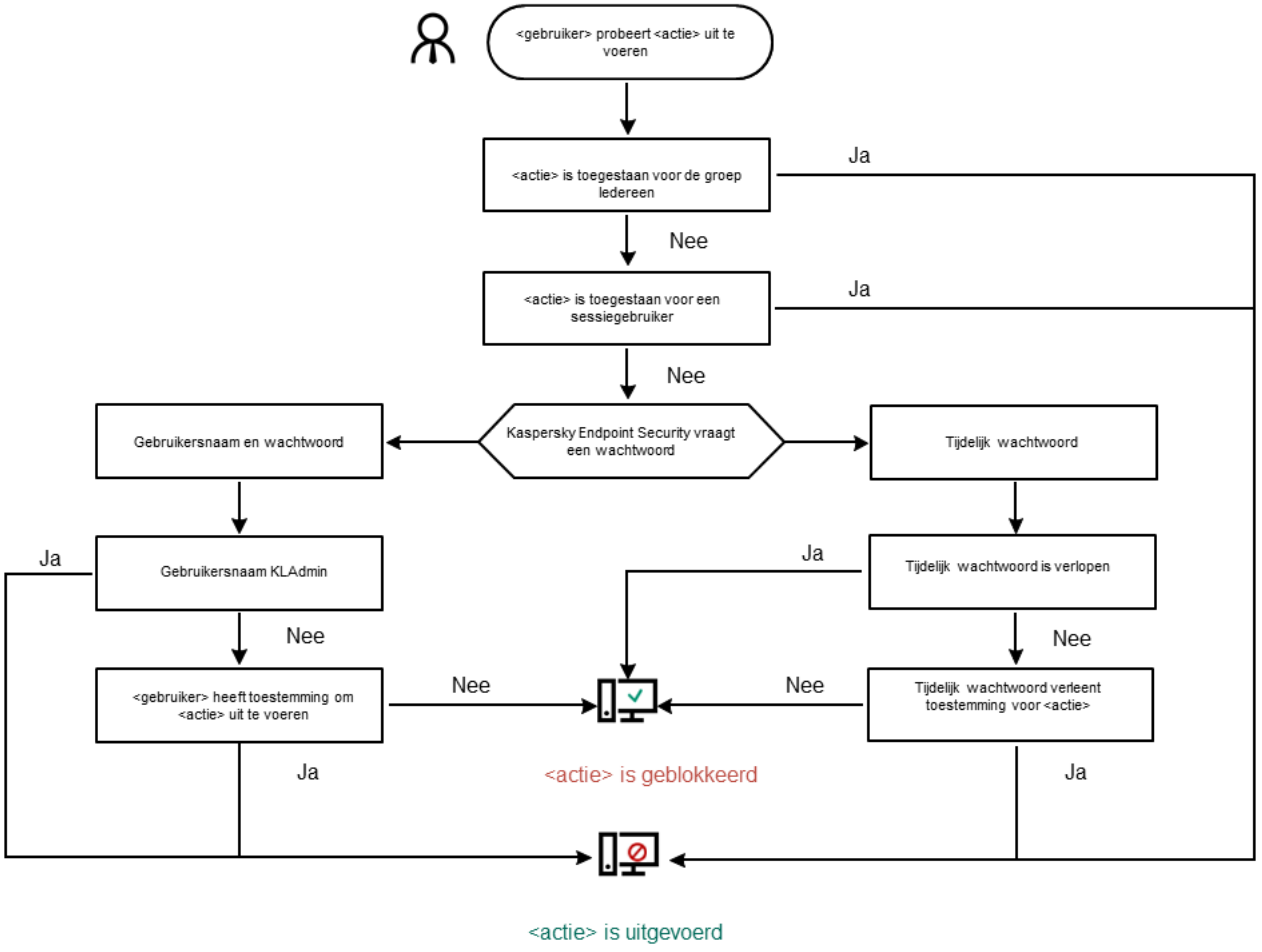
- **Sessiegebruiker**. Account van de gebruiker die de Windows-sessie heeft gestart. U kunt wisselen van sessiegebruiker wanneer u een wachtwoord wordt gevraagd (het selectievakje **Onthoud wachtwoord voor deze sessie**). In dit geval beschouwt Kaspersky Endpoint Security de gebruiker waarvan de accountgegevens 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).

Wachtwoordbeveiliging inschakelen via de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Algemene instellingen** → **Interface** in het beleidsvenster.
4. In het blok **Wachtwoordbeveiliging**, klikt u op de knop **Instellingen**.

   Dit opent een venster met instellingen voor wachtwoordbeveiliging.
5. Gebruik het selectievakje **Wachtwoordbeveiliging inschakelen** om het onderdeel in of uit te schakelen.
6. Selecteer onder **Machtigingen** het KLAdmin-account.
7. Klik in het venster dat wordt geopend op **Wachtwoord** en stel een wachtwoord in voor het KLAdmin-account.

   Het KLAdmin-account is gemachtigd om alle acties uit te voeren die met een wachtwoord zijn beveiligd.

   > Als u uw KLAdmin-accountwachtwoord bent vergeten, kunt u het wachtwoord opnieuw instellen in de beleidseigenschappen.
8. Ga terug naar de lijst met accounts.
9. Stel machtigingen voor alle gebruikers in het bedrijfsnetwerk in:

   a. Selecteer onder **Machtigingen** de groep "Iedereen".

      De *groep Iedereen* is een ingebouwde Windows-groep met alle gebruikers uit het bedrijfsnetwerk.

   b. Schakel in het geopende venster 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.
10. Sla uw wijzigingen op.

Wachtwoordbeveiliging inschakelen via de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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** → **Self-Defense**.

5. Gebruik onder **Password Protection** de schakelaar **Password Protection ENABLED** om het wachtwoord in of uit te schakelen.

6. Geef het wachtwoord voor het KLAdmin-account op en bevestig het.

   Het KLAdmin-account is gemachtigd om alle acties uit te voeren die met een wachtwoord zijn beveiligd.

   > Als u uw KLAdmin-accountwachtwoord bent vergeten, kunt u het wachtwoord opnieuw instellen in de beleidseigenschappen.

7. Ga terug naar de lijst met accounts.

8. Stel machtigingen voor alle gebruikers in het bedrijfsnetwerk in:

   a. Selecteer in de tabel met accounts de groep "Iedereen".

      De *groep Iedereen* is een ingebouwde Windows-groep met alle gebruikers uit het bedrijfsnetwerk.

   b. Schakel in het geopende venster 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 **Exit the application** 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.

9. Sla uw wijzigingen op.

Wachtwoordbeveiliging inschakelen via de programma-interface

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 KLAdmin-account op en bevestig het.

   Het KLAdmin-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 KLAdmin-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 KLAdmin-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 Iedereen te openen.

      De *groep Iedereen* 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 Iedereen zijn verleend. Het uitvoeren van de acties die zijn geblokkeerd voor de groep Iedereen 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

Met wachtwoordbeveiliging kan Kaspersky Endpoint Security toegang worden verleend tot individuele Active Directory-gebruikersaccounts en handmatig toegevoegde gebruikersaccounts.

Active Directory-gebruikersaccounts

U kunt Kaspersky Endpoint Security toegang verlenen aan individuele gebruikers of groepen binnen het Active Directory-domein. Als u het afsluiten van het programma bijvoorbeeld is geblokkeerd voor de groep Iedereen, 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.

Handmatig toegevoegde gebruikersaccounts

U kunt een gebruikersaccount maken dat niet aanwezig is in Active Directory en individuele machtigingen aan dat gebruikersaccount toewijzen. Dat wil zeggen dat u een *service-gebruikersaccount* kunt maken en deze kunt gebruiken in plaats van KLAdmin. Op deze manier hoeft u uw KLAdmin-wachtwoord niet met andere gebruikers te delen of nieuwe Active Directory-gebruikersaccounts aan te maken. U kunt elke gebruikersnaam en wachtwoord opgeven. U kunt bijvoorbeeld de **Rapporten bekijken** machtigingen verlenen aan de service-gebruikersaccount. Als gevolg hiervan, als het bekijken van rapporten verboden is voor de groep 'Alle', de rapporten openen via het service-gebruikersaccount of het KLAdmin-gebruikersaccount.

Machtigingen aan individuele gebruikers of groepen verlenen

Machtigingen verlenen aan individuele gebruikers of groepen in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Algemene instellingen** → **Interface** in het beleidsvenster.
4. In het blok **Wachtwoordbeveiliging**, klikt u op de knop **Instellingen**.

   Dit opent een venster met instellingen voor wachtwoordbeveiliging.
5. Klik in de account-tabel op **Toevoegen**.
6. Selecteer het type gebruikersaccount dat u wilt toevoegen:

   - **Selecteer een gebruiker/groep uit Active Directory** – Active Directory-gebruikersaccounts.

     Om een gebruikersaccount te selecteren, klik **Selecteren**. Selecteer een gebruiker of een groep in Active Directory en bevestig uw selectie.

   - **Handmatig een gebruiker / groep gebruikers toevoegen** voor een handmatig toegevoegde service-gebruikersaccount.

     Om een service-gebruikersaccount toe te voegen, voer een gebruikersnaam en een wachtwoord in (bijvoorbeeld SecureAdmin).

     U kunt het wachtwoord van een service-gebruikersaccount opnieuw instellen in de beleidsinstellingen. Het wachtwoord van de service-gebruikersaccount moet op dezelfde manier worden gereset als het KLAdmin-wachtwoord. Als het bewerken van de instellingen voor wachtwoordbeveiliging is toegestaan (het "slot" is open) of als er geen beleid wordt toegepast op de computer, kunt u het wachtwoord van het service-gebruikersaccount opnieuw instellen in het programma-interface. Om dit te doen, bevestigt de wijzigingen van de gegevens van het service-gebruikersaccount met het KLAdmin-wachtwoord.
7. 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.

8. Sla uw wijzigingen op.

Machtigingen verlenen aan individuele gebruikers of groepen in Web Console en Cloud Console

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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** → **Self-Defense**.
5. Klik in het blok **Password Protection** op de koppeling **User permissions**.

   Hiermee opent u het formulier voor het verlenen van machtigingen voor Wachtwoord inschakelen.
6. Klik op **Add**.
7. Selecteer het type gebruikersaccount dat u wilt toevoegen:

   - **Select from Active Directory** – Active Directory-gebruikersaccounts.

     Om een gebruikersaccount te selecteren, klik **Edit**. Selecteer een gebruiker of een groep in Active Directory en bevestig uw selectie.
   - **Add manually** voor een handmatig toegevoegde service-gebruikersaccount.

     Om een service-gebruikersaccount toe te voegen, voer een gebruikersnaam en een wachtwoord in (bijvoorbeeld SecureAdmin).

     U kunt het wachtwoord van een service-gebruikersaccount opnieuw instellen in de beleidsinstellingen. Het wachtwoord van de service-gebruikersaccount moet op dezelfde manier worden gereset als het KLAdmin-wachtwoord. Als het bewerken van de instellingen voor wachtwoordbeveiliging is toegestaan (het "slot" is open) of als er geen beleid wordt toegepast op de computer, kunt u het wachtwoord van het service-gebruikersaccount opnieuw instellen in het programma-interface. Om dit te doen, bevestigt de wijzigingen van de gegevens van het service-gebruikersaccount met het KLAdmin-wachtwoord.
8. Schakel in de lijst **Permissions** 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 **Exit the application** 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.

9. Klik op **Add**.
10. Sla uw wijzigingen op.

Machtigingen verlenen aan individuele gebruikers of groepen in de gebruikersinterface van het programma

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. Selecteer het type gebruikersaccount dat u wilt toevoegen:
   - **Selecteer een gebruiker/groep uit Active Directory** – Active Directory-gebruikersaccounts.

     Om een gebruikersaccount te selecteren, klik **Gebruiker of groep selecteren**. Selecteer een gebruiker of een groep in Active Directory en bevestig uw selectie.
   - **Handmatig een gebruiker toevoegen** voor een handmatig toegevoegde service-gebruikersaccount.

     Om een service-gebruikersaccount toe te voegen, voer een gebruikersnaam en een wachtwoord in (bijvoorbeeld SecureAdmin).

     U kunt het wachtwoord van een service-gebruikersaccount opnieuw instellen in de beleidsinstellingen. Het wachtwoord van de service-gebruikersaccount moet op dezelfde manier worden gereset als het KL Admin-wachtwoord. Als het bewerken van de instellingen voor wachtwoordbeveiliging is toegestaan (het "slot" is open) of als er geen beleid wordt toegepast op de computer, kunt u het wachtwoord van het service-gebruikersaccount opnieuw instellen in het programma-interface. Om dit te doen, bevestigt de wijzigingen van de gegevens van het service-gebruikersaccount met het KL Admin-wachtwoord.
5. 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 KL Admin, 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.

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)

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 **Applications** in het venster met computereigenschappen.
6. Selecteer **Kaspersky Endpoint Security voor Windows (14.1)** in de lijst met Kaspersky-programma's die op de computer zijn geïnstalleerd en dubbelklik om de eigenschappen van het programma te openen.
7. Selecteer **Algemene instellingen** → **Interface** in het venster met de programma-instellingen.
8. In het blok **Wachtwoordbeveiliging**, klikt u op de knop **Instellingen**.
9. Klik in het venster dat opent in het blok **Tijdelijk wachtwoord** op de knop **Lijst van tijdelijke wachtwoorden**.

   Het venster Beheer van tijdelijke wachtwoorden wordt geopend.
10. Klik op **Toevoegen**.
11. Geef in het veld **Verloopdatum** op wanneer het tijdelijke wachtwoord verloopt.
12. 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.
13. Klik op **Genereren**.

    Een venster met het tijdelijke wachtwoord wordt geopend (zie onderstaande afbeelding).
14. 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 **Asset management** → **Assets (Devices)**.
2. Klik op de naam van de computer waarop u een gebruiker een geblokkeerde actie wilt laten uitvoeren.
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. Selecteer **General settings** → **Interface** in het venster met de programma-instellingen.

7. In het blok **Temporary passwords**, klikt u op de knop **Add**.

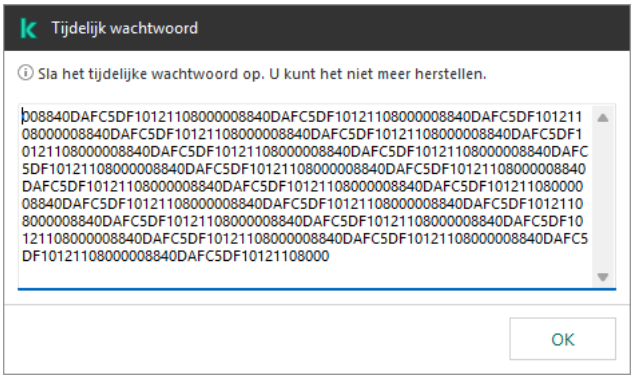
8. Geef in het veld **Verloopdatum** op wanneer het tijdelijke wachtwoord verloopt.

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.



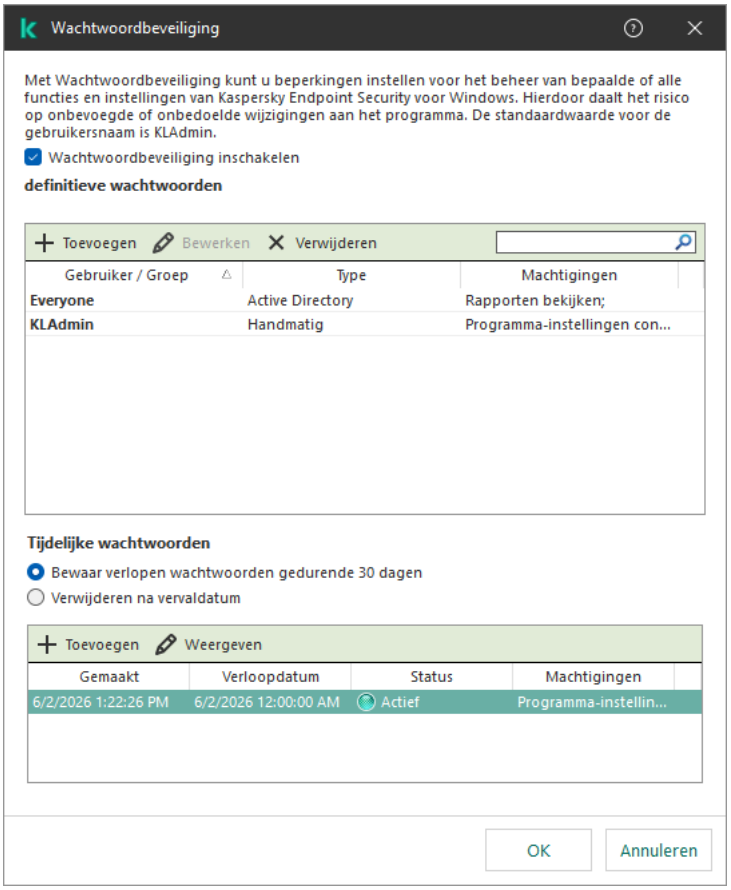
Tijdelijk wachtwoord

Tijdelijk wachtwoord intrekken

Vanaf versie 12.9 bevat Kaspersky Endpoint Security for Windows de: *Beheer van tijdelijke wachtwoorden* functionaliteit. Met het beheer van tijdelijke wachtwoorden kunt u de volgende acties uitvoeren:

- Wachtwoordgeschiedenis opslaan (maximaal 30 dagen).
- Status van tijdelijk wachtwoord bewaken: *Actief*, *Verlopen*, *Ingetrokken*.

- Tijdelijke wachtwoorden intrekken.



Beheer van tijdelijke wachtwoorden

Het beheer van tijdelijke wachtwoorden werkt de status van het wachtwoord bij en trekt het pas in nadat de computer met Kaspersky Security Center is gesynchroniseerd.

Tijdelijk wachtwoord intrekken 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 **Applications** in het venster met computereigenschappen.
6. Selecteer **Kaspersky Endpoint Security voor Windows (14.1)** in de lijst met Kaspersky-programma's die op de computer zijn geïnstalleerd en dubbelklik om de eigenschappen van het programma te openen.
7. Selecteer **Algemene instellingen** → **Interface** in het venster met de programma-instellingen.
8. In het blok **Wachtwoordbeveiliging**, klikt u op de knop **Instellingen**.
9. Hiermee open je een venster; in dat venster onder **Tijdelijk wachtwoord**, configureer de opslaginstellingen voor verlopen wachtwoorden.

10. Klik op **Lijst van tijdelijke wachtwoorden**.

    Het venster Beheer van tijdelijke wachtwoorden wordt geopend. Beheer van tijdelijke wachtwoorden toont de vervaldatum van het wachtwoord, de status van het wachtwoord en de lijst met machtigingen.

11. Selecteer het actieve tijdelijke wachtwoord dat u wilt intrekken en dubbelklik op het wachtwoord om de eigenschappen ervan te openen.

12. Klik in het venster op de knop **Ingetrokken**.

13. Sla uw wijzigingen op. Om het beleid op computers toe te passen, sluit de hangsloten .

Tijdelijk wachtwoord intrekken via de Webconsole en de Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Assets (Devices)**.

2. Klik op de naam van de computer waarop u een gebruiker een geblokkeerde actie wilt laten uitvoeren.

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. Selecteer **General settings** → **Interface** in het venster met de programma-instellingen.

7. Onder **Temporary passwords**, configureer de opslag van verlopen wachtwoorden.

8. Klik op de koppeling **Temporary password**.

   Het venster Beheer van tijdelijke wachtwoorden wordt geopend. Beheer van tijdelijke wachtwoorden toont de vervaldatum van het wachtwoord, de status van het wachtwoord en de lijst met machtigingen.

9. Selecteer het actieve tijdelijke wachtwoord dat u wilt intrekken.

10. Klik in het venster op de knop **Revoke password**.

11. Sla uw wijzigingen op. Om het beleid op computers toe te passen, sluit de hangsloten .

Als gevolg hiervan stelt Beheer van tijdelijke wachtwoorden de status van het wachtwoord in op: *Intrekken (synchroniseren met een host)*. Na de computer met Kaspersky Security Center te hebben gesynchroniseerd, trekt het programma het tijdelijke wachtwoord in en blokkeert het de verleende machtigingen onmiddellijk.

Aandachtspunten bij machtigingen met wachtwoordbeveiliging

Bij machtigingen met wachtwoordbeveiliging moet u wel rekening houden met enkele belangrijke aandachtspunten en beperkingen.

Programma-instellingen configureren

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.

Sleutel 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 schijf 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.

Instellingen exporteren

Standaard wordt het exporteren van programma-instellingen geweigerd voor de groep "Alle". U kunt programma-instellingen exporteren met het KLAdmin-gebruikersaccount. Het exporteren van programma-instellingen omvat alleen een configuratiebestand maken met de instellingen van Kaspersky Endpoint Security in de programma-interface. De machtiging vormt geen beperking voor het exporteren van lijsten met uitzonderingen voor scans, vertrouwde webadressen, vertrouwde apparaten of andere lijsten die door programma-onderdelen worden bijgehouden.

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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Algemene instellingen** → **Interface** in het beleidsvenster.
4. In het blok **Wachtwoordbeveiliging**, klikt u op de knop **Instellingen**.
5. Schakel in het venster dat opent het selectievakje **Wachtwoordbeveiliging inschakelen**.
6. Sla uw wijzigingen op.
7. Selecteer het selectievakje **Wachtwoordbeveiliging inschakelen** opnieuw.
8. Klik op **OK**.
   Hiermee wordt het venster voor het beheerderswachtwoord geopend.
9. Geef het wachtwoord voor het nieuwe KLAdmin-account op en bevestig het.
10. 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 **Asset management** → **Assets (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 **General Settings** → **Self-Defense**.
7. Schakel 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.

Administration Server verbindingsbeveiliging

Het verbinden van de computer met de Administration Server wordt bereikt met behulp van de *Netwerkagent*-onderdelen van Kaspersky Security Center. Als een indringer voldoende rechten heeft om de instellingen van de serververbinding te wijzigen, bestaat het risico dat de computer wordt verbonden met een niet-vertrouwde server. Hierdoor zou de indringer zijn eigen groepsbeleid kunnen toepassen en bijvoorbeeld de zelfverdediging van het programma kunnen uitschakelen. Kaspersky Endpoint Security kan voorkomen dat een computer zonder toestemming opnieuw verbinding maakt met een andere server. Om de serververbinding te beschermen, stelt het programma voor om een wachtwoord in te stellen en de Password-Based key Derivation Function (PBKDF2) te gebruiken. Hierdoor is toegang tot het programma zonder wachtwoord onmogelijk.

> Om een uitgebreide bescherming van Kaspersky Endpoint Security en Networkagent tegen ongeoorloofde toegang te garanderen, raden we aan aanvullende bescherming in te schakelen. Voor Kaspersky Endpoint Security raden we aan Wachtwoordbeveiliging in te schakelen. Om Network Agent te beschermen, raden we aan om een wachtwoord in te stellen om de installatie ongedaan te maken. Voor informatie over het beschermen van Network Agent tegen verwijdering, raadpleeg de Help van Kaspersky Security Center.

Het beheren van de verbinding van de computer met de Administration Server wordt bereikt met behulp van de *Administration Server verbindingsbescherming* taak. Met de taak kunt u dan de volgende acties uitvoeren:

- Stel een wachtwoord in om de serververbinding te beschermen.
- Verander het wachtwoord.
- Sluit de computer opnieuw aan op een andere server.
- Schakel de verbindingsbeveiliging van de server uit.

Authenticatie van de computer bij verbinding met de Administration Server

Nadat een wachtwoord is ingesteld, maakt het programma een gegevens-array met behulp van PBKDF2-transformatie van het wachtwoord. Het programma versleuteld vervolgens deze gegevens-array met behulp van de Networkagent-sleutel. Het programma gebruikt de versleutelde gegevens-array om de rechten en privileges van de Administration Server voor volgende verbindingen te controleren.

Wanneer vervolgens wordt geprobeerd de computer opnieuw met de Administration Server te verbinden, decrypt het programma de gegevens-array met de Networkagent-sleutel en vergelijkt deze met de lokale kopie. Als ze niet overeenkomen, wordt de toegang tot het programma beperkt.

Administration Server verbindingsbeveiliging

Een wachtwoord instellen voor bescherming van serververbindingen in Beheerconsole (MMC)

1. Selecteer **Tasks** in de structuur van de Beheerconsole van Kaspersky Security Center.

   De lijst met taken wordt geopend.

2. Klik op **New task**.

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

Stap 1. Een taaktype selecteren

Selecteer **Kaspersky Endpoint Security voor Windows 14.1.** → **Administration Server verbindingsbescherming**.

Stap 2. De verbinding met de Administration Server beveiligen

Stel een wachtwoord in om de Administration Server-verbinding te beschermen:

1. Onder **Administration Server verbindingsbescherming**, selecteer **Beveiligen met wachtwoord**.

2. Selecteer in de vervolgkeuzelijst **Administration Server** de optie **Nieuwe server**.

3. In het **Wachtwoord voor verbinding met de Administration Server** veld, stel een wachtwoord in om verbinding te maken met de Administration Server en bevestig het.

   Als u het wachtwoord bent vergeten, kunt u het wachtwoord wijzigen via een taak.

4. Als u Kaspersky Endpoint Security 12.7 of een eerdere versie van het programma hebt geïmplementeerd, selecteer het selectievakje **Sta wachtwoordvergrendelingscompatibiliteit voor eerdere programmaversies toe (12.7 en lager)**.

   Vanaf Kaspersky Endpoint Security 12.8 voor Windows maakt het programma gebruik van sterkere wachtwoordversleuteling. Als u Kaspersky Endpoint Security 12.8 of hoger hebt geïmplementeerd, raden wij u aan dit selectievakje uit te schakelen en de sterkere wachtwoordversleuteling te gebruiken. Eerdere versies van het programma ondersteunen geen sterke wachtwoordversleuteling. Om de taak uit te voeren, moet u het selectievakje aanvinken.

Stap 3: Het account selecteren om de taak uit te voeren

Selecteer **Default account**. Standaard start Kaspersky Endpoint Security de taak met het gebruikersaccount van het systeem (SYSTEM).

Stap 4. Een taakstartschema configureren

Onder **Scheduled start**, selecteer **Manually**.

Stap 5. Taaknaam definiëren

Voer een naam in voor de taak, bijvoorbeeld *Wachtwoord voor hoofdserververbinding*.

Stap 6. Aanmaak van de taak voltooien

Verlaat de wizard verlaten. Selecteer het selectievakje **Run the task after the wizard finishes** cf voer de taak handmatig uit. U kunt de voortgang van de taak volgen in de taakeigenschappen.

Een wachtwoord instellen voor bescherming van de serververbinding in Webconsole en Cloudconsole

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

   De lijst met taken wordt geopend.

2. Klik op **Add**.

   De wizard Taak wordt gestart.

3. Configureer de taakinstellingen:

   a. Selecteer in de vervolgkeuzelijst **Application** de optie **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. Selecteer in de vervolgkeuzelijst **Task type** de optie **Administration Server connection protection**.

c. In de **Task name** veld, typ een korte omschrijving, zoals *Wachtwoord voor hoofdserververbinding*.

d. Selecteer in het gedeelte **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. Ga naar de volgende stap.

5. Selecteer een standaard gebruikersaccount. Standaard start Kaspersky Endpoint Security de taak met het gebruikersaccount van het systeem (SYSTEM).

6. Verlaat de wizard verlaten.

   U ziet een nieuwe taak in de lijst met taken.

7. Klik op de taak **Administration Server connection protection** van Kaspersky Endpoint Security.

   U ziet nu het venster met de taakeigenschappen.

8. Selecteer het tabblad **Application settings**.

9. Onder **Administration Server connection protection**, selecteer **Protect with a password**.

10. Selecteer in de vervolgkeuzelijst **Connection to the Administration Server** de optie **New password**.

11. In het **Password** veld, stel een wachtwoord in om verbinding te maken met de Administration Server en bevestig het.

    Als u het wachtwoord bent vergeten, kunt u het wachtwoord wijzigen via een taak.

12. Als u Kaspersky Endpoint Security 12.7 of een eerdere versie van het programma hebt geïmplementeerd, selecteer het selectievakje **Enable password encryption compatibility for previous application versions (12.7 and lower)**.

    Vanaf Kaspersky Endpoint Security 12.8 voor Windows maakt het programma gebruik van sterkere wachtwoordversleuteling. Als u Kaspersky Endpoint Security 12.8 of hoger hebt geïmplementeerd, raden wij u aan dit selectievakje uit te schakelen en de sterkere wachtwoordversleuteling te gebruiken. Eerdere versies van het programma ondersteunen geen sterke wachtwoordversleuteling. Om de taak uit te voeren, moet u het selectievakje aanvinken.

13. Sla uw wijzigingen op.

14. Schakel het selectievakje naast de taak in.

15. Klik op **Start**.

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 computer opnieuw verbinden met een andere Administration Server

De computer opnieuw verbinden met een andere Administration Server vereist de volgende stappen:

1. In de console van de huidige `[KSC1]`-server, voer de *Change Administration Server* taak uit voor Networkagent.

   Nadat de taak is uitgevoerd, wordt de computer opnieuw verbonden met de nieuwe `[KSC2]`-server.

   De computer wordt weergegeven in de `[KSC1]` serverconsole met de *Critical* status. Het configureren van het programma met behulp van beleid of het op afstand uitvoeren van taken op de computer is onmogelijk.

2. In de console van de nieuwe [KSC2]-server, maak een nieuwe *Administration Server verbindingsbescherming* taak voor Kaspersky Endpoint Security. Voer in de taakeigenschappen het wachtwoord van de vorige server in en stel een wachtwoord in voor de nieuwe server.

Een nieuw wachtwoord instellen om opnieuw verbinding te maken met een nieuwe server in Beheerconsole (MMC)

1. Selecteer **Tasks** in de structuur van de Beheerconsole van Kaspersky Security Center.

   De lijst met taken wordt geopend.

2. Klik op **New task**.

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

Stap 1. Een taaktype selecteren

Selecteer **Kaspersky Endpoint Security voor Windows 14.1.** → **Administration Server verbindingsbescherming**.

Stap 2. De verbinding met de Administration Server beveiligen

Stel een wachtwoord in om de verbinding met de nieuwe Administation Server te beveiligen:

1. Onder **Administration Server verbindingsbescherming**, selecteer **Beveiligen met wachtwoord**.
2. Selecteer in de vervolgkeuzelijst **Administration Server** de optie **Opnieuw verbinden vanaf een andere server**.
3. In het veld **Huidig wachtwoord**, voer het wachtwoord in dat is ingesteld voor de verbinding met de eerder gebruikte vertrouwde server.
4. In het **Nieuw wachtwoord** veld, stel een wachtwoord in om verbinding te maken met de nieuwe Administration Server en bevestig het wachtwoord.

   Als u het wachtwoord bent vergeten, kunt u het wachtwoord wijzigen via een taak.

5. Als u Kaspersky Endpoint Security 12.7 of een eerdere versie van het programma hebt geïmplementeerd, selecteer het selectievakje **Sta wachtwoordvergrendelingscompatibiliteit voor eerdere programmaversies toe (12.7 en lager)**.

   Vanaf Kaspersky Endpoint Security 12.8 voor Windows maakt het programma gebruik van sterkere wachtwoordversleuteling. Als u Kaspersky Endpoint Security 12.8 of hoger hebt geïmplementeerd, raden wij u aan dit selectievakje uit te schakelen en de sterkere wachtwoordversleuteling te gebruiken. Eerdere versies van het programma ondersteunen geen sterke wachtwoordversleuteling. Om de taak uit te voeren, moet u het selectievakje aanvinken.

Stap 3: Het account selecteren om de taak uit te voeren

Selecteer **Default account**. Standaard start Kaspersky Endpoint Security de taak met het gebruikersaccount van het systeem (SYSTEM).

Stap 4. Een taakstartschema configureren

Onder **Scheduled start**, selecteer **Manually**.

Stap 5. Taaknaam definiëren

Voer een naam in voor de taak, bijvoorbeeld *Wachtwoord voor hoofdserververbinding*.

Stap 6. Aanmaak van de taak voltooien

Verlaat de wizard verlaten. Selecteer het selectievakje **Run the task after the wizard finishes** cf voer de taak handmatig uit. U kunt de voortgang van de taak volgen in de taakeigenschappen.

Een nieuw wachtwoord instellen om opnieuw verbinding te maken met een nieuwe server in Webconsole en Cloudconsole

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

   De lijst met taken wordt geopend.

2. Klik op **Add**.

   De wizard Taak wordt gestart.

3. Configureer de taakinstellingen:

   a. Selecteer in de vervolgkeuzelijst **Application** de optie **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. Selecteer in de vervolgkeuzelijst **Task type** de optie **Administration Server connection protection**.

   c. In de **Task name** veld, typ een korte omschrijving, zoals *Wachtwoord voor hoofdserververbinding*.

   d. Selecteer in het gedeelte **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. Ga naar de volgende stap.

5. Selecteer een standaard gebruikersaccount. Standaard start Kaspersky Endpoint Security de taak met het gebruikersaccount van het systeem (SYSTEM).

6. Verlaat de wizard verlaten.

   U ziet een nieuwe taak in de lijst met taken.

7. Klik op de taak **Administration Server connection protection** van Kaspersky Endpoint Security.

   U ziet nu het venster met de taakeigenschappen.

8. Selecteer het tabblad **Application settings**.

9. Onder **Administration Server connection protection**, selecteer **Protect with a password**.

10. Selecteer in de vervolgkeuzelijst **Connection to the Administration Server** de optie **Reconnect from another server**.

11. In het veld **Current password**, voer het wachtwoord in dat is ingesteld voor de verbinding met de eerder gebruikte vertrouwde server.

12. In het **New password** veld, stel een wachtwoord in om verbinding te maken met de nieuwe Administration Server en bevestig het wachtwoord.

    Als u het wachtwoord bent vergeten, kunt u het wachtwoord wijzigen via een taak.

13. Als u Kaspersky Endpoint Security 12.7 of een eerdere versie van het programma hebt geïmplementeerd, selecteer het selectievakje **Sta wachtwoordvergrendelingscompatibiliteit voor eerdere programmaversies toe (12.7 en lager)**.

    Vanaf Kaspersky Endpoint Security 12.8 voor Windows maakt het programma gebruik van sterkere wachtwoordversleuteling. Als u Kaspersky Endpoint Security 12.8 of hoger hebt geïmplementeerd, raden wij u aan dit selectievakje uit te schakelen en de sterkere wachtwoordversleuteling te gebruiken. Eerdere versies van het programma ondersteunen geen sterke wachtwoordversleuteling. Om de taak uit te voeren, moet u het selectievakje aanvinken.

14. Sla uw wijzigingen op.

15. Schakel het selectievakje naast de taak in.

16. Klik op **Start**.

    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.

Na het voltooien van de taak, zorg ervoor dat de computer in de console van de nieuwe `[KSC2]`-server, de *OK* status heeft. Test of u taken op afstand kunt uitvoeren en het programma kunt configureren met behulp van het beleid.

Het verbindingswachtwoord van de Administration Server opnieuw instellen

Als u uw Administration Server-verbindingswachtwoord bent vergeten of als het wachtwoord is gecompromitteerd, kunt u het wachtwoord opnieuw instellen in de taakeigenschappen. U kunt ook het wachtwoord opnieuw instellen en een nieuw wachtwoord instellen voor een groep computers met verschillende statussen voor verbindingsbeveiliging van de Administratie Server. Dat wil zeggen, als de beveiliging op sommige computers is ingeschakeld en op andere computers is uitgeschakeld, stelt de taak een wachtwoord in voor alle computers.

U kunt het verbindingswachtwoord van de Administration Server alleen opnieuw instellen in de console van de

vertrouwde server waarmee de computer is verbonden.

Het wachtwoord van de Administration Server-verbinding opnieuw instellen met behulp van de beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de beheerconsole **Tasks**.
3. Selecteer de **Administration Server verbindingsbescherming** taak en dubbelklik om de taakeigenschappen te openen.
4. Selecteer het gedeelte **Instellingen** in het venster met taakeigenschappen.
5. Onder **Administration Server verbindingsbescherming**, selecteer **Wachtwoord beschermen en wijzigen**.
6. In het veld **Wachtwoord voor verbinding met de Administration Server**, stel een nieuw wachtwoord in om verbinding te maken met de huidige vertrouwde server en bevestig het wachtwoord.
7. Sla uw wijzigingen op.
8. Voer de taak uit.

Het wachtwoord van de Administration Server-verbinding opnieuw instellen in Webconsole en Cloudconsole

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

   De lijst met taken wordt geopend.
2. Klik op de taak **Administration Server connection protection** van Kaspersky Endpoint Security.

   U ziet nu het venster met de taakeigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Onder **Administration Server connection protection**, selecteer **Protect and change password**.
5. In het veld **Password**, stel een nieuw wachtwoord in om verbinding te maken met de huidige vertrouwde server en bevestig het wachtwoord.
6. Sla uw wijzigingen op.
7. Schakel het selectievakje naast de taak in.
8. Klik op **Start**.

Als gevolg hiervan wordt het verbindingswachtwoord van de Administration Server opnieuw ingesteld nadat de taak is voltooid.

Schakel de verbindingsbeveiliging van Administration Server uit

U kunt de verbindingsbeveiliging van Administration Server alleen op afstand uitschakelen in de console van de vertrouwde server waarmee de computer is verbonden. U kunt de beveiliging ook lokaal via de opdrachtregel uitschakelen.

De bescherming van de serververbinding uitschakelen in de Beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de beheerconsole **Tasks**.
3. Selecteer de **Administration Server verbindingsbescherming** taak en dubbelklik om de taakeigenschappen te openen.
4. Selecteer het gedeelte **Instellingen** in het venster met taakeigenschappen.
5. Onder **Administration Server verbindingsbescherming**, selecteer **Niet beschermen**.
6. Sla uw wijzigingen op.
7. Voer de taak uit.

   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 bescherming van de serververbinding uitschakelen in Webconsole en Cloudconsole

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

   De lijst met taken wordt geopend.
2. Klik op de taak **Administration Server connection protection** van Kaspersky Endpoint Security.

   U ziet nu het venster met de taakeigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Onder **Administration Server connection protection**, selecteer **Do not protect**.
5. Sla uw wijzigingen op.
6. Schakel het selectievakje naast de taak in.
7. Klik op **Start**.

   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 verbindingsbeveiliging van de server op de opdrachtregel uitschakelen

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 SERVERBINDINGDISABLE [/password=<password>]
```

waarbij `<password>` het wachtwoord is van de KL Admin-gebruikersaccount of het wachtwoord van de *Administration Server verbindingsbescherming* taak. Als de parameter niet is opgegeven, vraagt Kaspersky Endpoint Security u op de volgende regel om een wachtwoord in te voeren.

Voor het uitvoeren van deze opdracht moet Wachtwoordbeveiliging ingeschakeld zijn.

Voorbeeld

```
avp.com SERVERBINDINGDISABLE /password=samplePassword
```

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 Advanced Encryption Standard (AES) encryptiealgoritme.

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 Kaspersky Endpoint Security is geïnstalleerd op een Arm-computer, is alleen BitLocker Drive Encryption beschikbaar. Het programma ondersteunt geen andere onderdelen van de gegevensencryptie.

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 encryptiefunctionaliteit of zonder toegang tot de encryptiefunctionaliteit behoudt het bestand hierdoor een niet-geëncrypte toestand.

Kaspersky Endpoint Security beschikt over de volgende aspecten voor gegevensbescherming:

- **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 encryptiefunctionaliteit.

- **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 de taak *Accounts voor Authenticatie-agent beheren*. Dit account is gebaseerd op een Microsoft Windows-account waarmee een gebruiker zich bij het besturingssysteem aanmeldt. U kunt ook gebruikmaken van Single Sign-On (SSO)-technologie, 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-functionaliteit 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.

- Als Kaspersky Endpoint Security is geïnstalleerd op een Arm-computer, is alleen Full Disk Encryption met BitLocker -stationsversleuteling beschikbaar. Andere versleutelingsonderdelen worden niet ondersteund.

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, IEEE1934, 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 partitities: 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 ThinkCentre 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 10O
- 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 distributiepakket van dezelfde versie van het programma dat op uw computer is geïnstalleerd zonder het programma eerst te verwijderen.

Kaspersky Disk Encryption

Kaspersky Disk Encryption wordt niet ondersteund op Arm-computers.

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 welkomstscherm 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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Gegevensencryptie → Full Disk Encryption** in het beleidsvenster.
4. Selecteer in de vervolgkeuzelijst **Encryptietechnologie** de optie **Kaspersky Disk Encryption**.

   Kaspersky Disk Encryption-technologie kan niet worden gebruikt als de computer harde schijven heeft die met BitLocker zijn geëncrypt.

5. 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.

6. Configureer geavanceerde Kaspersky Disk Encryption-opties (zie onderstaande tabel).
7. Sla uw wijzigingen op.

Kaspersky Disk Encryption uitvoeren via de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management → Policies**.
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 **Kaspersky Disk Encryption**-technologie.

   Kaspersky Disk Encryption-technologie kan niet worden gebruikt als de computer harde schijven heeft die met BitLocker zijn geëncrypt.

6. Selecteer in het blok **Action on devices Encrypt all hard drives**.

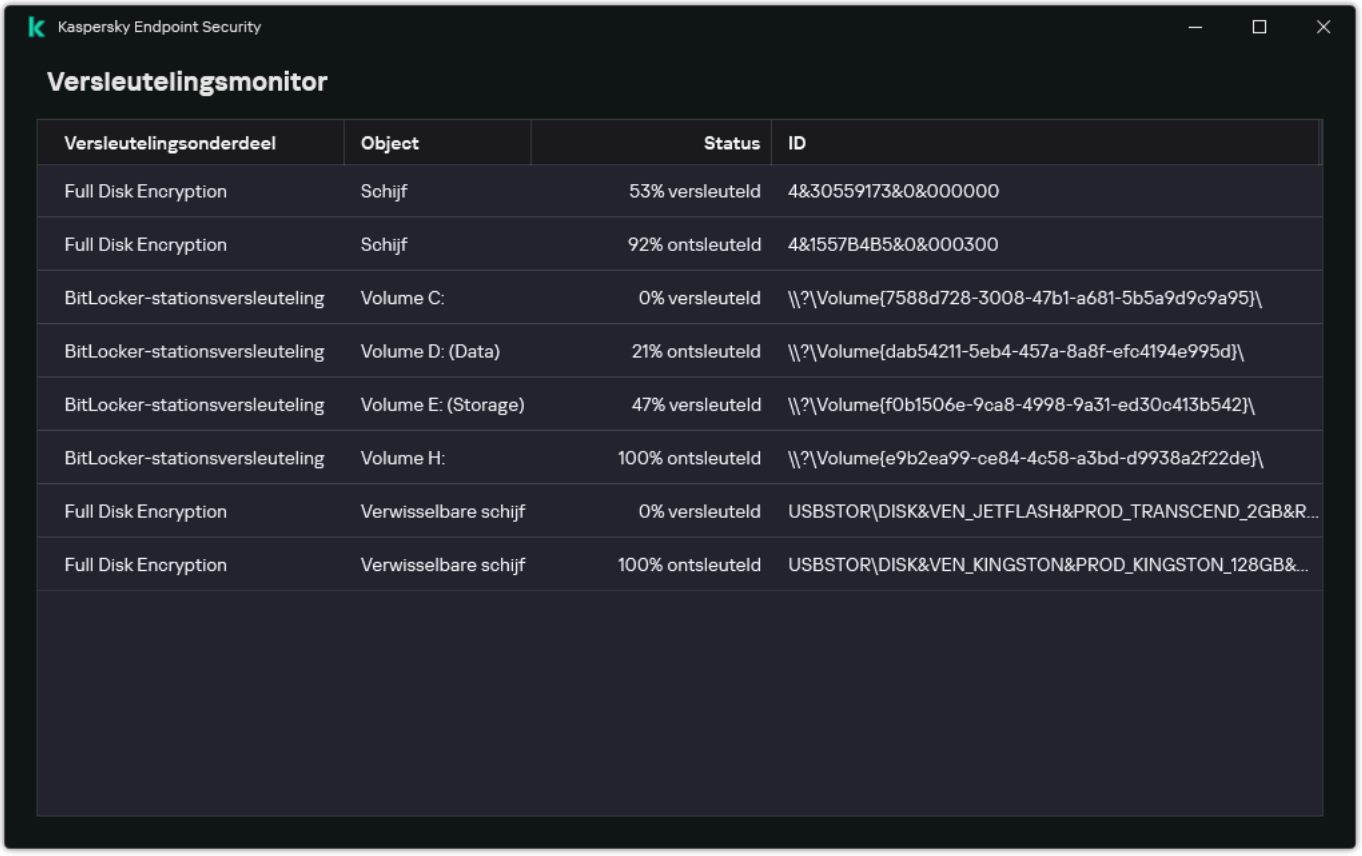
   Als verschillende besturingssystemen zijn geïnstalleerd op de computer, kunt u na de encryptie alleen het besturingssysteem laden dat u hebt gebruikt om de encryptie uit te voeren.

Als u wilt instellen dat enkele harde schijven niet moeten worden geëncrypt, maakt u een lijst met die harde schijven aan.

7. Configureer geavanceerde Kaspersky Disk Encryption-opties (zie onderstaande tabel).

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.



Versleutelingsmonitor

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
Accounts voor Authenticatie-agent automatisch maken voor gebruikers tijdens encryptie	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.
Accounts in Authenticatie-agent automatisch aanmaken voor alle gebruikers van deze computer bij aanmelding	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 handmatig Authenticatie-agent-accounts toe te voegen met de taak *Accounts voor Authenticatie-agent beheren* voor computers met reeds versleutelde stations.

Parameter	Beschrijving
Ingevoerde gebruikersnaam in Authenticatie-agent opslaan	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.
Alleen gebruikte schijfruimte encrypten (snellere encryptie)	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. De in- of uitschakeling van de functie **Alleen gebruikte schijfruimte encrypten (snellere encryptie)** 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. Het selectievakje is standaard uitgeschakeld.
Ondersteuning voor verouderde USB-apparaten gebruiken (niet aanbevolen)	Dit selectievakje schakelt de Legacy USB Support functionaliteit in of uit. *Ondersteuning voor verouderde USB-apparaten* **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). Legacy USB Support is niet van invloed op de ondersteuning voor USB-apparaten nadat het besturingssysteem is gestart. Als het selectievakje is ingeschakeld, wordt de ondersteuning voor USB-apparaten tijdens de initiële opstart van de computer ingeschakeld. Wanneer de functie Legacy USB Support 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.

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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Gegevensencryptie** → **Full Disk Encryption** in het beleidsvenster.

4. Selecteer in de vervolgkeuzelijst **Encryptietechnologie** de optie **Kaspersky Disk Encryption**.

   De items die overeenkomen met harde schijven die niet moeten worden geëncrypt worden in de tabel **Encrypt de volgende harde schijven niet** weergegeven. Deze tabel is leeg als u eerder geen lijst met harde schijven die niet moeten worden geëncrypt hebt gemaakt.

5. Zo voegt u harde schijven toe aan de lijst met harde schijven die niet moeten worden geëncrypt:

   a. Klik op **Toevoegen**.

   b. Geef in het venster dat opent de waarden voor **Apparaatnaam**, **Computer**, **Schijftype**, **Kaspersky Disk Encryption**.

   c. Klik op **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.

6. 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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.

2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

3. Selecteer **Gegevensencryptie** → **Full Disk Encryption** in het beleidsvenster.

4. Selecteer in de vervolgkeuzelijst **Encryptietechnologie** de optie **Kaspersky Disk Encryption**.

   De items die overeenkomen met harde schijven die niet moeten worden geëncrypt worden in de tabel **Encrypt de volgende harde schijven niet** weergegeven.

5. 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 knop → **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.

6. De lijst met regels importeren:

a. Klik op de knop → **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.

7. Sla uw wijzigingen op.

Een lijst met uitzonderingen voor de encryptie van harde schijven exporteren en importeren in de Webconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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**.

Selecteer de **Kaspersky Disk Encryption**-technologie.

5. Klik 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 de knop → **Export**.

Kaspersky Endpoint Security exporteert de lijst met uitzonderingen naar een JSON-bestand in de standaard downloadmap.

7. De lijst met uitzonderingen importeren:

a. Klik op de knop → **Import**.

Selecteer in het geopende venster het JSON-bestand waaruit u de lijst met uitzonderingen wil importeren.

b. 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 JSON-bestand.

8. 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. Dit betekent dat een gebruiker slechts één keer een wachtwoord hoeft in te voeren wanneer hij zich aanmeldt bij Windows (wachtwoord voor authenticatieagent-account). Met Single Sign-On-technologie kunt u ook automatisch het wachtwoord van het Authenticatie-agent-account bijwerken wanneer het wachtwoord van het Windows-account wordt gewijzigd.

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.

Single Sign-On-technologie inschakelen

Het gebruik van Single Sign-On-technologie inschakelen in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Gegevensencryptie → Algemene encryptie-instellingen** in het beleidsvenster.
4. In het blok **Wachtwoordinstellingen**, klikt u op de knop **Instellingen**.
5. In het venster dat opent, op het tabblad **Authenticatie-agent**, schakelt u het selectievakje **Eenmalige aanmelding (SSO) gebruiken** in.
6. Als u een externe referentieprovider gebruikt, schakel dan het selectievakje **Wrap gebruikersgegevens van andere leveranciers** 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 inschakelen in de webconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management → Policies**.
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 **Kaspersky Disk Encryption**-technologie.
6. Schakel in het blok **Password settings** het selectievakje **Use Single Sign-On (SSO) technology** in.

7. Als u een externe referentieprovider gebruikt, schakel dan het selectievakje **Wrap third-party credential providers** 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 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. Deze acties hoeven slechts één keer te worden uitgevoerd om de wachtwoorden te synchroniseren. Daarna zal Kaspersky Endpoint Security het wachtwoord van het Authenticatieagent-account vervangen door het wachtwoord van het Windows-account. Wanneer het wachtwoord van het Windows-account wordt gewijzigd, werkt het programma het wachtwoord voor de Authenticatie-agent-account automatisch bij.

Externe referentieprovider

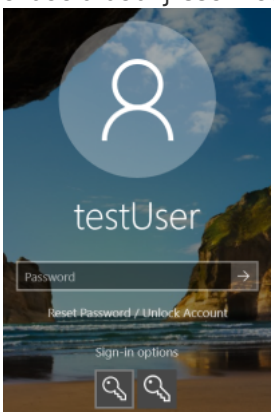
Kaspersky Endpoint Security ondersteunt de externe referentieprovider ADSelfService Plus.

Bij het werken met externe referentieproviders onderschept de authenticatie-agent het wachtwoord voordat het besturingssysteem wordt geladen. Dit betekent dat een gebruiker slechts één keer een wachtwoord hoeft in te voeren wanneer hij zich aanmeldt bij Windows. Na aanmelding bij Windows, kan de gebruiker gebruikmaken van een externe referentieprovider voor authenticatie in bijvoorbeeld bedrijfsservices. Externe referentieproviders stellen gebruikers ook in staat om onafhankelijk hun eigen wachtwoord opnieuw in te stellen. In dit geval werkt Kaspersky Endpoint Security het wachtwoord voor Authenticatie-agent automatisch bij.

Als u een externe referentieprovider gebruikt die niet door het programma wordt ondersteund, kunt u enkele beperkingen tegenkomen bij de werking van Single Sign-On-technologie. Wanneer u zich aanmeldt bij Windows, zijn er twee profielen beschikbaar voor de gebruiker: de referentieprovider in het systeen zelf en de externe referentieprovider. De pictogrammen van deze profielen zullen identiek zijn (zie onderstaande figuur). De gebruiker heeft de volgende opties om door te gaan:

- Als de gebruiker de *externe referentieprovider* selecteert, zal Authenticatie-agent het wachtwoord niet kunnen synchroniseren met het Windows-account. Daarom kan Kaspersky Endpoint Security het wachtwoord voor de Authenticatie-agent-account niet bijwerken als de gebruiker het wachtwoord van het Windows-account heeft gewijzigd. Als resultaat moet de gebruiker de authenticatieprocedure twee keer uitvoeren: in de interface van de authenticatie-agent en voordat het besturingssysteem wordt geladen. In dit geval kan de gebruiker gebruikmaken van een externe referentieprovider voor authenticatie in bijvoorbeeld bedrijfsservices.

- Als de gebruiker de *referentieprovider in het systeem* selecteert, zal Authenticatie-agent het wachtwoord synchroniseren met het Windows-account. In dit geval kan de gebruiker geen gebruikmaken van een externe referentieprovider voor authenticatie in bijvoorbeeld bedrijfsservices.



Systeem-authenticatieprofiel en authenticatieprofiel van derden voor Windows-aanmelding

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. Selecteer **Tasks** in de structuur van de Beheerconsole van Kaspersky Security Center.

   De lijst met taken wordt geopend.

2. Klik op **New task**.

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

Stap 1. Een taaktype selecteren

Selecteer **Kaspersky Endpoint Security voor Windows 14.1. → 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 **Run the task after the wizard finishes** 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.

De taak voor het beheren van accounts voor Authenticatie-agent maken in de Webconsole

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

   De lijst met taken wordt geopend.

2. Klik op **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** de optie **Kaspersky Endpoint Security for Windows (14.1)**.
2. Selecteer in de vervolgkeuzelijst **Task type** de optie **Manage Authentication Agent accounts**.
3. Typ in het veld **Task name** een korte omschrijving, zoals *Administrator-accounts*.
4. Selecteer in het gedeelte **Devices to which the task will be assigned** 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 **Start** 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.

Een account voor Authenticatie-agent toevoegen via de Webconsole

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

   De lijst met taken wordt geopend.

2. Klik op de taak **Manage Authentication Agent accounts** 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 **Start** 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 **Tasks**.

   De lijst met taken wordt geopend.

2. Klik op de taak **Manage Authentication Agent accounts** 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 **Start** 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 **Tasks**.

   De lijst met taken wordt geopend.

2. Klik op de taak **Manage Authentication Agent accounts** 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 **Start** 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. Selecteer in de beheerconsole **Devices**.

3. Dubbelklik om het venster met de eigenschappen van de computer te openen.

4. Selecteer het gedeelte **Tasks** in het venster met computereigenschappen.

5. Selecteer in de takenlijst **Accounts voor Authenticatie-agent beheren** en open de taakeigenschappen door te dubbelklikken.

6. Selecteer in de taakeigenschappen het gedeelte **Instellingen**.

   U hebt hierdoor toegang tot een lijst met accounts voor Authenticati-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 **Asset management** → **Assets (Devices)**.

2. Klik op de naam van de computer waarop u de lijst met accounts voor Authenticatie-agent wilt bekijken.

3. Selecteer het tabblad **Tasks** in de computereigenschappen.

4. Selecteer in de lijst met taken **Manage Authentication Agent accounts**.

5. Selecteer het tabblad **Application settings** in de taakeigenschappen.

   U hebt hierdoor toegang tot een lijst met accounts voor Authenticati-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

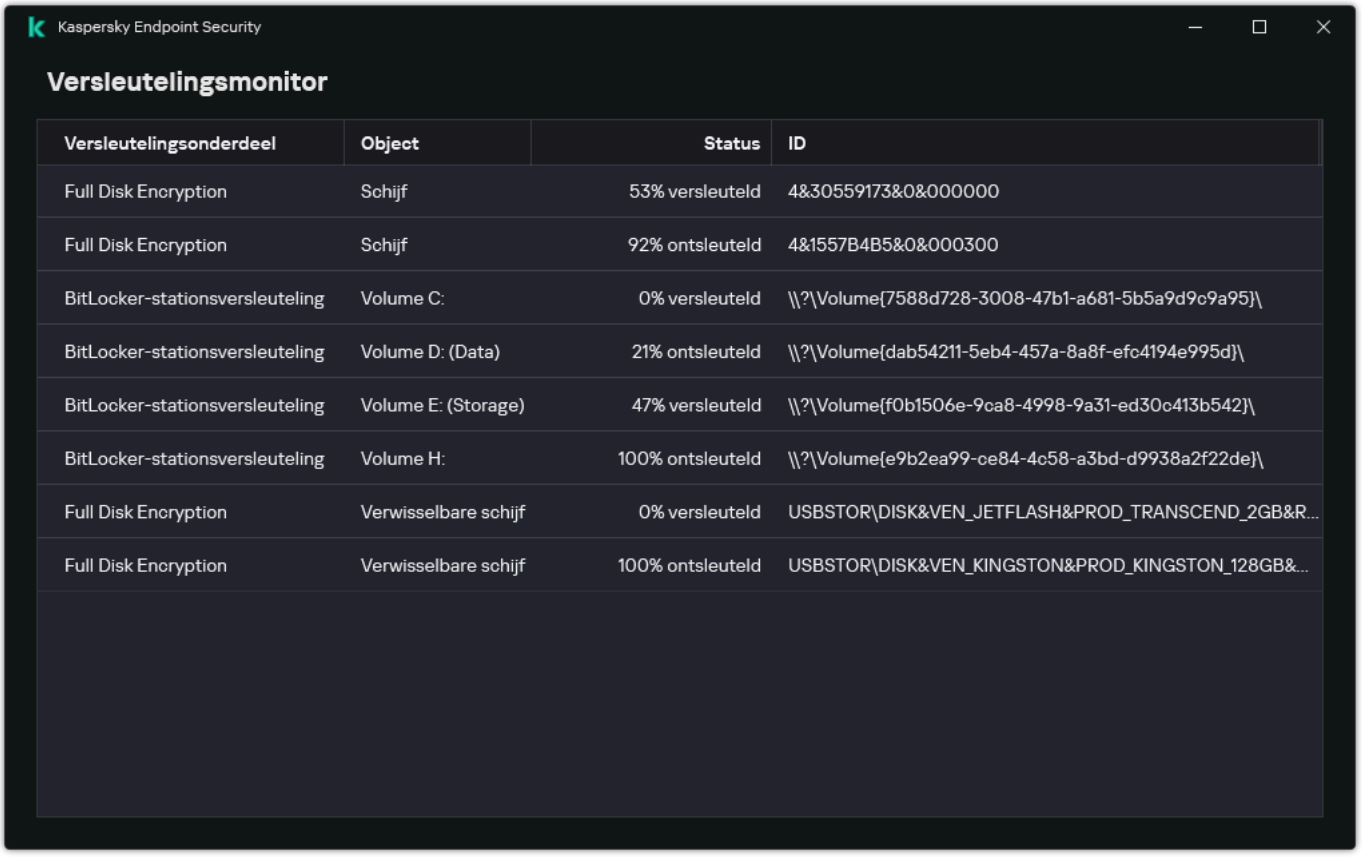
U kunt harde schijven decrypten zelfs als er geen actuele licentie is die gegevensencryptie toestaat.

Zo decrypt u harde schijven:

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Gegevensencryptie** → **Full Disk Encryption** in het beleidsvenster.
4. Selecteer in de vervolgkeuzelijst **Encryptietechnologie** de technologie waarmee de harde schijven zijn geëncrypt.
5. 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.
6. 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.



Versleutelingsmonitor

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 gedecrypt die werden 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.

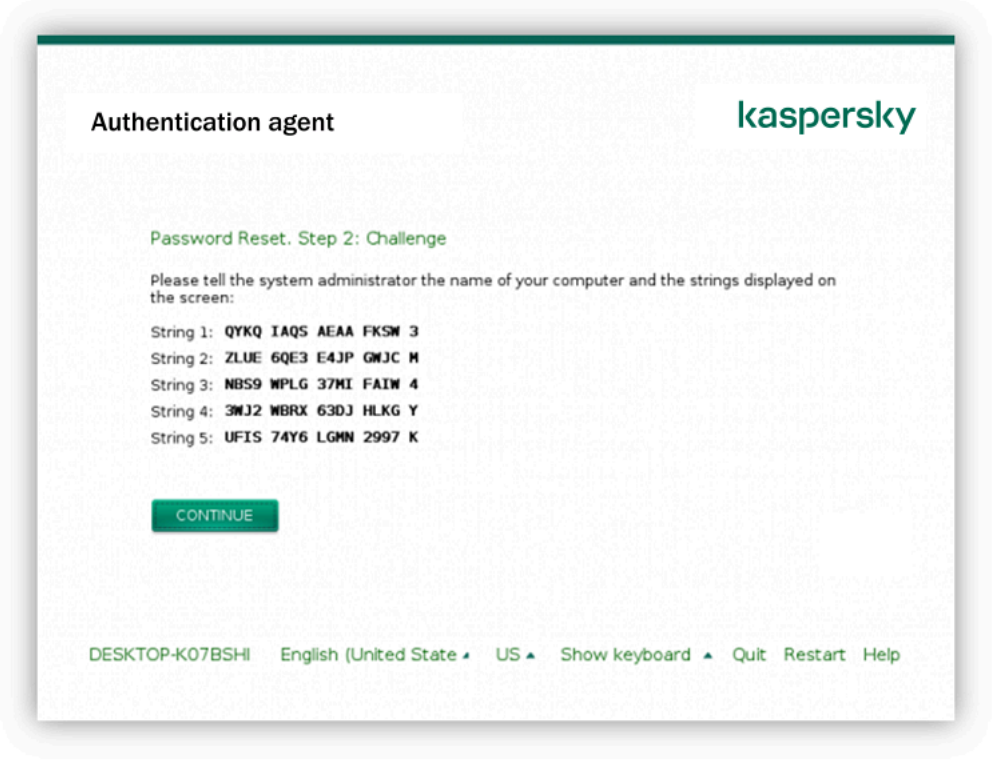
Toegang herstellen tot een schijf beschermd met de Kaspersky Disk Encryption-technologie

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.



Toegang herstellen tot een harde schijf van het systeem beschermd met de Kaspersky Disk Encryption-technologie

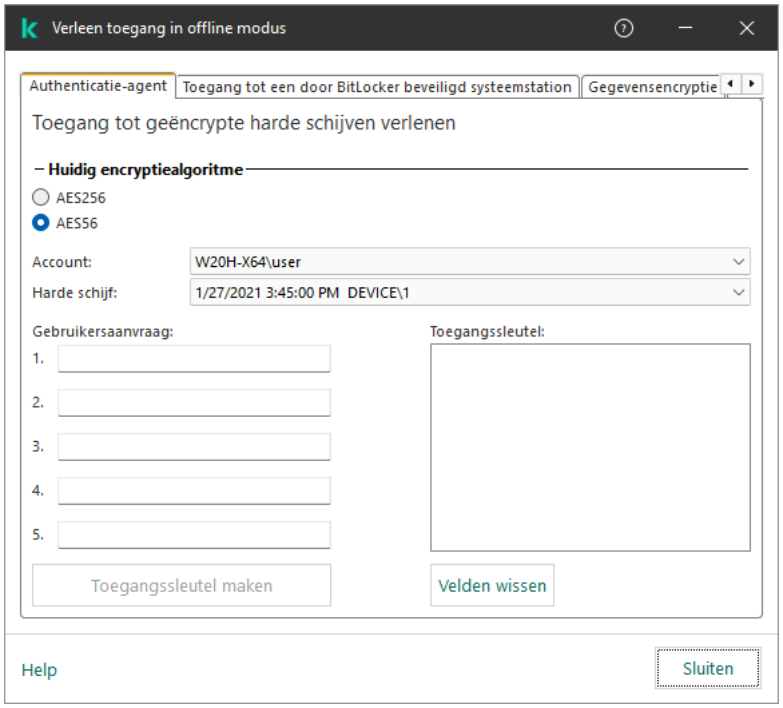
Om de herstelprocedure te starten, moet de gebruiker op de knop **Forgot your password** klikken in de interface van Authenticatie-agent.

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. Selecteer in de beheerconsole **Devices**.
3. 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.
4. Selecteer in het contextmenu de optie **Verleen toegang in offline modus**.
5. Dit opent een venster; selecteer in dat venster het tabblad **Authenticatie-agent**.
6. 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: *Strong encryption (AES256)* of *Lite encryption (AES56)*. De AES-encryptiebibliotheek wordt samen met het programma geïnstalleerd.
7. 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.
8. Selecteer in de vervolgkeuzelijst **Harde schijf** de geëncrypte harde schijf waarvoor u de toegang wilt herstellen.
9. 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.



Toegang verlenen in offline modus

Antwoordblokken verkrijgen voor een systeemschijf beschermd met de Kaspersky Disk Encryption-technologie in de webconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Assets (Devices)**.
2. Schakel het selectievakje in naast de naam van de computer waarvoor u toegang tot de schijf wilt herstellen.
3. Klik op **Grant access to the device in offline mode**.
4. Selecteer in het geopende venster het gedeelte **Authentication 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)

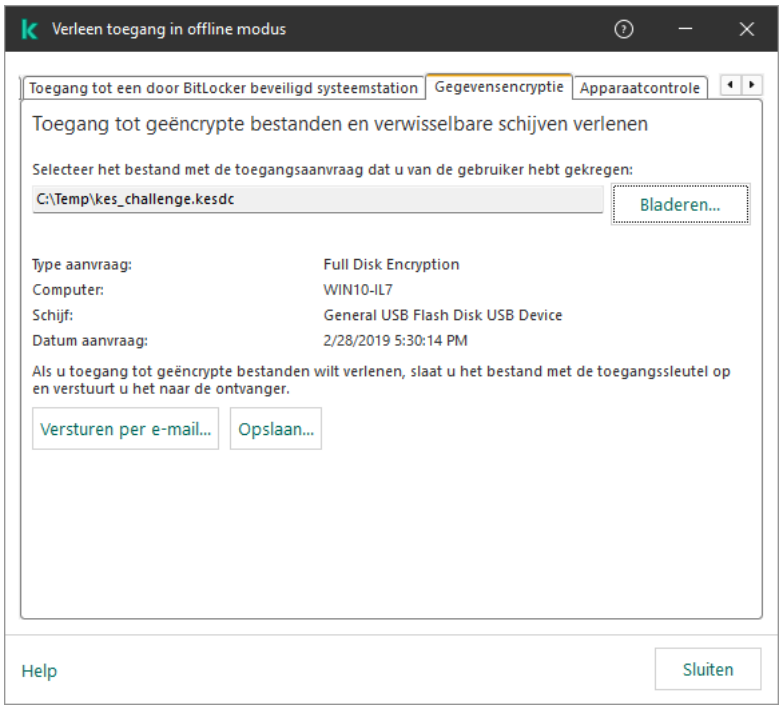
1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de beheerconsole **Devices**.
3. Selecteer op het tabblad **Devices** de computer van de gebruiker die toegang tot de geëncrypte gegevens vraagt en klik rechts om het contextmenu te openen.
4. Selecteer in het contextmenu de optie **Verleen toegang in offline modus**.

5. Dit opent een venster; selecteer in dat venster het tabblad **Gegevensencryptie**.

6. Klik op het tabblad **Gegevensencryptie** op de knop **Bladeren**.

7. 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.



Toegang verlenen in offline modus

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 **Asset management** → **Assets (Devices)**.

2. Schakel het selectievakje in naast de naam van de computer waarvoor u toegang tot de gegevens wilt herstellen.

3. Klik op **Grant access to the device in offline mode**.

4. Selecteer **Data Encryption**.

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 **Save key** 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 authentiseren 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. Selecteer in de beheerconsole **Devices**.
3. Dubbelklik om het venster met de eigenschappen van de computer te openen.
4. Selecteer het gedeelte **Tasks** in het venster met computereigenschappen.
5. Selecteer in de takenlijst **Accounts voor Authenticatie-agent beheren** en open de taakeigenschappen door te dubbelklikken.
6. Selecteer het gedeelte **Instellingen** in het venster met taakeigenschappen.
7. Selecteer in de lijst met accounts de serviceaccount van de authenticatie-agent (bijvoorbeeld `WIN10-USER\ServiceAccount`).
8. Selecteer in de vervolgkeuzelijst **Actie** de optie **Account weergeven**.
9. Selecteer in accounteigenschappen het selectievakje **Oorspronkelijk wachtwoord tonen**.
10. 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 **Asset management** → **Assets (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 **Tasks** in de computereigenschappen.
4. Selecteer in de lijst met taken **Manage Authentication Agent accounts**.
5. Selecteer het tabblad **Application settings** 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 **Show password**.
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 authenticeert. Nadat u zich heeft geathenticeerd 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.

Functies van de update van het besturingssysteem:

- **Besturingssysteem bijwerken via WSUS**. U kunt het besturingssysteem op de gebruikelijke manier bijwerken.
- **Besturingssysteem bijwerken vanaf ISO**. Als u het besturingssysteem wilt bijwerken, moet u de map met de Kaspersky-stuurprogramma's voor schijfversleuteling opgeven. Het programma kopieert de stuurprogramma's automatisch naar een aparte map. Doe het volgende:

  1. Koppel het ISO-image.
  2. Start de installatie van de systeemupdate met de volgende licentie:

     ```
     setup.exe /ReflectDrivers %ProgramFiles(x86)%\Kaspersky Lab\KES.14.1\reflect_drivers
     ```

Automatische update van het besturingssysteem is alleen beschikbaar als de computer Windows 10 1607 (RS1) of hoger gebruikt. Als u een upgrade van oudere versies van het besturingssysteem wilt uitvoeren, wordt aanbevolen dat u eerst de schijf decrypt, een upgrade van het besturingssysteem uitvoert en vervolgens de schijf encrypt.

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 encryptiefunctionaliteit verhelpen

Full Disk Encryption wordt bijgewerkt wanneer een oudere versie van het programma wordt bijgewerkt naar Kaspersky Endpoint Security voor Windows 14.1.

Bij de start van het updateproces voor de functionaliteit Full Disk Encryption kunnen de volgende fouten optreden:

- De update kan niet worden geïnitialiseerd.
- 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,

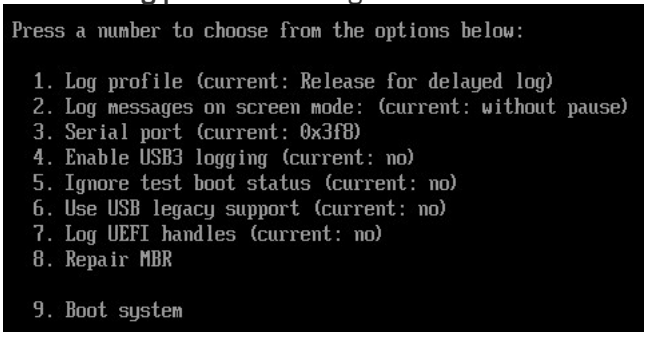
herstelt u de toegang tot geëncrypte apparaten met behulp van de Herstelvoorziening.

De authenticatie-agent traceren

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.

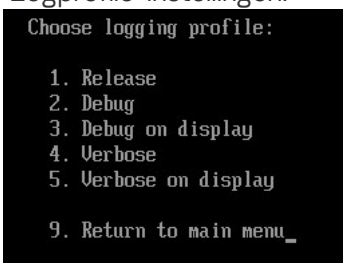
Om Authenticatie-agent-tracering in te schakelen:

1. Kaspersky Endpoint Security Tracering inschakelen.
2. Start de computer opnieuw op.
3. 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.
4. Nadat de FDE-bootloader is gestart, selecteert u de **KES (FDE <version>)** bootmanager.
5. Ga in het bootmanager-menu naar de **Log profile**-instellingen.



Bootmanagermenu

6. Selecteer het tracingniveau in het venster Logprofile-instellingen:



Traceringsniveaus van authenticatie-agent

- **Release**. Als deze optie is geselecteerd, registreert het programma in het tracebestand geen informatie over gebeurtenissen van Authenticatie-agent.
- **Debug**. 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.
- **Debug on display**. 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.
- **Verbose**. 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 **Debug**. De registratie van meer details kan de opstart van Authenticatie-agent en het besturingssysteem vertragen.
- **Verbose on display**. 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 **Debug on display**. De registratie van meer details kan de opstart van Authenticatie-agent en het besturingssysteem vertragen.

Nadat u een traceringsniveau hebt geselecteerd, toont de bootmanager het menu opnieuw.

7. Selecteer in het bootmanagermenu **Boot system**.

   De FDE-bootloader start de Authenticatie-agent.

   Reproduceer het probleem.

   De gegevens worden in het tracebestand van Authenticatie-agent geregistreerd als de computer geëncrypte harde schijven heeft of tijdens een Full Disk Encryption.

8. Keer terug naar het venster Tools voor ondersteuning en schakel tracering uit om het traceringsproces te stoppen

Hierdoor worden tracebestanden gemaakt van de werking van Authenitcation Agent KES.SRV in de map `%ProgramData%\Kaspersky Lab\KES.14.1\Traces`. 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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Gegevensencryptie → Algemene encryptie-instellingen** in het beleidsvenster.
4. In het blok **Sjablonen**, klikt u op de knop **Help**.
5. 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.
6. 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.
7. 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)
- Munteenheidsymbolen (20A0 - 20CF)
- Letterachtige symbolen (2100 - 214F)
- Geometrische figuren (25A0 - 25FF)
- Presentatievormen van Arabisch schrift-B (FE70 - FEFF)

Tekens die niet in deze lijst voorkomen worden niet in een preboot-omgeving ondersteund. U wordt 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.

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

1. Voer het bestand met de naam fdert.exe uit, het uitvoerbare bestand van het Herstelprogramma. Dit bestand wordt door Kaspersky Endpoint Security aangemaakt.

2. Selecteer in het venster Herstelprogramma het vereiste apparaat.

3. Klik op **Scannen**.

4. Als u na de diagnose van de harde schijf van het systeem een bericht ontvangt met de melding dat objecten en gegevens zijn overgebleven van de testwerking van Authentication-agent, klik op **Verwijder AA-objecten en -gegevens**.

   De **Verwijder AA-objecten en -gegevens** is alleen beschikbaar als er objecten en gegevens worden gedetecteerd die na de testwerking van de Authentication-agent zijn achtergebleven.

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 en controleren via de Kaspersky Next-infrastructuur. 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.

Bij het encrypten van de schijf plaatst BitLocker de bootloader en andere hulpbestanden in de system partition. Deze partitie is niet geëncrypt. Het besturingssysteem maakt de systeempartitie automatisch aan tijdens de installatie van Windows. Als de schijf volledig is gepartitioneerd voordat Windows wordt geïnstalleerd, kan het besturingssysteem geen systeempartitie maken. In dit geval wordt u door het besturingssysteem gevraagd de schijf opnieuw te partitioneren en een systeempartitie te maken wanneer u BitLocker schijfversleuteling start. Na het maken van een systeempartitie start het besturingssysteem de BitLocker encryptie.

Het BitLocker-versleutelingsalgoritme is niet afhankelijk van de AES-libraryversie die is inbegrepen in het distributiepakket (AES256 of AES56). Versleuteling maakt gebruik van de ingebouwde versleutelingslibrary van het besturingssysteem.

Het programma gebruikt standaard het BitLocker-versleutelingsalgoritme met een effectieve sleutellengte van 256 bits om apparaten te versleutelen die nog nooit zijn versleuteld. Voor een apparaat dat vóór de installatie van het programma is versleuteld, kan het versleutelingsalgoritme verschillen. Voor gedetailleerde informatie over het selecteren van het versleutelingsalgoritme, zie de Website van de Technische Support van Microsoft. Vanaf versie 12.9 verstuurt Kaspersky Endpoint Security de oorspronkelijke herstelsleutel voor apparaten die eerder zijn versleuteld door programma's van derden naar Kaspersky Security Center.

BitLocker biedt veilige opslag van toegangssleutels met behulp van een vertrouwde platformmodule. Een *Trusted Platform Module* (TPM) is een men 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 de harde schijf van het systeem, moet de gebruiker BitLocker-verificatie doorlopen om het besturingssysteem op te starten. Na de authenticatie staat BitLocker de gebruiker toe zich aan te melden. BitLocker ondersteunt geen technologie voor eenmalige aanmelding (SSO).

Na het encrypten van een schijf, maakt BitLocker een herstelsleutel aan. Kaspersky Endpoint Security stuurt de herstelsleutel naar Kaspersky Security Center zodat u de toegang tot de schijf kunt herstellen, bijvoorbeeld als een gebruiker zijn wachtwoord is vergeten.

Als een gebruiker een schijf van encryptie voorziet met BitLocker, stuurt Kaspersky Endpoint Security de herstelsleutel en informatie over schijfencryptie naar Kaspersky Security Center.

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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Gegevensencryptie** → **Full Disk Encryption** in het beleidsvenster.
4. Selecteer in de vervolgkeuzelijst **Encryptietechnologie** de optie **BitLocker-stationsversleuteling**.
5. 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.

6. Configureer geavanceerde BitLocker-stationsversleutelingsopties (zie onderstaande tabel).
7. Sla uw wijzigingen op.

BitLocker-stationsversleuteling uitvoeren via de Webconsole en Cloudconsole

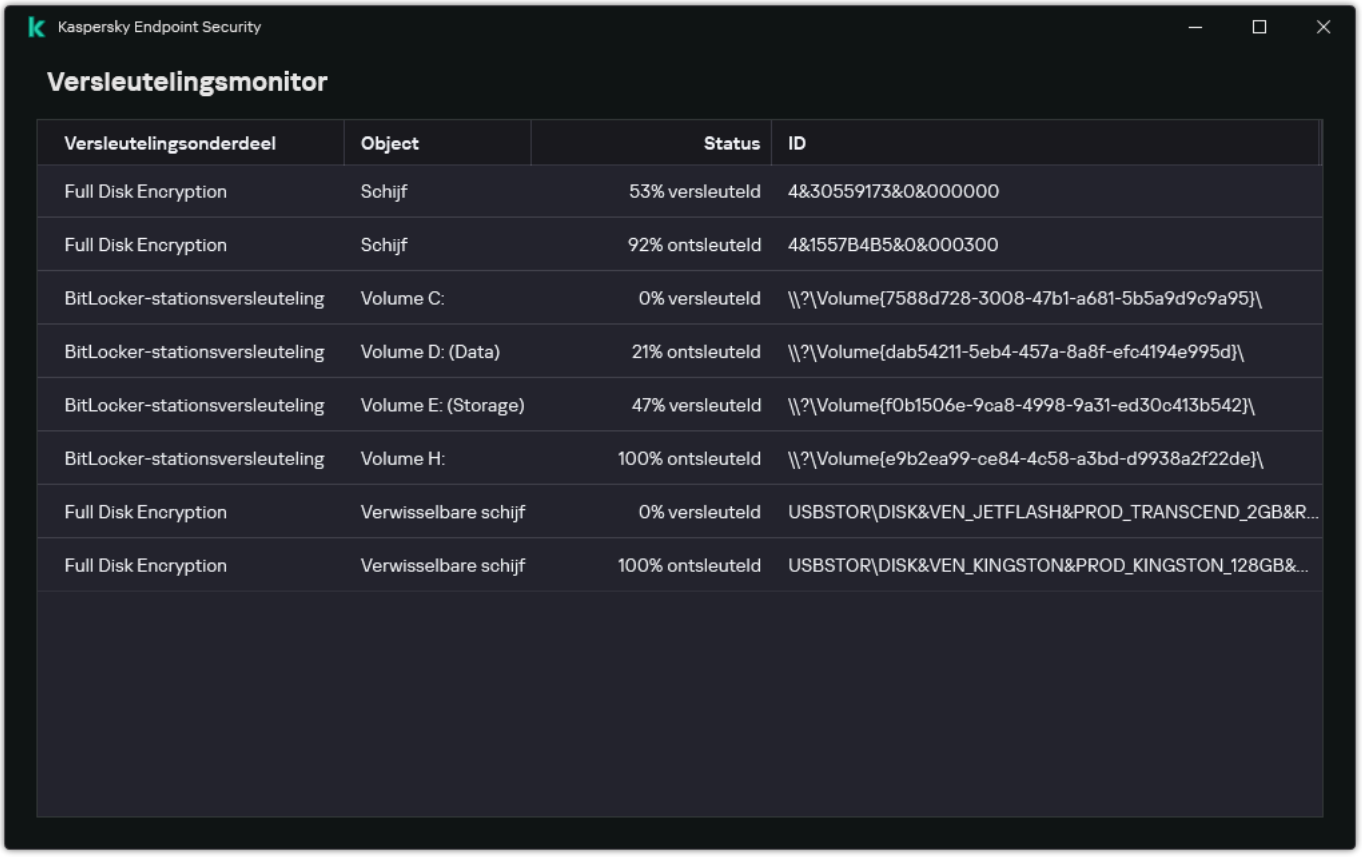
1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.

   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 **BitLocker Disk Encryption**-technologie.
6. Selecteer in het blok **Action on devices 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.

7. Configureer geavanceerde BitLocker-stationsversleutelingsopties (zie onderstaande tabel).
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.



Versleutelingsmonitor

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).

Parameter	Beschrijving
Gebruik van BitLocker-authenticatie inschakelen die preboot-toetsenbordinvoer op tablets vereist	Verificatie gebruiken die gegevensinvoer vereist in een preboot-omgeving, zelfs als het platform geen mogelijkheid heeft voor preboot-invoer (bijvoorbeeld met toetsenborden op aanraakschermen van tablets). 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. Als het selectievakje is ingeschakeld, is het gebruik van een authenticatie met invoer vóór de opstart toegestaan. We raden aan deze instelling alleen te gebruiken voor apparaten die beschikken over alternatieve middelen voor gegevensinvoer vóór de opstart, zoals een USB-toetsenbord naast schermtoetsenborden. Als het selectievakje is uitgeschakeld, is BitLocker-stationsversleuteling niet mogelijk op tablets.
Hardware-encryptie gebruiken (Windows 8 en nieuwer)	Als het selectievakje is ingeschakeld, past het programma een hardware-encryptie toe. Hiermee kunt u sneller encrypten en gebruikt u minder computerbronnen.
Alleen gebruikte schijfruimte encrypten (Windows 8 en nieuwer)	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. De in- of uitschakeling van de functie **Alleen gebruikte schijfruimte encrypten (snellere encryptie)** 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. Het selectievakje is standaard uitgeschakeld.

Parameter	Beschrijving
Authenticatiemethode	**Alleen wachtwoord (Windows 8 en nieuwer)** 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. **Trusted Platform Module (TPM)** Als deze optie is geselecteerd, gebruikt BitLocker een Trusted Platform Module (TPM). Een *Trusted Platform Module* (TPM) is een men 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: • **Pincode gebruiken voor 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. • **Trusted Platform Module (TPM), of wachtwoord als TPM niet beschikbaar is**. Als deze optie 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. De geselecteerde authenticatiemethode moet worden geconfigureerd door wachtwoord- of pincodevereisten op te geven: • **Minimale lengte van pincode (tekens)**. • **Minimale lengte van wachtwoord (tekens)**. • **Geldigheidsduur van wachtwoord / pincode voor TPM beperken (dagen)**. • **Geavanceerde pincode gebruiken (letters en cijfers)**. Met *Geavanceerde pincode* kunt u naast cijfers ook andere tekens gebruiken: hoofdletters en kleine letters, speciale tekens en spaties.
Herstelsleutel automatisch opnieuw maken (dagen)	Werk het wachtwoord automatisch bij om de toegang tot een schijf die wordt beschermd door BitLocker te herstellen. Als het selectievakje is ingeschakeld, geef de geldigheidsperiode van het wachtwoord voor de herstelsleutel op. Dit helpt hergebruik van het wachtwoord voor de herstelsleutel te voorkomen.

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)

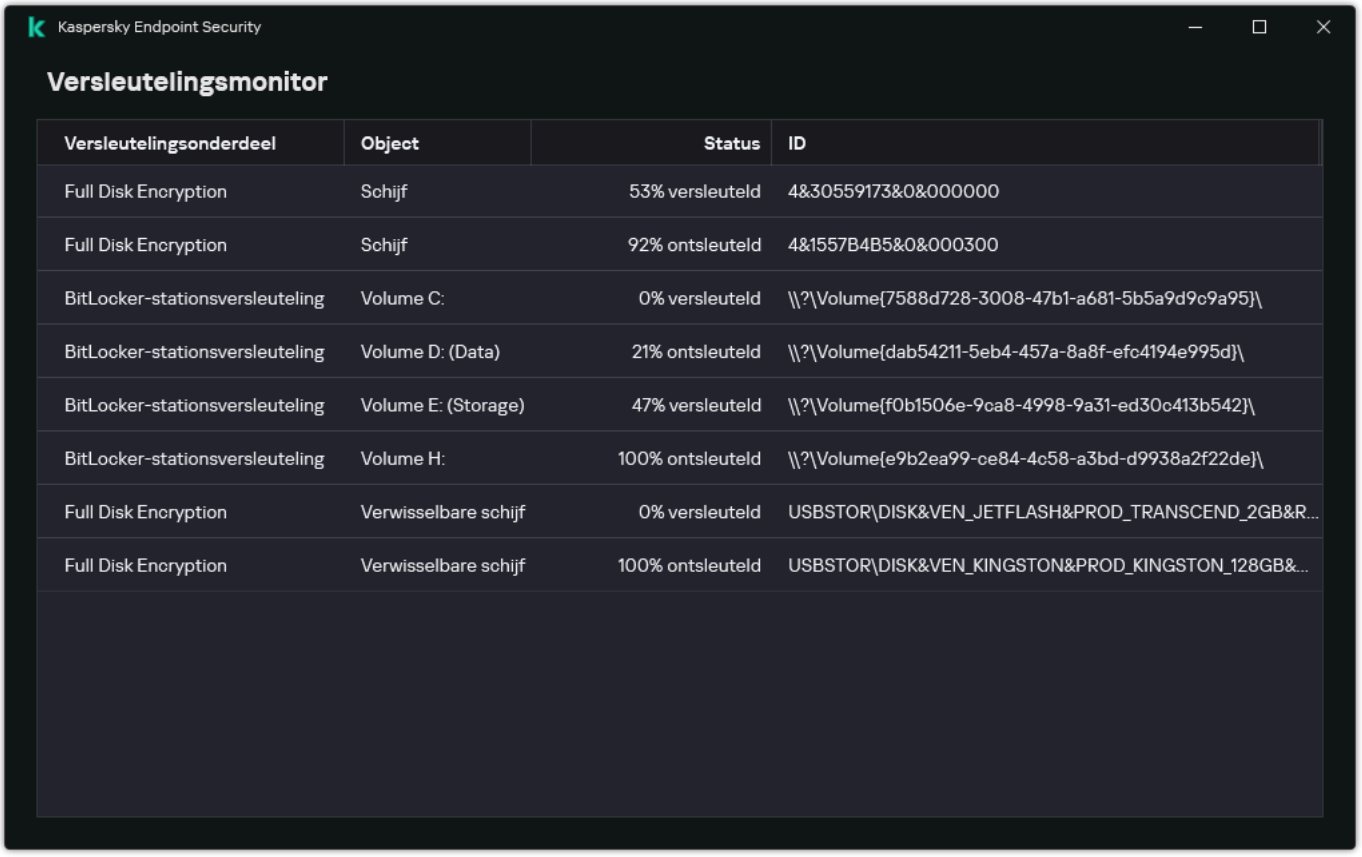
1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Gegevensencryptie** → **Full Disk Encryption** in het beleidsvenster.
4. Selecteer in de vervolgkeuzelijst **Encryptietechnologie** de optie **BitLocker-stationsversleuteling**.

5. Selecteer in de vervolgkeuzelijst **Encryptiemodus** de optie **Alle harde schijven decrypten**.
6. Sla uw wijzigingen op.

Een met BitLocker versleutelde harde schijf decrypten via de webconsole en de cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **BitLocker Disk Encryption**-technologie.
6. Selecteer in het blok **Action on devices Decrypt all hard drives**.
7. 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.



Versleutelingsmonitor

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.

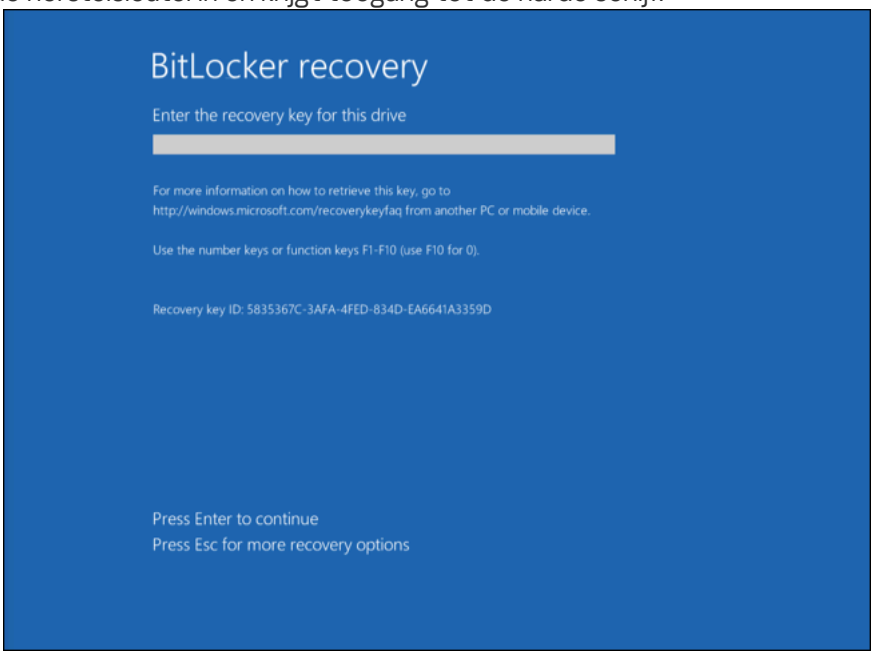
   Een herstelsleutelbestand wordt gebruikt voor computers met de volgende besturingssystemen:

   - Windows 7
   - Windows 8
   - Windows Server 2008
   - Windows Server 2011
   - Windows Server 2012

   Voor alle andere besturingssystemen wordt een herstelsleutel gebruikt.

   Om te voorkomen dat het wachtwoord van de herstelsleutel opnieuw wordt gebruikt, kunt u automatische wachtwoordupdate configureren in de beleidsinstellingen.

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

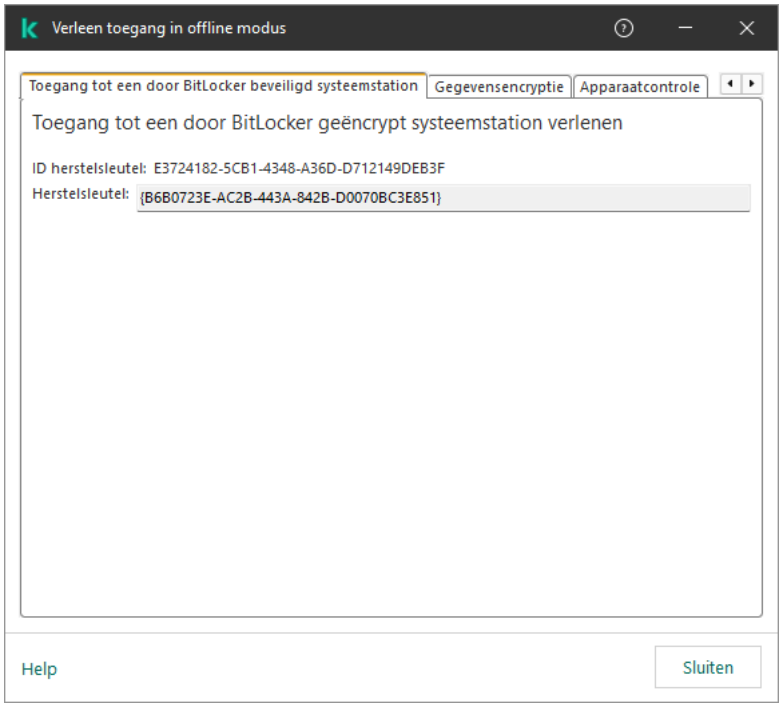
Om de herstelprocedure te starten, moet de gebruiker op de **Esc**-toets drukken tijdens de authenticatiefase vóór het opstarten.

De herstelsleutel bekijken voor een systeemstation geëncrypt met BitLocker in de beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de beheerconsole **Managed devices**.
3. 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.
4. Selecteer in het contextmenu de optie **Verleen toegang in offline modus**.
5. Dit opent een venster; selecteer in dat venster het tabblad **Toegang tot een door BitLocker beveiligd systeemstation**.
6. 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.



Toegang herstellen tot een schijf versleuteld met BitLocker

De herstelsleutel voor een met BitLocker versleuteld systeemstation in de Webconsole en Cloudconsole bekijken

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Assets (Devices)**.
2. Schakel het selectievakje in naast de naam van de computer waarvoor u toegang tot de schijf wilt herstellen.
3. Klik op **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 **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 herstelsleutel 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. In de Beheerconsole structuur, selecteer de map **Advanced → 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**.
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.



Toegang herstellen tot een schijf versleuteld met BitLocker

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 **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. Select de plugin **Kaspersky Endpoint Security for 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 **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-beschermingsbeheer* 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-beschermingsbeheer* 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. Selecteer **Tasks** in de structuur van de Beheerconsole van Kaspersky Security Center.

   De lijst met taken wordt geopend.
2. Klik op **New task**.

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

Stap 1. Een taaktype selecteren

Selecteer **Kaspersky Endpoint Security voor Windows 14.1.** → **BitLocker-beschermingsbeheer**.

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 **Run the task after the wizard finishes** 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 **Asset management** → **Tasks**.

   De lijst met taken wordt geopend.

2. Klik op **Add**.

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

Stap 1. Algemene taakinstellingen configureren

Algemene taakinstellingen configureren:

1. Selecteer **Kaspersky Endpoint Security** in de vervolgkeuzelijst **Application**.
2. Selecteer in de vervolgkeuzelijst **Task type** de optie **BitLocker Protection Management**.
3. Typ in het veld **Task name** een korte omschrijving, zoals *Updaten naar Windows 10*.
4. Selecteer in het gedeelte **Devices to which the task will be assigned** het bereik van de taak.

Stap 2. BitLocker Protection Management

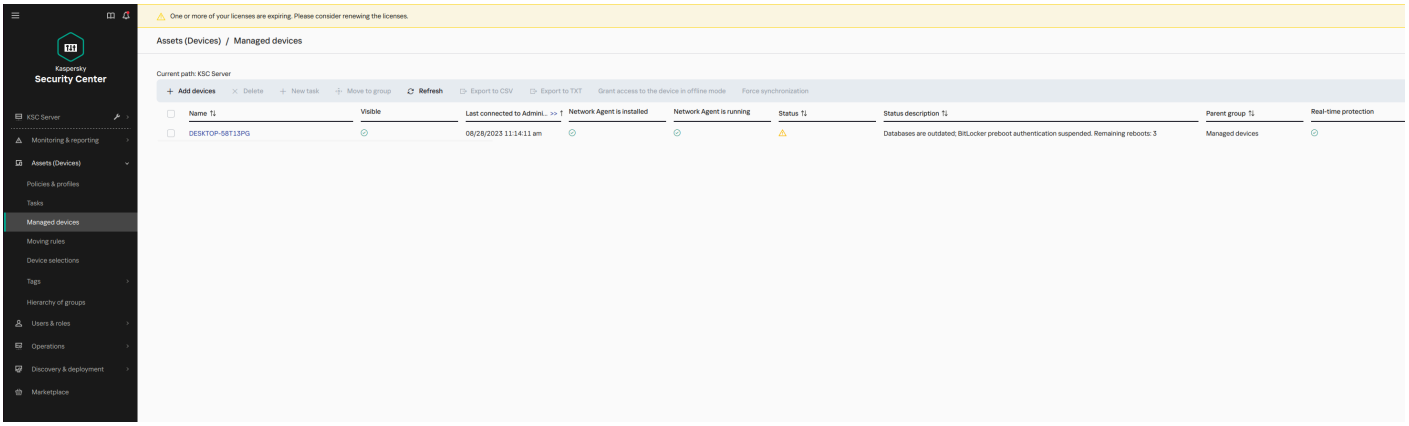
BitLocker-authenticatie configureren Selecteer om BitLocker-authenticatie te pauzeren **Temporarily allow skipping BitLocker authentication** en voer het aantal herstarts in zonder BitLocker-authenticatie (1 tot 15 keer). Voer indien nodig een vervaldatum en -tijd in voor de taak. Op het opgegeven tijdstip 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 **Start** 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 bekijken in de **Managed devices** map van de Kaspersky Security Center-console in de beschrijving van de apparaatstatus.



De lijst met beheerde apparaten

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-beschermingsbeheer* en selecteert u **Authenticatie telkens vóór opstarten vragen**.

File Level Encryption op lokale schijven van de computer

Bestandsencryptie wordt niet ondersteund op Arm-computers.

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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Data Encryption** → **File Level Encryption** in het beleidsvenster.
4. Selecteer in de vervolgkeuzelijst **Encryptiemodus** de optie **Volgens regels**.
5. 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.

        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.

      - **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.

6. 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

Standaard werken alle programma's met geëncrypte bestanden in gedecrypte staat. Als u bepaalde programma's vaak gebruikt (bijvoorbeeld browsers of teksteditors), kunt u geëncrypte regels voor bestandstoegang maken om informatie te beschermen.

We raden aan dat u een regel voor de toegang tot geëncrypte bestanden maakt voor Microsoft Internet Explorer en Microsoft Edge-browsers. Vanwege de manier waarop deze browsers werken, wordt het bestand automatisch geëncrypt als u een geëncrypt bestand uploadt naar een website (bijvoorbeeld cloudopslag). Dit kan een datalek veroorzaken. Het is niet mogelijk om een geëncrypt bestand te uploaden met deze browsers. We raden aan om de **Alleen toegang tot geëncrypte bestanden in ciphertext verlenen** regel in te stellen. U hoeft geen regel voor andere browsers (zoals Google Chrome) te maken.

Zo maakt u toegangsregels voor geëncrypte bestanden voor programma's:

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Data Encryption** → **File Level Encryption** in het beleidsvenster.
4. Selecteer in de vervolgkeuzelijst **Encryptiemodus** de optie **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.

5. Selecteer rechts in het venster het tabblad **Regels voor programma's**.
6. 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 **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**.

7. 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**.

8. 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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.

2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

3. Selecteer **Data Encryption** → **File Level Encryption** in het beleidsvenster.

4. Selecteer in de vervolgkeuzelijst **Encryptiemodus** de optie **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.

5. Selecteer rechts in het venster het tabblad **Regels voor programma's**.

6. 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 **Vernieuwen**.

      In de tabel ziet u programma's die aan de toegepaste filters voldoen.

   c. Schakel in de kolom **Programma** de selectievakjes in naast de programma's die bestanden aanmaken die u wilt encrypten.

   d. Selecteer in de vervolgkeuzelijst **Regel voor programma's** de optie **Alle gemaakte bestanden encrypten**.

   e. Selecteer in de vervolgkeuzelijst **Acties voor programma's die eerder zijn geselecteerd** de actie die Kaspersky Endpoint Security moet uitvoeren op de encryptieregels voor bestanden die eerder voor die programma's zijn gemaakt.

   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**.

7. 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 optie **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**.

8. Sla uw wijzigingen op.

Een decryptieregel genereren

Zo genereert u een decryptieregel:

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Data Encryption** → **File Level Encryption** in het beleidsvenster.
4. Selecteer in de vervolgkeuzelijst **Encryptiemodus** de optie **Volgens regels**.
5. 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.
6. 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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Data Encryption** → **File Level Encryption** in het beleidsvenster.
4. Selecteer rechts in het venster het tabblad **Encryptie**.

5. 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.

6. Maak een decryptielijst voor bestanden.

7. 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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.

2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

3. Selecteer **Gegevensencryptie → Algemene encryptie-instellingen** in het beleidsvenster.

4. In het blok **Wachtwoordinstellingen**, klikt u op de knop **Instellingen**.

5. Dit opent een venster; selecteer in dat venster het tabblad **Geëncrypte pakketten**.

6. Configureer instellingen voor wachtwoordcomplexiteit bij het maken van geëncrypte pakketten.

Controle van wachtwoordsterkte inschakelen bij het maken van geëncrypte archieven in de webconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management → Policies**.

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 **Encrypted package password settings**, configureert u de criteria voor wachtwoordsterkte vereist bij het maken van versleutelde pakketten.

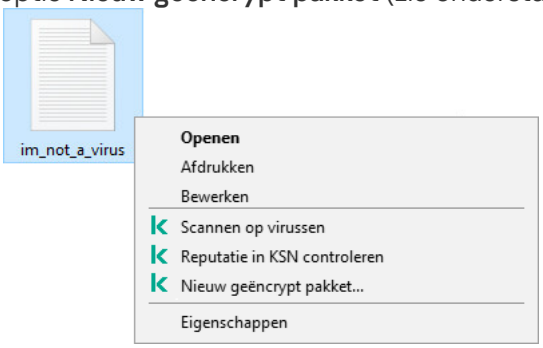
U kunt geëncrypte pakketten maken op computers waarop Kaspersky Endpoint Security is geïnstalleerd en waarop File Level Encryption beschikbaar is.

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).



Een geëncrypt pakket maken

3. Geef in het geopende venster het wachtwoord op en bevestig het.

   Het wachtwoord moet voldoen aan de complexiteitscriteria die in het beleid zijn gespecificeerd.

4. Klik op **Aanmaken**.

   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.

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:

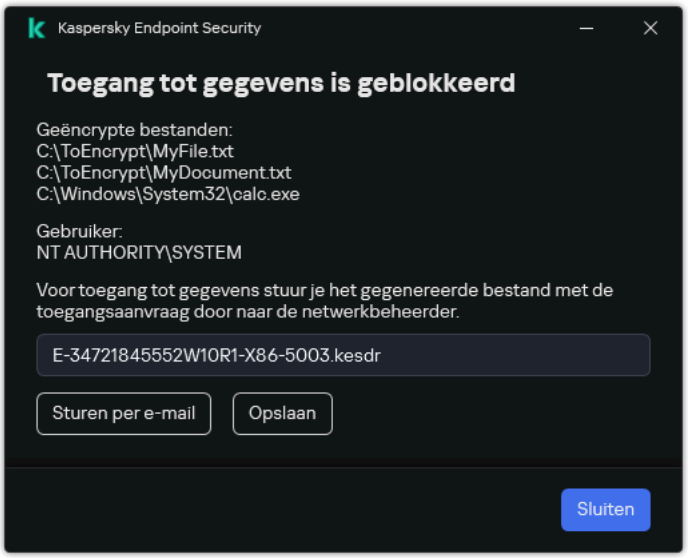
  - De bestanden zitten in geëncrypte pakketten die zijn aangemaakt op een computer waarop Kaspersky Endpoint Security is geïnstalleerd.
  - De bestanden zijn opgeslagen op verwisselbare schijven waarop de portable modus is toegestaan.

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

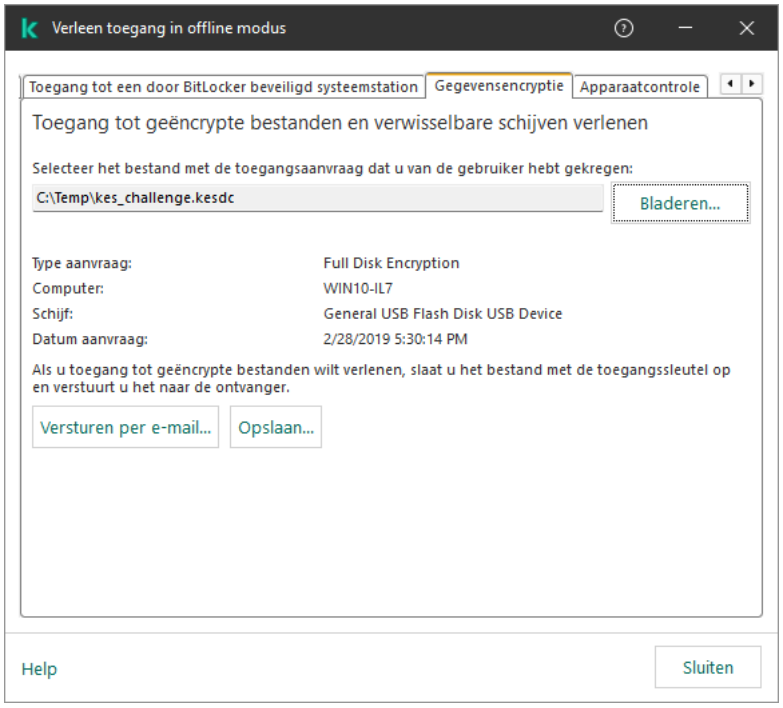
Om de herstelprocedure te starten, moet de gebruiker proberen toegang te krijgen tot een bestand. Als gevolg hiervan zal Kaspersky Endpoint Security een bestand van de toegangsaanvraag maken (een bestand met de extensie KESDC), dat de gebruiker bijvoorbeeld per e-mail naar de beheerder moet sturen.

Kaspersky Endpoint Security genereert een bestand van de toegangsaanvraag 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. Selecteer in de beheerconsole **Devices**.
3. 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.
4. Selecteer in het contextmenu de optie **Verleen toegang in offline modus**.
5. Dit opent een venster; selecteer in dat venster het tabblad **Gegevensencryptie**.
6. Klik op het tabblad **Gegevensencryptie** op de knop **Bladeren**.
7. 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.



Toegang verlenen in offline modus

Hoe een bestand met toegangssleutel voor geëncrypte bestanden verkrijgt in de webconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Assets (Devices)**.
2. Schakel het selectievakje in naast de naam van de computer waarvoor u toegang tot de gegevens wilt herstellen.
3. Klik op **Grant access to the device in offline mode**.
4. Selecteer **Data Encryption**.
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 **Save key** 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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Gegevensencryptie** → **Algemene encryptie-instellingen** in het beleidsvenster.
4. In het blok **Sjablonen**, klikt u op de knop **Sjablonen**.
5. 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 volgende venster 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 (zie onderstaande afbeelding). Door te klikken op de knop **Sturen per e-mail** wordt automatisch een gebruikersbericht gemaakt. Dit bericht wordt naar de netwerkbeheerder van het bedrijf verstuurd samen met het bestand met de aanvraag voor toegang tot geëncrypte bestanden.

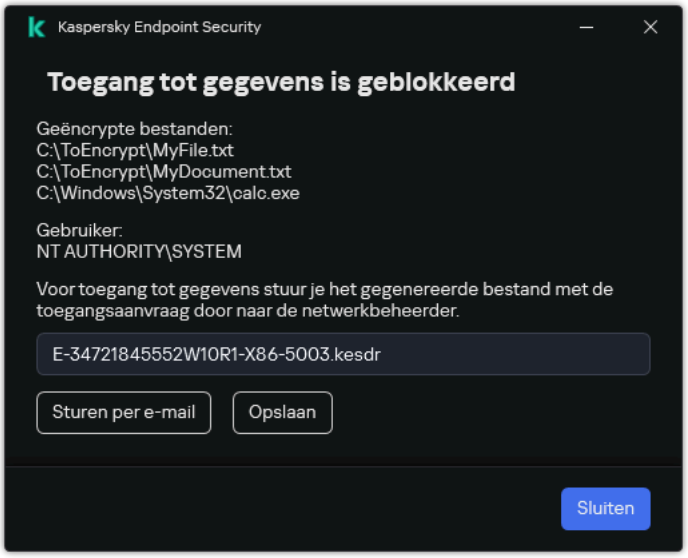
   - Als u de sjabloon van het bericht van de beheerder wilt bewerken, selecteert u het tabblad **Bericht van beheerder**. De gebruiker ontvangt dit bericht nadat toegang tot gecodeerde bestanden is verleend.

6. Bewerk de sjablonen van de berichten.

   Als u een variabele aan de sjabloontekst wilt toevoegen, plaats dan de cursor op de gewenste positie, klik op **Variabele** en selecteer de gewenste variabele in de lijst met beschikbare opties.

   U kunt de standaardsjabloontekst ook herstellen met de knop **Standaard**.

7. Sla uw wijzigingen op.



Toegang tot geëncrypte gegevens herstellen

Encryptie van verwisselbare schijven

Versleuteling van verwisselbare schijven wordt niet ondersteund op Arm-gebaseerde computers.

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

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 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.

Voordat u bestanden op een verwisselbare schijf versleutelt, moet u ervoor zorgen dat deze is geformatteerd en dat er geen verborgen partities zijn (zoals een EFI-systeempartitie). Als de schijf niet-geformatteerde of verborgen partities bevat, kan de bestandscodering mislukken met een fout.

Zo encrypt u verwisselbare schijven:

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Gegevensencryptie** → **Encryptie van verwisselbare schijven** in het beleidsvenster.
4. 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.

5. 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.

6. 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.

7. Definieer encryptieregels als u encryptie voor afzonderlijke verwisselbare schijven wilt configureren.

8. 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.

9. Sla uw wijzigingen op.

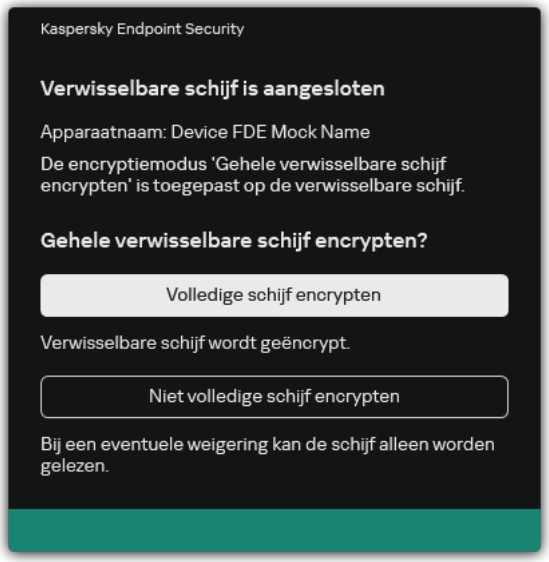
Wanneer het beleid is toegepast en de gebruiker een verwisselbare schijf aansluit, of als er al een verwisselbare schijf is aangesloten, zal de gebruiker door Kaspersky Endpoint Security worden gevraagd om de encryptie te bevestigen (zie onderstaande afbeelding).

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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Gegevensencryptie → Encryptie van verwisselbare schijven** in het beleidsvenster.
4. 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**.
5. 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.
6. 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.
7. 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 beschermd zijn, 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.

8. 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**.

9. 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. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **<N> 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 koppeling **Import**.

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.

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.

2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

3. Selecteer **Gegevensencryptie → Encryptie van verwisselbare schijven** in het beleidsvenster.

4. 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 koppeling **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.

5. De lijst met encryptieregels voor verwisselbare schijven importeren:

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.

6. 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:

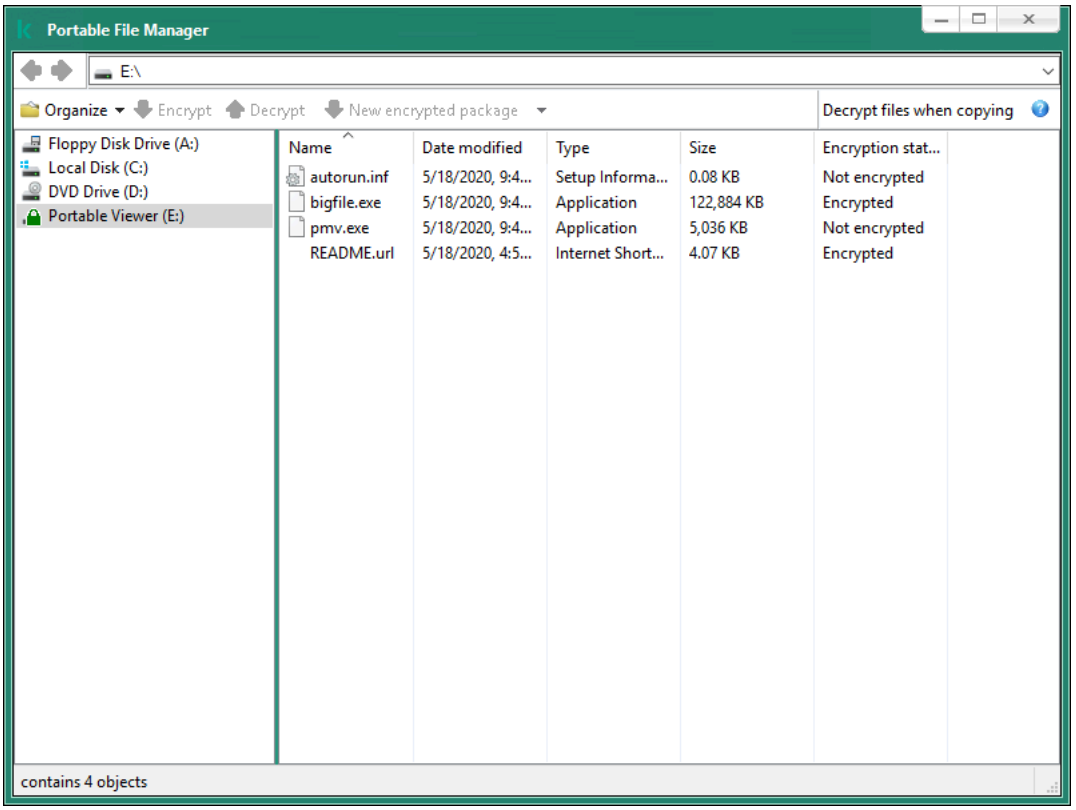
- Er is geen verbinding tussen de computer en de Kaspersky Security Center Administration Server.
- De infrastructuur is veranderd met de wijziging van de Kaspersky Security Center Administration Server.
- Kaspersky Endpoint Security is niet op de computer geïnstalleerd.

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

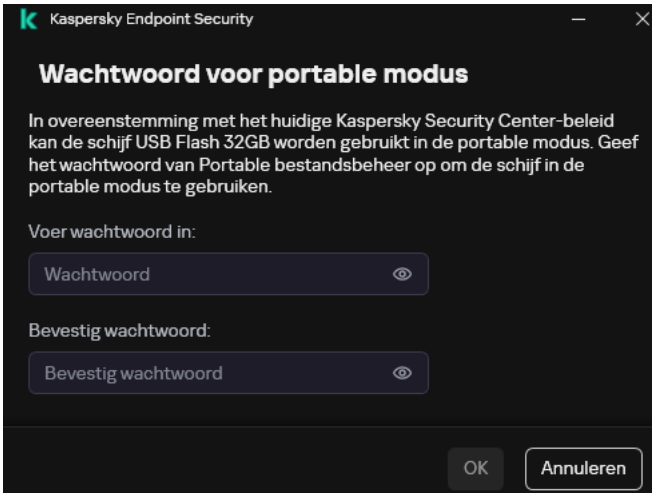
Ondersteuning voor portable modus inschakelen voor het werken met geëncrypte bestanden op verwisselbare schijven in de beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Gegevensencryptie → Encryptie van verwisselbare schijven** in het beleidsvenster.
4. 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).

5. Selecteer het selectievakje **Portable modus**.
6. Voeg indien nodig encryptieregels toe voor individuele verwisselbare schijven.
7. Sla uw wijzigingen op.
8. Sluit de verwisselbare schijf aan op de computer nadat u het beleid hebt toegepast.
9. Bevestig de encryptie van de verwisselbare schijf.

U ziet nu een venster waarin u een wachtwoord voor Portable bestandsbeheer kunt aanmaken.



Wachtwoord voor portable modus

10. Geef een wachtwoord op dat sterk genoeg is en bevestig het.
11. Sla uw wijzigingen op.

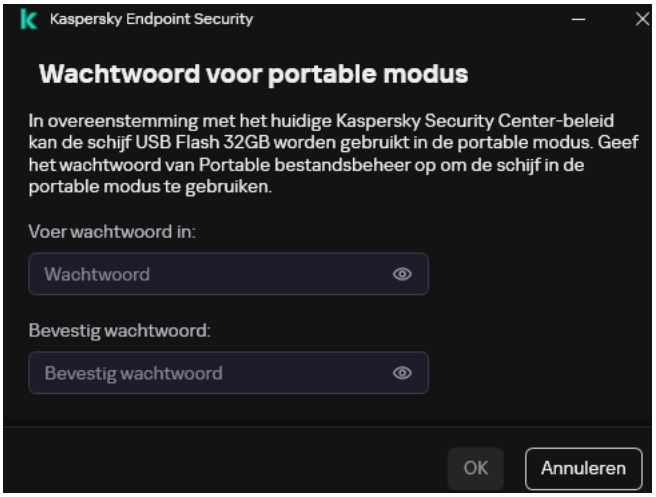
Ondersteuning voor portable modus inschakelen voor het werken met geëncrypte bestanden op verwisselbare schijven in de webconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Default action Encrypt all files** of **Encrypt new files only**.

   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. Selecteer het selectievakje **Portable mode**.
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.



Wachtwoord voor portable modus

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 (zie onderstaande afbeelding).

- 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.



Geëncrypte bestanden op een verwisselbare schijf openen

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).

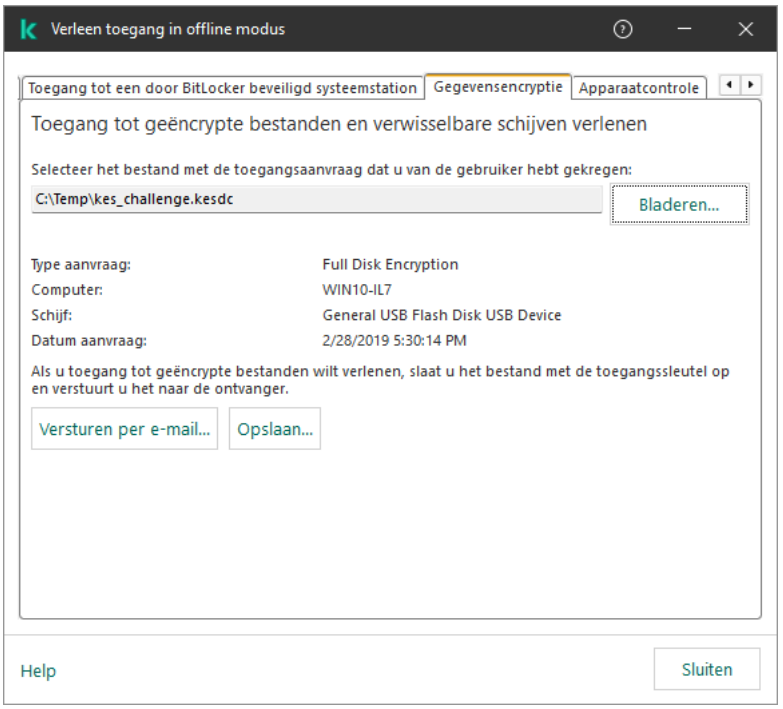
  Nadat u de procedure van aanvraag en antwoord voor wachtwoordherstel hebt voltooid, ontvangt u transparante toegang tot de bestanden op de verwisselbare schijf en volledige toegang tot de verwisselbare schijf (lees- en schrijfmachtiging).

  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. Selecteer in de beheerconsole **Devices**.
  3. 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.
  4. Selecteer in het contextmenu de optie **Verleen toegang in offline modus**.
  5. Dit opent een venster; selecteer in dat venster het tabblad **Gegevensencryptie**.
  6. Klik op het tabblad **Gegevensencryptie** op de knop **Bladeren**.
  7. 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.



Toegang verlenen in offline modus

Een geëncrypt gegevenstoegangsbestand verkrijgen in de webconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Assets (Devices)**.
2. Schakel het selectievakje in naast de naam van de computer waarvoor u toegang tot de gegevens wilt herstellen.
3. Klik op **Grant access to the device in offline mode**.
4. Selecteer **Data Encryption**.
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 **Save key** 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. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Gegevensencryptie → Encryptie van verwisselbare schijven** in het beleidsvenster.
4. Als u alle geëncrypte bestanden op verwisselbare schijven wilt decrypten, selecteert u in de vervolgkeuzelijst **Encryptiemodus** de optie **Gehele verwisselbare schijf decrypten**.
5. 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. In het contextmenu van de **Een regel instellen** knop, selecteer het **Gehele verwisselbare schijf decrypten** item.
6. 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 bekijken

U kunt de status bekijken om gegevensversleuteling te controleren. Kaspersky Endpoint Security wijst de volgende encryptiestatussen toe:

- **Does not meet the policy; canceled by user**. De gebruiker heeft gegevensencryptie geannuleerd.
- **Does not meet the policy due to an error**. Fout gegevensencryptie, er ontbreekt bijvoorbeeld een licentie.
- **Applying the policy; restart is required**. De encryptie van gegevens wordt op de computer uitgevoerd. Start de computer opnieuw op om de gegevensencryptie te voltooien.
- **No encryption policy specified**. Gegevensencryptie wordt uitgeschakeld in beleidsinstellingen.
- **Not supported**. Componten gegevensencryptie zijn niet geïnstalleerd op de computer.
- **Applying the policy**. De encryptie en / of decryptie van gegevens wordt op de computer uitgevoerd.

Zo bekijkt u de encryptiestatus van gegevens op de computer:

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de beheerconsole **Managed devices**.
3. Schuif op het tabblad **Devices** in de werkruimte de schuifbalk helemaal naar rechts. Als de kolom **Encryption status** kolom niet wordt weergegeven, voeg deze kolom dan toe in de console-instellingen van Kaspersky Security Center.

   In de kolom **Encryption status** 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.
4. Als de status van gegevensencryptie voor de computer **Applying policy**, is, dan kunt u het voortgangspaneel van de encryptie volgen:

   a. Open de eigenschappen van de computer met de status **Applying policy** door erop te dubbelklikken.

   b. Selecteer het gedeelte **Applications** in het venster met computereigenschappen.

   c. Selecteer in de lijst met Kaspersky-programma's geïnstalleerd op de computer **Kaspersky Endpoint Security for Windows**.

   d. Klik op **Statistics**.

   e. Onder **Encryption of devices** kunt u de huidige vooruitgang zien van gegevensencryptie als een percentage.

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 **Add**.
   c. Dit opent een venster. Voer in dat venster de naam van de pagina 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. Selecteer in de beheerconsole **Managed devices**.
3. Selecteer op het tabblad **Devices** de naam van de computer in de lijst en klik er met de rechtermuisknop op om het contextmenu te openen.
4. Selecteer in het contextmenu van de computer het item **Properties**. Selecteer in het geopende venster het gedeelte **Protection**.
5. Klik op de link **View data encryption errors Data encryption errors** 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

Met Kaspersky Security Center kunt u rapporten over gegevensencryptie maken:

- **Report on encryption status of managed devices**. Het rapport bevat informatie over of de encryptiestatus van de computer voldoet aan het encryptiebeleid.
- **Report on encryption status of mass storage devices**. Het rapport bevat informatie over de encryptiestatus van externe apparaten en opslagapparaten.
- **Report on rights to access encrypted drives**. Het rapport bevat informatie over de status van accounts die toegang hebben tot versleutelde schijven.
- **Report on file encryption errors**. Het rapport bevat informatie over fouten die optraden tijdens de uitvoering van taken van gegevensencryptie of decryptie op computers.
- **Report on blockage of access to encrypted files**. Het rapport bevat informatie over programma's die worden geblokkeerd om toegang te krijgen tot versleutelde bestanden.

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 rapporten over gegevensencryptie.

   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.

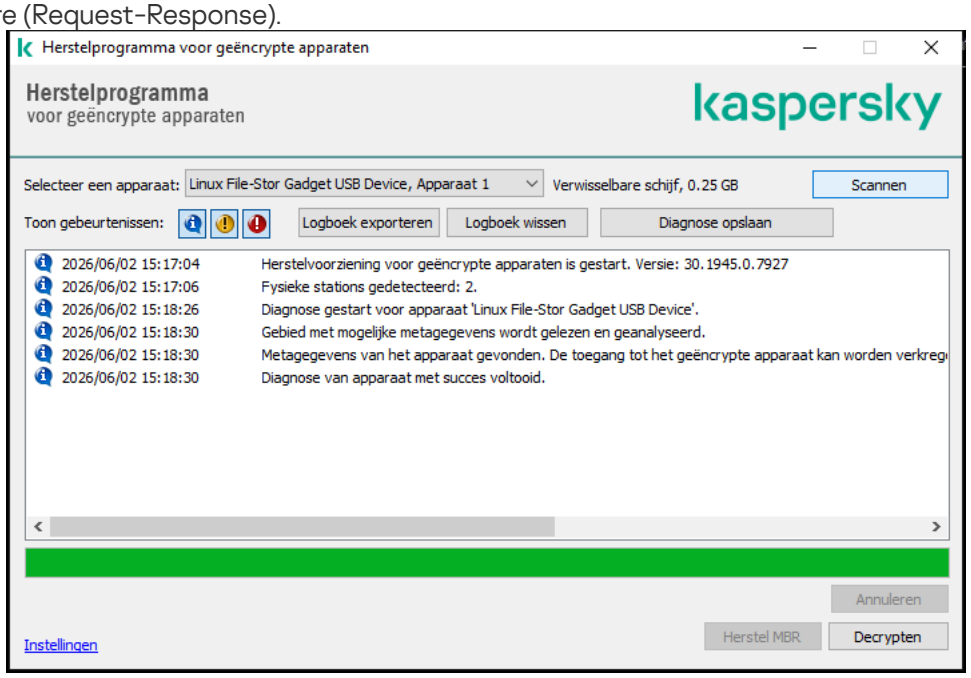
Gegevens herstellen met behulp van de FDERT Restore Utility

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 zelfstandige 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 encryptiefunctionaliteit van Kaspersky Endpoint Security, wordt u door de Herstelvoorziening gevraagd om het apparaat te ontgrendelen. Hoewel het ontgrendelen van het apparaat het niet decrypt, wordt het apparaat onmiddellijk toegankelijk omdat het wordt ontgrendeld. Als de computer geen toegang heeft tot de encryptiefunctionaliteit van Kaspersky Endpoint Security, wordt u door de Herstelvoorziening gevraagd om het apparaat te decrypten.

4. 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 toegangsaanvraag op in het computergeheugen (een bestand met de extensie FDERTC).

   c. Stuur het bestand met de toegangsaanvraag 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. In de Beheerconsole structuur, selecteer de map **Advanced → 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**.

    Als u niet zeker weet voor welke computer het bestand met toegangsverzoeken is gegenereerd, selecteert u in de Beheerconsole structuur de **Advanced → Data encryption and protection** map en in de werkruimte, klik **Krijg encryptiesleutel voor apparaat in Kaspersky Endpoint Security**.

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: *Strong encryption (AES256)* of *Lite encryption (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 **Ontgrendelen**.

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 **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: *Strong encryption (AES256)* of *Lite encryption (AES56)*. De AES-encryptiebibliotheek wordt samen met het programma geïnstalleerd.

   c. Selecteer het bestand van de toegangsaanvraag dat u van de gebruiker hebt ontvangen (een bestand met de extensie FDERTC).

   d. 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 Detection and Response-oplossingen zijn beveiligingssystemen die geavanceerde bedreigingen en aanvalsindicatoren detecteren op verschillende niveaus van de infrastructuur van een organisatie. Detection and Response-oplossingen geven informatie over de gedetecteerde dreiging en maken beheer van Threat Response-acties mogelijk.

De Detection and Response-oplossing doet dus het volgende:

- Informatie ontvangen over de werking van een computer, server of andere apparaten (telemetrie).
- De informatie automatisch analyseren om dreigingen te detecteren.
- Waarschuwingsdetails genereren als kolommen van de keten van dreigingsontwikkeling voor analyse en het kiezen van Threat Response-acties.
- Threat Response-acties uitvoeren (bijvoorbeeld netwerkisolatie van de computer).

Kaspersky Endpoint Security ondersteunt Detection and Response oplossingen met behulp van een ingebouwde agent. De ingebouwde agent stuurt telemetrie naar servers van oplossingen en voert Threat Response-acties uit. 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 Anti Targeted Attack Platform:
  - Endpoint Detection and Response (EDR) versie 7.1 of eerder
  - Network Detection and Response (NDR)
  - KATA Sandbox
- Kaspersky Endpoint Detection and Response Expert (on-premises)
- Kaspersky Sandbox 2.0

U kunt Kaspersky Endpoint Security met Detection and Response-oplossing in verschillende configuraties gebruiken, bijvoorbeeld [EDR Optimum+MDR].

MDR en EDR Optimum-licenties

Kaspersky Endpoint Security ondersteunt de functionaliteit van de Kaspersky Managed Detection and Response (MDR) en Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) oplossingen. U kunt Kaspersky Endpoint Security met deze oplossingen in verschillende configuraties gebruiken en een aangepast beveiligingssysteem bouwen dat aan uw specifieke vereisten voldoet. Om dit te doen, moet u een licentie aanschaffen voor elk van de oplossingen. De licentie kan betrekking hebben op het recht om een enkele oplossing (bijvoorbeeld alleen MDR Add-on) of meerdere oplossingen, [EDR Optimum+MDR] Add-on, te gebruiken.

MDR en EDR Optimum ondersteunen de volgende licentiemethoden:

- De MDR of EDR Optimum-functionaliteit is inbegrepen in de Kaspersky Endpoint Security for Windows-licentie.

  De functionaliteit is onmiddelijk beschikbaar na de activering van Kaspersky Endpoint Security voor Windows. U hoeft slechts één sleutel toe te voegen.

- Aparte licenties voor MDR of EDR Optimum (MDR Add-on, EDR Optimum Add-on, [EDR Optimum+MDR] Add-on).

  De functionaliteit komt beschikbaar na het toevoegen van een aparte sleutel voor MDR Add-on, EDR Optimum Add-on of [EDR Optimum+MDR] Add-on. Hierdoor worden er twee sleutels op de computer toegevoegd: een sleutel voor Kaspersky Endpoint Security en een sleutel voor MDR of EDR Optimum. De Kaspersky Endpoint Security-sleutel moet als eerste worden toegevoegd.

Kaspersky Endpoint Security staat het toevoegen van slechts één *actieve sleutel* toe voor MDR- en EDR Optimum-licenties. Als u beide oplossingen moet activeren, moet u daarom één [EDR Optimum+MDR] Add-on-sleutel toevoegen in plaats van een afzonderlijke sleutel voor elke oplossing. U kunt ook één *reservecodes* toevoegen.

Als je een BLOB-bestand hebt gebruikt bij het implementeren van MDR, heb je geen aparte sleutel nodig om MDR te activeren. Het BLOB-bestand bevat al licentie-informatie.

Initiële licentiebeheer van oplossingen

Bij de eerste implementatie van MDR en EDR Optimum worden de oplossingen op dezelfde manier geactiveerd als de Kaspersky Endpoint Security-programma. U kunt een sleutel toevoegen met de *Licentie toevoegen* taak of gebruik de functie voor automatische sleuteldistributie. De licentiesleutel wordt aan het programma toegevoegd als een tweede actieve sleutel of als een reservesleutel als u het betreffende selectievakje inschakelt.

Overstappen van de ene licentie naar de andere

Als uw organisatie al een van deze oplossingen heeft geïmplementeerd en de bijbehorende sleutel aan het programma heeft toegevoegd, zijn er enkele speciale overwegingen bij het licentiebeheer van de nieuwe configuratie. Bij het overschakelen naar een andere licentie, voegt het programma de nieuwe sleutel niet toe aan het programma, maar vervangt de huidige sleutel door de nieuwe sleutel. De reden hiervan is de beperking waardoor het programma slechts één sleutel kan toevoegen om MDR en EDR Optimum te activeren.

Stel voor dat uw organisatie de [EDR Optimum+MDR] oplossing heeft geïmplementeerd en u heeft besloten om over te schakelen op de MDR Add-on configuratie. Om over te schakelen naar de nieuwe configuratie, moet u de [EDR Optimum+MDR] Add-on-sleutel vervangen door de MDR Add-on-sleutel.

Een aparte licentie voor EDR Optimum en MDR ([EDR Optimum+MDR] Add-on) is niet meer beschikbaar. Als u beide oplossingen wilt gebruiken, moet u MDR activeren met een BLOB-bestand en EDR Optimum met een licentiesleutel.

Met de automatische functie sleuteldistributie weigert het programma licentiesleutels die hetzelfde aantal oplossingen dekken. Dat wil zeggen, als u een EDR Optimum Add-on-sleutel hebt toegevoegd, kunt u deze sleutel niet vervangen door een MDR Add-on-sleutel. U kunt de EDR Optimum Add-on-sleutel echter vervangen door een [EDR Optimum+MDR] Add-on-sleutel. Het programma weigert ook sleutels als u een MDR Add-on-sleutel probeert te vervangen door een EDR Add-on-sleutel. Om een sleutel te vervangen, kunt u de *Licentie toevoegen* taak uitvoeren. De *Licentie toevoegen* task maakt het mogelijk om licentiesleutels te vervangen door een willekeurig aantal oplossingen.

Als u een [EDR Optimum+MDR] Add-on-reservesleutel heeft toegevoegd, moet u, om correct een actieve sleutel voor EDR Optimum Add-on of MDR Add-on toe te voegen, eerst de reservesleutel vervangen door een EDR Optimum Add-on of MDR Add-on key, of verwijder de reservesleutel en vervang vervolgens de actieve sleutel.

Compatibiliteit met oplossingen van derden EDR

U kunt Kaspersky Endpoint Security gebruiken om werkstations en servers te beschermen in combinatie met EDR-oplossingen van derden. Om false positives te voorkomen, raden we aan dat u uitvoerbare bestanden van Kaspersky Endpoint Security en Network Agent toevoegt aan de vertrouwde zone van uw EDR-oplossing van derden.

Vertrouwde zone voor compatibiliteit met EDR-oplossingen van derden

	Kaspersky Endpoint Security voor Windows	Kaspersky Security Center Network Agent
Werkmap	`C:\Program Files (x86)\Kaspersky Lab\KES.14.1.0`	`C:\Program Files (x86)\Kaspersky Lab\NetworkAgent`

Uitvoerbare bestanden	`avp.exe`
	`avp.com`
	`avpsus.exe`
	`avpui.exe`
	`dump_writer_agent.exe`
	`kescli.exe`
	`kesdr.exe`
	`kldw.exe`
	`klpsm.exe`
	`kvdb_upgrader.exe`
	`modify_watcher.exe`
	`pmv.exe`
	`remediation.exe`
	`service_stub.exe`
		`AVPDTAgt.exe`
		`fix_gflags.exe`
		`getsysteminfo.exe`
		`integrity_checker.exe`
		`klcpuld.exe`
		`klcsldcl.exe`
		`klcsngtgui.exe`
		`klcspxy.exe`
		`kldumper.exe`
		`klmover.exe`
		`klnagchk.exe`
		`klnagent.exe`
		`klnagntf.exe`
		`klnagwds.exe`
		`klosprep.exe`
		`klrbtagt.exe`
		`klscflag.exe`
		`klscmodchk.exe`
		`klshwmsg.exe`
		`klwd.exe`
		`ksnproxy.exe`
		`Patch.exe`
		`tslauncher.exe`
		`Up2Date.exe`
		`vapm.exe`

Kaspersky Endpoint Agent

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 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

De distributiekit voor Kaspersky Endpoint Security versies 11.2.0 – 11.8.0 bevat Kaspersky Endpoint Agent. U kunt Kaspersky Endpoint Agent selecteren bij het installeren van Kaspersky Endpoint Security voor Windows. Als gevolg hiervan worden twee programma's op uw computer geïnstalleerd: KEA en KES. In Kaspersky Endpoint Security 11.9.0 maakt het Kaspersky Endpoint Agent-distributiepakket niet langer deel uit van de Kaspersky Endpoint Security-distributiekit.

Overeenkomst van KEA-versies (als onderdeel van KES) met KES-versies

Kaspersky Endpoint Security voor Windows	Kaspersky Endpoint Agent
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

Kaspersky schakelt alle Detection and Response over op het werken met de ingebouwde agent van Kaspersky Endpoint Security in plaats van Kaspersky Endpoint Agent. Kaspersky voegt geleidelijk ondersteuning toe voor deze oplossingen en annuleert Kaspersky Endpoint Agent (zie onderstaande tabel). Vanaf versie 12.1 ondersteunt het programma alle Detection and Response-oplossingen. Bovendien is het programma vanaf versie 12.1 niet langer compatibel met Kaspersky Endpoint Agent en is het niet langer mogelijk om beide programma's naast elkaar op dezelfde computer te installeren.

Versie van Kaspersky Endpoint Security	Kaspersky Managed Detection and Response	Kaspersky Sandbox	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Endpoint Detection and Response Expert	Kaspersky Anti Attack Plat (onderdeel E Detection and R
11.5.0	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endp
11.6.0	**Ingebouwde agent**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endp
11.7.0	**Ingebouwde agent**	**Ingebouwde agent**	**Ingebouwde agent**	Kaspersky Endpoint Agent	Kaspersky Endp
11.8.0	**Ingebouwde agent**	**Ingebouwde agent**	**Ingebouwde agent**	**Ingebouwde agent**	Kaspersky Endp
11.9.0	**Ingebouwde agent**	**Ingebouwde agent**	**Ingebouwde agent**	**Ingebouwde agent**	Kaspersky Endp
11.10.0	**Ingebouwde agent**	**Ingebouwde agent**	**Ingebouwde agent**	**Ingebouwde agent**	Kaspersky Endp
11.11.0	**Ingebouwde agent**	**Ingebouwde agent**	**Ingebouwde agent**	**Ingebouwde agent**	Kaspersky Endp
12	**Ingebouwde agent**	**Ingebouwde agent**	**Ingebouwde agent**	**Ingebouwde agent**	Kaspersky Endp
12.1	**Ingebouwde agent**	**Ingebouwde agent**	**Ingebouwde agent**	**Ingebouwde agent**	**Ingebouwde**
12.6	**Ingebouwde agent**	**Ingebouwde agent**	**Ingebouwde agent**	**Ingebouwde agent**	**Ingebouwde**

De [KES+KEA]-configuratie migreren naar [KES+built-in agent]

Kaspersky Endpoint Security omvat een ingebouwde agent voor het werken met Detection and Response-oplossingen. U hebt geen apart Kaspersky Endpoint Agent-programma meer nodig om met deze oplossingen te werken. Wanneer u Kaspersky Endpoint Security implementeert op computers waarop Kaspersky Endpoint Agent is geïnstalleerd, blijven Detection and Response-oplossingen werken met Kaspersky Endpoint Security. Daarnaast wordt Kaspersky Endpoint Agent van de computer verwijderd.

De distributiekit voor Kaspersky Endpoint Security versies 11.2.0 – 11.8.0 bevat Kaspersky Endpoint Agent. U kunt Kaspersky Endpoint Agent selecteren bij het installeren van Kaspersky Endpoint Security voor Windows. Als gevolg hiervan worden twee programma's op uw computer geïnstalleerd: KEA en KES. In Kaspersky Endpoint Security 11.9.0 maakt het Kaspersky Endpoint Agent-distributiepakket niet langer deel uit van de Kaspersky Endpoint Security-distributiekit.

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 of later, inclusief de Newerkagent, 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 of later. Voor het beheren van EDR Optimum- en Kaspersky Sandbox-onderdelen moet u Webconsole gebruiken.

   Als u Kaspersky Anti Targeted Attack Platform (EDR) wilt gebruiken, hebt u een webplug-in nodig voor Kaspersky Endpoint Security versie 12.1 of hoger.

   Als u Kaspersky Anti Targeted Attack Platform (NDR) wilt gebruiken, hebt u een webplug-in nodig voor Kaspersky Endpoint Security versie 12.7 of hoger.

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 *Inactive*. Om het beleid toe te passen, opent u de beleidseigenschappen, accepteert u de Kaspersky Security Network-verklaring en stelt u de status in op *Active*.

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 Add-on-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 *Add key*.

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.

Alleen de Kaspersky Anti Targeted Attack Platform-licentie kan worden gebruikt om Kaspersky Endpoint Security te activeren als onderdeel van de Kaspersky Anti Targeted Attack Platform-oplossing. Nadat u het programma hebt geüpgraded naar versie 12.1, wordt de EDR (KATA)-functionaliteit automatisch geactiveerd. U hoeft verder niets te doen.

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 onderdelen voor Detection and Response-oplossingen in de instellingen van het installatiepakket.
- Sluit het Kaspersky Endpoint Agent-onderdeel uit in de instellingen van het installatiepakket (voor Kaspersky Endpoint Security voor Windows versies 11.2.0 – 11.8.0).
- Als Wachtwoordbeveiliging is ingeschakeld om de toegang tot Kaspersky Endpoint Agent te beperken, voert u het verwijderingswachtwoord in de instellingen van de *Install application remotely* taak in. Je kunt het verwijderingswachtwoord invoeren vanaf Kaspersky Security Center Linux 15.1.

U kunt het programma ook upgraden met behulp van de volgende methoden:

- Kaspersky-updateservice gebruiken (Seamless Update – SMU).
- Lokaal, met behulp van de Installatiewizard.

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 actuele 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 actuele licenties van Kaspersky-oplossingen. In dit geval selecteert Kaspersky Endpoint Security automatisch onderdelen op basis van de Kaspersky Endpoint Agent-configuratie: Hierna 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 *Critical* heeft in de Kaspersky Security Center-console:

   - Zorg ervoor dat op de computer Netwerkagent versie 13.2 of hoger is geïnstalleerd.
   - Controleer de werkingsstatus van het ingebouwde agent door het *Report on status of application components* te bekijken. Als een onderdeel de status *Not installed* heeft, installeer dan de onderdeel met de taak *Change application components*.
   - 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 *Report on status of application components* dat de EDR Optimum-functionaliteit is geactiveerd. Als een onderdeel de status *Geen onderdeel van licentie* heeft, zorg er dan voor dat de functie voor automatische distributie van licentiesleutels van EDR Optimum is ingeschakeld.

Migratie van beleid en taken voor Kaspersky Endpoint Agent

Kaspersky Endpoint Security for Windows een wizard voor het migreren 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 Anti Targeted Attack Platform

Een wizard voor het migreren van Kaspersky Endpoint Agent naar Kaspersky Endpoint Security werkt alleen in webconsole en cloudconsole. In de beheerconsole (MMC) kunt u instellingen voor Kaspersky Anti Targeted Attack Platform (EDR)-oplossing alleen migreren met de standaard Kaspersky Security Center-migratiewizard.

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 in het hoofdvenster van de webconsole achtereenvolgens **Operations → Migration from Kaspersky Endpoint Agent**.

Hiermee wordt de wizard beleiden- en takenmigratie uitgevoerd. 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 het 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. 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. Als gevolg hiervan doet de wizard het volgende:

- Maakt een nieuw Kaspersky Endpoint Security-beleid.

  Het beleid voegt instellingen van Kaspersky Endpoint Security en Kaspersky Endpoint Agent samen. Het beleid krijgt de naam *<Naam van Kaspersky Endpoint Security-beleid> & <Naam van Kaspersky Endpoint Agent-beleid>*. Het nieuwe beleid heeft de status *Inactive*. Wijzig nu de statussen van het Kaspersky Endpoint Agent-beleid en het Kaspersky Endpoint Security-beleid in *Inactive* 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.

Tijdens het migreren van Kaspersky Endpoint Agent naar Kaspersky Endpoint Security voor de Kaspersky Anti Targeted Attack Platform (EDR)-oplossing, kunnen er fouten optreden tijdens het verbinden van de computer met de Central Node servers. De reden is dat de migratiewizard in Web Console de volgende beleidsinstellingen overslaat en deze niet migreert:

- Verbod op wijzigen van de instellingen **Connection to KATA servers** ("hangslot").

  Standaard kunnen de instellingen gewijzigd worden (het “hangslot” is open). De instellingen zijn daarom niet toegepast op de computer. U zult de wijziging van de instellingen moeten verbieden en het "hangslot" sluiten.

- Crypto-container.

  Als u twee-weg verificatie gebruikt om contact te maken met de Central Node servers, moet u de crypto-container opnieuw toevoegen. De migratiewizard migreert correct het TLS-certificaat van de server.

De wizard Beleids- en Taakmigratie in Beheerconsole (MMC) migreert alle instellingen voor het Kaspersky Anti Targeted Attack Platform (EDR)-oplossing.

- Maakt nieuwe Kaspersky Endpoint Security-taken.

  Nieuwe taken zijn kopieën van Kaspersky Endpoint Agent-taken voor Kaspersky Endpoint Detection and Response en Kaspersky Sandbox oplossingen. De taken van Kaspersky Endpoint Agent worden door de wizard niet gewijzigd.

Beleids- en taakinstellingen migreren van Kaspersky Endpoint Agent naar Kaspersky Endpoint Security in de beheerconsole (MMC) (alleen voor KATA (EDR))

1. Selecteer Beheerserver in de Beheerconsole en klik met de rechtermuisknop om het contextmenu te openen.
2. Selecteer **All tasks** → **Policies and tasks batch conversion wizard**.

De wizard Batchconversie beleid en taken wordt gestart. Volg de instructies van de wizard.

Stap 1. Het programma selecteren waarvoor u beleid en taken moet converteren

Bij deze stap moet u Kaspersky Endpoint Security voor Windows selecteren. Ga naar de volgende stap.

Stap 2. Conversie van beleid

De migratiewizard maakt een nieuw Kaspersky Endpoint Security-beleid waarin de beleidsinstellingen van Kaspersky Endpoint Agent worden gemigreerd. In de beleidslijst selecteert u het Kaspersky Endpoint Agent-beleid waarvan u de instellingen wilt overdragen naar het Kaspersky Endpoint Security-beleid. Ga naar de volgende stap.

De migratiewizard begint dan met het converteren van het beleid. Tijdens de beleidsconversie vraagt de migratiewizard u de verklaring voor Kaspersky Security Network te accepteren. Nieuwe beleiden krijgen een naam *<Naam beleid> (geconverteerd)*.

Stap 3. Conversie van taken

Sla deze stap over. De Wizard ondersteunt taken alleen voor Kaspersky Endpoint Detection and Response Optimum en Kaspersky Sandbox. Beheer van deze onderdelen is alleen beschikbaar in de webconsole. Ga naar de volgende stap.

Stap 4. Voltooiing van wizard

Verlaat de wizard verlaten. Als gevolg van de wizard wordt een nieuw Kaspersky Endpoint Security-beleid gemaakt.

Endpoint Detection and Response Agent (EDR Agent)

Vanaf Kaspersky Endpoint Security 12.3 voor Windows bevat het programma de configuratie Endpoint Detection and Response Agent (EDR Agent). *Endpoint Detection and Response Agent* is een programma die op individuele werkstations en servers in de IT-infrastructuur van de organisatie wordt geïnstalleerd ter ondersteuning van de volgende Detection and Response-oplossingen van Kaspersky:

- Kaspersky Managed Detection and Response
- Kaspersky Anti Targeted Attack Platform (EDR)
- Kaspersky Unified Monitoring and Analysis Platform (KUMA) (vanaf versie 12.6)
- Kaspersky Anti Targeted Attack Platform (NDR) (vanaf versie 12.7)
- Kaspersky Endpoint Detection and Response Expert (on-premises) (vanaf versie 12.11)

EDR Agent ondersteunt integratie met de Kaspersky Endpoint Detection and Response Expert (cloud)-oplossingen niet.

EDR-agent controleert voortdurend de processen die op deze computers worden uitgevoerd, open netwerkverbindingen en bestanden die worden gewijzigd. Beveiligings- en besturingscomponenten van het programma zijn niet beschikbaar voor EDR Agent.

EDR-agent compatibel met EPP-applicaties van derden. Hierdoor kunt u hulpmiddelen voor infrastructuurbeveiliging van derden gebruiken naast Detection and Response van Kaspersky.

Om EDR-agent te implementeren, moet op de computer de Network Agent geïnstalleerd zijn en moet de computer toegevoegd zijn aan de Kaspersky Security Center-console. Om de interactie van EDR-agent met Kaspersky Security Center mogelijk te maken, moet u de beheerplug-in van Kaspersky Endpoint Security voor Windows installeren. U kunt EDR-agent instellingen opgeven met behulp van een groepsbeleid. Om EDR-agent te integreren, moet u de integratie configureren in de juiste beleidssecties.

De volgende Kaspersky-programma's moeten op de infrastructuur worden geïnstalleerd om Kaspersky Detection and Response-oplossingen te ondersteunen:

	• Netwerkagent • EDR Agent
Endpoint	
	Kaspersky Endpoint Security voor Windows beheerplug-in
Kaspersky Security Center	
	
Detectie and Response-oplossingen: MDR, KATA (EDR), KATA (NDR), KUMA, EDR Expert (on-premises)	

EDR-agent installeren

Kaspersky Endpoint Security in de Endpoint Detection and Response Agent (EDR Agent)-configuratie voor Kaspersky Detection and Response-oplossingen wordt op dezelfde manier geïnstalleerd.

EDR-agent kan op een van de volgende manieren op de computer worden geïnstalleerd:

- Op afstand via Kaspersky Security Center.
- Lokaal met behulp van de Installatiewizard.
- Lokaal op de opdrachtregel (alleen voor KATA (EDR) en EDR Expert (on-premises)).

Om EDR-agent te installeren, moet u de juiste configuratie selecteren in de Instellingen van het installatiepakket of in de Installatiewizard.

Hoe EDR-agent installeren met behulp van de Installatiewizard

1. Kopieer de distributiekit map naar de computer van de gebruiker.
2. Voer setup_kes.exe uit.

   De Installatiewizard wordt gestart.

Configuratie van Kaspersky Endpoint Security



De configuratie van het programma kiezen

Selecteer de **Endpoint Detection and Response Agent** configuratie. In deze configuratie kunt u alleen de onderdelen installeren die ondersteuning bieden voor Detection and Response-oplossingen: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), evenals KUMA. Deze configuratie is nodig als een Endpoint Protection Platform (EPP) van derden wordt geïmplementeerd in uw organisatie naast een Kaspersky Detection and Response-oplossing. Hierdoor is Kaspersky Endpoint Security in de Endpoint Detection and Response Agent-configuratie compatibel met EPP-programma's van derden.

Kaspersky Endpoint Security-onderdelen

Selecteer de onderdelen die u wilt installeren. 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.

Geavanceerde instellingen



Geavanceerde instellingen van programma-installatie

Bescherm het installatieproces van het programma. 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 Remote Desktop), wordt u aanbevolen de bescherming van het installatieproces uit te schakelen.

Zorg voor compatibiliteit met Citrix PVS. U kunt de ondersteuning voor Citrix Provisioning Services inschakelen om Kaspersky Endpoint Security op een virtuele machine te installeren.

Voeg het pad naar het bestand avp.com toe aan de systeemvariabele %PATH%. U kunt het pad voor de installatie toevoegen aan de variabele %PATH% om de opdrachtregel-interface eenvoudig te gebruiken.

Installeer de EDR-agent via de opdrachtregel (alleen voor KATA (EDR) en EDR Expert (on-premises))

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 /pSTANDALONEMODE=1 [/s]
   ```

   of

   ```
   msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 STANDALONEMODE=1 [/qn]
   ```

   Als gevolg hiervan wordt de EDR-agent programma voor integratie met Kaspersky Anti Targeted Attack Platform (EDR) of Kaspersky Endpoint Detection and Response Expert (on-premises) op de computer geïnstalleerd. U kunt bevestigen dat het programma is geïnstalleerd en de programma-instellingen controleren door de opdracht `status`.

EDR-agent installeren met behulp van de Beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de consolestructuur de map **Advanced** → **Remote installation** → **Installation packages**.

   Er wordt een lijst geopend met installatiepakketten die zijn gedownload naar Kaspersky Security Center.
3. Open de eigenschappen van het installatiepakket.

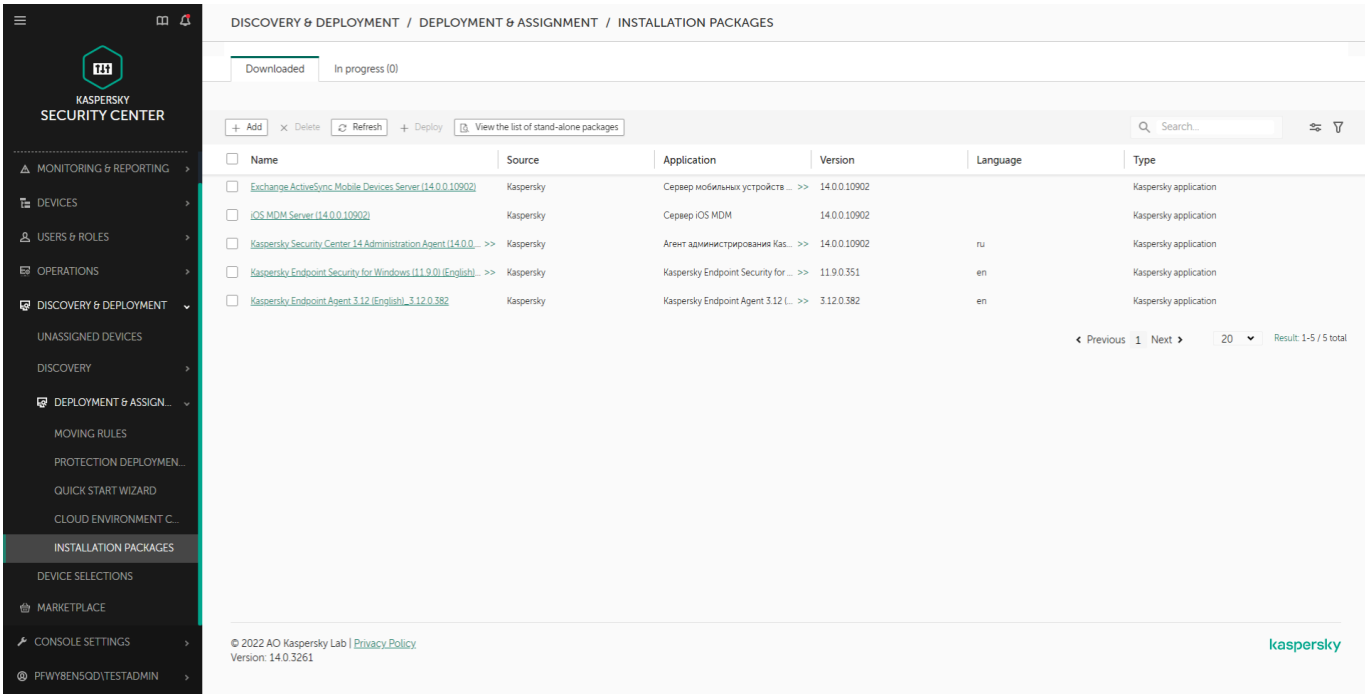
   Indien nodig, maak een nieuw installatiepakket.
4. Ga naar het gedeelte **Protection components**.
5. Selecteer de **Endpoint Detection and Response Agent ter bescherming tegen geavanceerde bedreigingen en gerichte aanvallen** configuratie. In deze configuratie kunt u alleen de onderdelen installeren die ondersteuning bieden voor Detection and Response-oplossingen: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), evenals KUMA. Deze configuratie is nodig als een Endpoint Protection Platform (EPP) van derden wordt geïmplementeerd in uw organisatie naast een Kaspersky Detection and Response-oplossing. Hierdoor is Kaspersky Endpoint Security in de Endpoint Detection and Response Agent-configuratie compatibel met EPP-programma's van derden.
6. Selecteer de onderdelen die u wilt installeren.

   U kunt de beschikbare programmaonderdelen wijzigen nadat het programma geïnstalleerd is.
7. Sla uw wijzigingen op.
8. Een taak voor een externe installatie maken. Selecteer in taakeigenschappen het installatiepakket dat u hebt gemaakt.

Hoe EDR-agent installeren met behulp van de Webconsole

1. Selecteer 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.



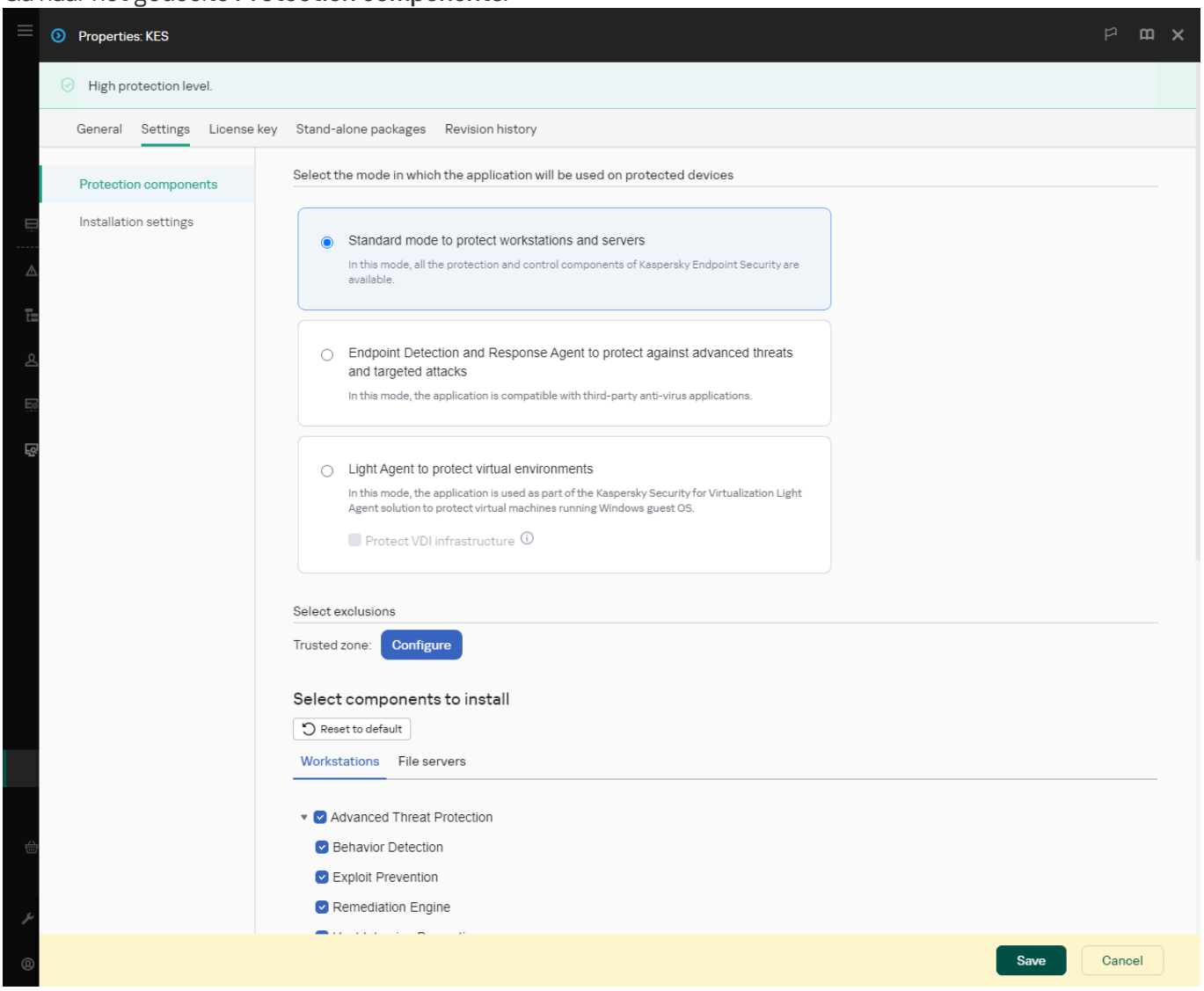
Lijst van installatiepakketten

2. Open de eigenschappen van het installatiepakket.

   Indien nodig, maak een nieuw installatiepakket.

3. Selecteer het tabblad **Settings**.

4. Ga naar het gedeelte **Protection components**.



Onderdelen opgenomen in het installatiepakket

5. Selecteer de **Endpoint Detection and Response Agent to protect against advanced threats and targeted attacks** configuratie. In deze configuratie kunt u alleen de onderdelen installeren die ondersteuning bieden voor Detection and Response-oplossingen: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), evenals KUMA. Deze configuratie is nodig als een Endpoint Protection Platform (EPP) van derden wordt geïmplementeerd in uw organisatie naast een Kaspersky Detection and Response-oplossing. Hierdoor is Kaspersky Endpoint Security in de Endpoint Detection and Response Agent-configuratie compatibel met EPP-programma's van derden.

6. Selecteer de onderdelen die u wilt installeren.

   U kunt de beschikbare programmaonderdelen wijzigen nadat het programma geïnstalleerd is.

7. Sla uw wijzigingen op.

8. Een taak voor een externe installatie maken. Selecteer in taakeigenschappen het installatiepakket dat u hebt gemaakt.

Als gevolg hiervan wordt het EDR-agent op de computer van de gebruiker geïnstalleerd. U kunt de interface van het programma gebruiken en er wordt een pictogram van het programma weergegeven in het systeemvak .

In Kaspersky Security Center heeft de computer met het geïnstalleerde programma in de EDR- Agent configuratie de status *Critical* status – . De computer heeft deze status omdat het onderdeel File Threat Protection ontbreekt. U hoeft niets te doen.

Als u EDR-agent niet kunt installeren op een computer met een EPP-programma van derden omdat het installatieprogramma incompatibele software op de computer heeft aangetroffen, kunt u de controle op incompatibele software overslaan.



Hoofdvenster van EDR-agent

Nu moet u de integratie met de Kaspersky Managed Detection and Response, Kaspersky Anti Targeted Attack (EDR), of Kaspersky Anti Targeted Attack (NDR)-oplossing configureren. Ook kunt u geavanceerde instellingen van het programma opgeven en bijvoorbeeld een vertrouwde zone aanmaken of de interface van de applicatie verbergen. Instellingen in de volgende secties zijn beschikbaar:

- Kaspersky Security Network
- Programma-instellingen
- Netwerkinstellingen
- Uitzonderingen
- Rapporten

- Interface
- Instellingen beheren

EDR-agent integreren met MDR

EDR-agent wordt geïnstalleerd op werkstations en servers in de IT-infrastructuur van de organisatie. EDR-agent verwerkt gegevens en verzendt deze via Kaspersky Security Network-stromen naar Kaspersky Managed Detection and Response.

U moet 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.

Een achtergrondverbinding tot stand brengen in Webconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Settings** → **Integration**.
2. Ga naar het gedeelte **Integration**.
3. Zet de schakelaar **Background connection for integration Enabled** aan.
4. Sla uw wijzigingen op.

Integratie met Kaspersky Managed Detection and Response bestaat uit de volgende stappen:

1. **Het onderdeel installeren Managed Detection and Response**

   U kunt het MDR-component selecteren tijdens: installatie of upgrade, alsook tijdens het gebruik van de taak *Programmaonderdelen wijzigen*.

   > Om het Managed Detection and Response-onderdeel te installeren zonder de computer opnieuw op te starten, met gebruik van de *Programmaonderdelen wijzigen*-taak, moet u de optie **Controleer op incompatibele programma's van derden** in de taakinstellingen uitschakelen.

2. **Kaspersky Private Security Network configureren**

   > Sla deze stap over als u Kaspersky Security Center Cloud Console gebruikt. Kaspersky Security Center Cloud Console configureert automatisch Kaspersky Private Security Network bij het installeren van de MDR plug-in.

   Kaspersky Private Security Network (KPSN) is een oplossing waarmee gebruikers van computers waarop Kaspersky Endpoint Security of andere Kaspersky-programma's worden gehost toegang krijgen tot reputatiedatabases van Kaspersky en tot andere statistische gegevens zonder gegevens naar Kaspersky te versturen vanaf hun eigen computers.

   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 Managed Detection and Response-console. Raadpleeg de help van Kaspersky Security Center voor meer informatie over de configuratie van Kaspersky Private Security Network. U kunt ook een Kaspersky Security Network-configuratiebestand uploaden naar de computer vanaf de opdrachtregel (zie onderstaande instructies).

Het Kaspersky Private 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 <file name>
   ```

   Waarbij `<file name>` is de naam van het configuratiebestand met de Kaspersky Private Security Network-instellingen (PKCS7- of PEM-bestandsindeling).

   Voorbeeld:
   `avp.com KSN /private C:\kpsn_config.pkcs7`

Als gevolg hiervan zal Kaspersky Private Security Network gebruiken om de reputatie van bestanden, programma's en websites te bepalen. **Kaspersky Security Network** gedeelte van de beleidsinstellingen geeft de volgende bedrijfsstatus weer: *Infrastructuur: Kaspersky Private Security Network*.

U moet de uitgebreide KSN-modus inschakelen zodat Managed Detection and Response kan werken.

3 **Kaspersky Managed Detection and Response activeren**

Beginnend met Kaspersky Endpoint Security for Windows 12.10, activeer de functionaliteit Managed Detection and Response als alternatief voor een activatiecode, u kunt ook een licentiebestand gebruiken.

U moet een afzonderlijke licentie kopen voor MDR (Kaspersky Managed Detection and Response Add-on).

De functie wordt functioneel beschikbaar na het toevoegen van een afzonderlijke sleutel voor Kaspersky Managed Detection and Response Add-on. Licenties voor de zelfstandige Managed Detection and Response-functionaliteit zijn hetzelfde als de licenties van Kaspersky Endpoint Security.

Zorg ervoor dat de MDR-functionaliteit is inbegrepen in de licentie en werkt in de lokale interface van het programma.

4 **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 Managed Detection and Response. Het BLOB-bestand bevindt zich in het ZIP-archief van het MDR-configuratiebestand. U kunt het Ziparchief verkrijgen in de Kaspersky Managed Detection and Response-console. Raadpleeg de Help van Kaspersky Managed Detection and Response voor gedetailleerde informatie over een BLOB-bestand.

Vanaf Kaspersky Endpoint Security 12.6 voor Windows is het toevoegen van een BLOB-bestand optioneel voor Kaspersky Managed Detection and Response zonder tenants als u een huidige licentie hebt.

Managed Detection and Response inschakelen in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)** in het beleidsvenster.
4. Selecteer het selectievakje **Managed Detection and Response (Industrial CyberSecurity)**.

5. Klik in het blok **Instellingen** op **Uploaden** en selecteer het BLOB-bestand ontvangen in de Kaspersky Managed Detection and Response-console. Het bestand heeft de extensie P7.

   Standaard mag de gebruiker de programma-instellingen beheren (het "hangslot" staat open). Om het beleid op computers toe te passen, sluit de hangsloten.

6. Sla uw wijzigingen op.

Managed Detection and Response activeren in de Webconsole en cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Built-in Agents Configuration** → **Managed Detection and Response**.
5. Zet de schakelaar **Managed Detection and Response ENABLED** aan.
6. Klik op **Upload** en selecteer het BLOB-bestand dat is verkregen in de Kaspersky Managed Detection and Response-console. Het bestand heeft de extensie P7.

   Standaard mag de gebruiker beleidsinstellingen beheren (het "hangslot" staat open). Om het beleid op computers toe te passen, sluit de hangsloten.

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 machtiging **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 downloaden en naar de computer sturen tijdens de volgende synchronisatie met Kaspersky Security Center. Controleer de werkingsstatus van het onderdeel door het *Report on status of application components* 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.

5. **Andere onderdelen van het programma configureren om telemetrie te ontvangen**

   U moet de volgende componenten inschakelen zodat Managed Detection and Response kan werken.

   - Kaspersky Security Network (uitgebreide modus).
   - Gedragsdetectie.
   - Exploit-preventie.
   - Web Threat Protection.
   - Mail Threat Protection.
   - File Threat Protection.
   - Network Threat Protection.
   - Firewall.
   - AMSI-bescherming.
   - Achtergrondscan.

     1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
     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 **Built-in Agents Configuration** → **Managed Detection and Response**.
     5. Zet de schakelaar **Managed Detection and Response ENABLED** aan.
     6. Sla uw wijzigingen op.

     1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
     2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
     3. Selecteer **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)** in het beleidsvenster.
     4. Selecteer het selectievakje **Managed Detection and Response (Industrial CyberSecurity)**.
     5. Sla uw wijzigingen op.

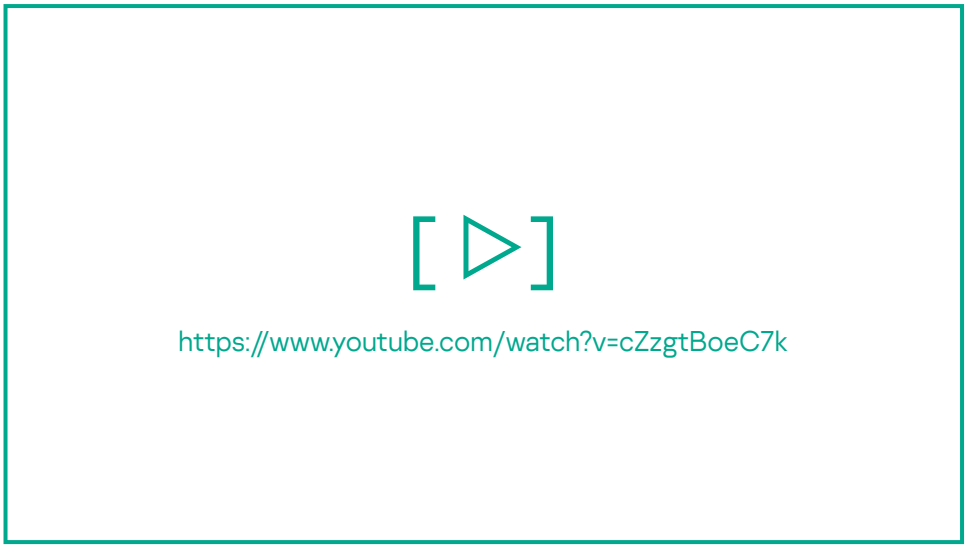
EDR-agent integreren met EDR (KATA)

EDR-agent wordt geïnstalleerd op werkstations en servers in de IT-infrastructuur van de organisatie. Op deze computers controleert EDR-agent voortdurend processen, open netwerkverbindingen en bestanden die worden gewijzigd, en stuurt monitoringgegevens naar de server met het onderdeel Central Node.

Om te integreren met EDR (KATA), moet u het onderdeel Endpoint Detection and Response (KATA) inschakelen en EDR-agent configureren.

Aan de volgende voorwaarden moet worden voldaan om Endpoint Detection and Response (KATA) te laten werken:

- Kaspersky Anti Targeted Attack Platform versies 5.0-7.1.
- Kaspersky Security Center versie 14.2 of hoger. In eerdere versies van Kaspersky Security Center is het onmogelijk om de Endpoint Detection and Response (KATA)-functie te activeren.



De integratie met Endpoint Detection and Response (KATA) omvat de volgende stappen:

1. **Endpoint Detection and Response (KATA) activeren**

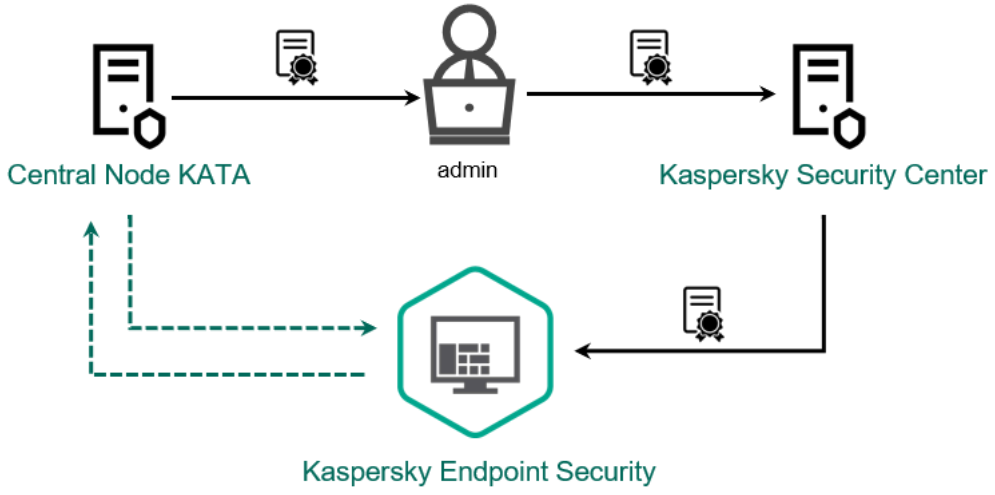
   U moet een afzonderlijke licentie kopen voor EDR (KATA) (Kaspersky Endpoint Detection and Response (KATA) add-on).

   De functie wordt beschikbaar na toevoeging van een afzonderlijke sleutel voor Kaspersky Endpoint Detection and Response (KATA). Licenties voor de zelfstandige Endpoint Detection and Response (KATA)-functionaliteit zijn hetzelfde als de licenties van Kaspersky Endpoint Security.

   Zorg ervoor dat de EDR (KATA)-functionaliteit is inbegrepen in de licentie en wordt uitgevoerd in de lokale interface van het programma.

2. **Verbinden met Central Node**

Kaspersky Anti Targeted Attack Platform heeft een vertrouwde verbinding nodig tussen Kaspersky Endpoint Security en het onderdeel Central Node. Gebruik een TLS-certificaat om een vertrouwde verbinding te configureren. U kunt een TLS-certificaat verkrijgen in de Kaspersky Anti Targeted Attack Platform-console (zie de instructies in de Help van Kaspersky Anti Targeted Attack Platform). Vervolgens moet u het TLS-certificaat toevoegen aan Kaspersky Endpoint Security (zie onderstaande instructies).



Een TLS-certificaat toevoegen aan Kaspersky Endpoint Security

Standaard controleert Kaspersky Endpoint Security alleen het TLS-certificaat van Central Node. Om de verbinding veiliger te maken, kunt u bovendien de verificatie van de computer op Central Node (twee-weg verificatie) inschakelen. Als u deze verificatie wilt inschakelen, moet u twee-weg verificatie inschakelen in de instellingen Central Node en Kaspersky Endpoint Security. Om twee-weg verificatie te gebruiken hebt u ook een crypto-container nodig. Een *crypto-container* is een PFX-archief met een certificaat en een privésleutel. U kunt een crypto-container verkrijgen in de Kaspersky Anti Targeted Attack Platform-console (zie de instructies in de Help van Kaspersky Anti Targeted Attack Platform).

Een Kaspersky Endpoint Security-computer verbinden met Central Node via de Beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de beheerconsole **Policies**.
3. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
4. Selecteer **Detection and Response** → **Endpoint Detection and Response Expert (on-premises)** in het beleidsvenster.
5. Selecteer het selectievakje **Endpoint Detection and Response Expert (on-premises)**.
6. Klik op **Serververbindingsinstellingen**.
7. Configureer de serververbinding:
   - **Time-out (sec.)**. Maximale time-out voor de serverrespons van Central Node. Wanneer de time-out is verstreken, probeert Kaspersky Endpoint Security verbinding te maken met een andere Central Node-server.
   - **Server TLS certificaat**. TLS-certificaat voor het tot stand brengen van een vertrouwde verbinding met de Central Node-server. U kunt een TLS-certificaat verkrijgen in de Kaspersky Anti Targeted Attack Platform-console (zie de instructies in de Help van Kaspersky Anti Targeted Attack Platform).

- **Gebruik twee-weg verificatie**. Tweerichtingsverificatie bij het tot stand brengen van een beveiligde verbinding tussen Kaspersky Endpoint Security en de Central Node-server. Om tweerichtingsverificatie te gebruiken, moet u tweerichtingsverificatie inschakelen in de Central Node-server instellingen, vervolgens een crypto-container ophalen en een wachtwoord instellen om de crypto-container te beschermen. Een *crypto-container* is een PFX-archief met een certificaat en een privésleutel. U kunt een crypto-container verkrijgen in de Kaspersky Anti Targeted Attack Platform-console (zie de instructies in de Help van Kaspersky Anti Targeted Attack Platform). Na het configureren van de Central Node-instellingen, moet u ook tweerichtingsverificatie inschakelen in de instellingen van Kaspersky Endpoint Security en een met een wachtwoord beveiligde crypto-container laden.

  De crypto-container moet met een wachtwoord worden beveiligd. Het is niet mogelijk om een crypto-container toe te voegen met een leeg wachtwoord.

8. Klik op **OK**.
9. Voeg central node-servers toe. Hiertoe geeft u het serveradres (IPv4, IPv6) en de poort op om verbinding te maken met de server.

   U kunt meerdere Central Node-serveradressen toevoegen. Kaspersky Endpoint Security probeert verbinding te maken met de server op het eerste IP-adres. Als er geen verbinding tot stand kan worden gebracht, probeert Kaspersky Endpoint Security verbinding te maken via het tweede IP-adres in de lijst, enzovoort.
10. Indien nodig, telemetrie configureren.
11. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Een Kaspersky Endpoint Security-computer verbinden met Central Node via de webconsole

1. Selecteer in het hoofdvenster van de Webconsole het tabblad **Asset management** → **Policies**.
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 **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (on-premises)**.
5. Zet de schakelaar **Endpoint Detection and Response Expert (on-premises) ENABLED** aan.
6. Als u EDR (KATA) wilt configureren, selecteert u **Endpoint Detection and Response Expert (version 7.1 or earlier)** in de lijst met oplossingen.
7. Klik op **Connection settings**.
8. Configureer de serververbinding:

   - **Timeout (sec)**. Maximale time-out voor de serverrespons van Central Node. Wanneer de time-out is verstreken, probeert Kaspersky Endpoint Security verbinding te maken met een andere Central Node-server.
   - **Server certificate**. TLS-certificaat voor het tot stand brengen van een vertrouwde verbinding met de Central Node-server. U kunt een TLS-certificaat verkrijgen in de Kaspersky Anti Targeted Attack Platform-console (zie de instructies in de Help van Kaspersky Anti Targeted Attack Platform).

- **Use two-way authentication**. Tweerichtingsverificatie bij het tot stand brengen van een beveiligde verbinding tussen Kaspersky Endpoint Security en de Central Node-server. Om tweerichtingsverificatie te gebruiken, moet u tweerichtingsverificatie inschakelen in de Central Node-server instellingen, vervolgens een crypto-container ophalen en een wachtwoord instellen om de crypto-container te beschermen. Een *crypto-container* is een PFX-archief met een certificaat en een privésleutel. U kunt een crypto-container verkrijgen in de Kaspersky Anti Targeted Attack Platform-console (zie de instructies in de Help van Kaspersky Anti Targeted Attack Platform). Na het configureren van de Central Node-instellingen, moet u ook tweerichtingsverificatie inschakelen in de instellingen van Kaspersky Endpoint Security en een met een wachtwoord beveiligde crypto-container laden.

  De crypto-container moet met een wachtwoord worden beveiligd. Het is niet mogelijk om een crypto-container toe te voegen met een leeg wachtwoord.

9. Klik op **OK**.
10. Voeg central node-servers toe. Hiertoe geeft u het serveradres (IPv4, IPv6) en de poort op om verbinding te maken met de server.

    U kunt meerdere Central Node-serveradressen toevoegen. Kaspersky Endpoint Security probeert verbinding te maken met de server op het eerste IP-adres. Als er geen verbinding tot stand kan worden gebracht, probeert Kaspersky Endpoint Security verbinding te maken via het tweede IP-adres in de lijst, enzovoort.
11. Indien nodig, telemetrie configureren.
12. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Als resultaat wordt de computer toegevoegd aan de Kaspersky Anti Targeted Attack Platform-console. Controleer de werkingsstatus van het onderdeel door het *Report on status of application components* 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 Expert (on-premises)** wordt toegevoegd aan de lijst met Kaspersky Endpoint Security-onderdelen.

EDR-agent integreren met NDR (KATA)

EDR-agent wordt geïnstalleerd op werkstations en servers in de IT-infrastructuur van de organisatie. Op deze computers controleert EDR-agent voortdurend processen, open netwerkverbindingen en bestanden die worden gewijzigd, en stuurt monitoringgegevens naar de server met het onderdeel Central Node.

Om te integreren met NDR (KATA), moet u het onderdeel Network Detection and Response (KATA) inschakelen en EDR-agent configureren.

Aan de volgende voorwaarden moet worden voldaan om Network Detection and Response (KATA) te laten werken:

- Kaspersky Anti Targeted Attack Platform versie 7.0 of hoger.
- Kaspersky Security Center versie 14.2 of hoger. In eerdere versies van Kaspersky Security Center is het onmogelijk om de Network Detection and Response (KATA)-functie te activeren.

https://www.youtube.com/watch?v=gd-rySv0ThQ

De integratie met Network Detection and Response (KATA) omvat de volgende stappen:

1. **Network Detection and Response (KATA) activeren**

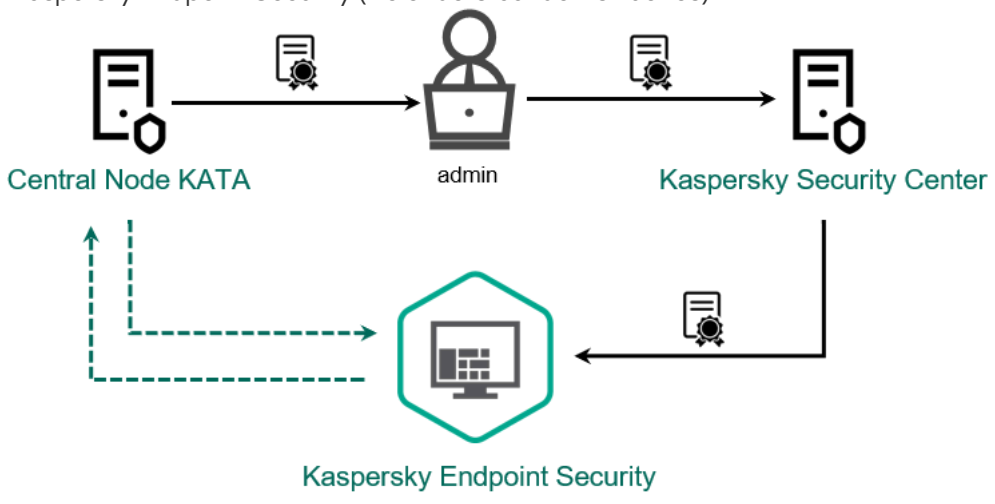
   U moet een afzonderlijke licentie kopen voor NDR (KATA) (Kaspersky Network Detection and Response (KATA) add-on).

   De functie wordt beschikbaar na toevoeging van een afzonderlijke sleutel voor Kaspersky Network Detection and Response (KATA). Licenties voor de zelfstandige Network Detection and Response (KATA)-functionaliteit zijn hetzelfde als de licenties van Kaspersky Endpoint Security.

   Zorg ervoor dat de NDR (KATA)-functionaliteit is inbegrepen in de licentie en wordt uitgevoerd in de lokale interface van het programma.

2. **Verbinden met Central Node**

   Kaspersky Anti Targeted Attack Platform heeft een vertrouwde verbinding nodig tussen Kaspersky Endpoint Security en het onderdeel Central Node. Gebruik een TLS-certificaat om een vertrouwde verbinding te configureren. U kunt een TLS-certificaat verkrijgen in de Kaspersky Anti Targeted Attack Platform-console (zie de instructies in de Help van Kaspersky Anti Targeted Attack Platform). Vervolgens moet u het TLS-certificaat toevoegen aan Kaspersky Endpoint Security (zie onderstaande instructies).



Een TLS-certificaat toevoegen aan Kaspersky Endpoint Security

Standaard controleert Kaspersky Endpoint Security alleen het TLS-certificaat van Central Node. Om de verbinding veiliger te maken, kunt u bovendien de verificatie van de computer op Central Node (twee-weg verificatie) inschakelen. Als u deze verificatie wilt inschakelen, moet u twee-weg verificatie inschakelen in de instellingen Central Node en Kaspersky Endpoint Security. Om twee-weg verificatie te gebruiken hebt u ook een crypto-container nodig. Een *crypto-container* is een PFX-archief met een certificaat en een privésleutel. U kunt een crypto-container verkrijgen in de Kaspersky Anti Targeted Attack Platform-console (zie de instructies in de Help van Kaspersky Anti Targeted Attack Platform).

Een Kaspersky Endpoint Security-computer verbinden met Central Node via de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Detection and Response** → **Network Detection and Response (KATA)** in het beleidsvenster.
4. Selecteer het selectievakje **Network Detection and Response (KATA)**.
5. Klik op **Connection settings**.
6. Configureer de serververbinding:
   - **Timeout (sec)**. Maximale time-out voor de serverrespons van Central Node. Wanneer de time-out is verstreken, probeert Kaspersky Endpoint Security verbinding te maken met een andere Central Node-server.
   - **Server certificate**. TLS-certificaat voor het tot stand brengen van een vertrouwde verbinding met de Central Node-server. U kunt een TLS-certificaat verkrijgen in de Kaspersky Anti Targeted Attack Platform-console (zie de instructies in de Help van Kaspersky Anti Targeted Attack Platform).
   - **Use two-way authentication**. Tweerichtingsverificatie bij het tot stand brengen van een beveiligde verbinding tussen Kaspersky Endpoint Security en de Central Node-server. Om tweerichtingsverificatie te gebruiken, moet u tweerichtingsverificatie inschakelen in de Central Node-server instellingen, vervolgens een crypto-container ophalen en een wachtwoord instellen om de crypto-container te beschermen. Een *crypto-container* is een PFX-archief met een certificaat en een privésleutel. U kunt een crypto-container verkrijgen in de Kaspersky Anti Targeted Attack Platform-console (zie de instructies in de Help van Kaspersky Anti Targeted Attack Platform). Na het configureren van de Central Node-instellingen, moet u ook tweerichtingsverificatie inschakelen in de instellingen van Kaspersky Endpoint Security en een met een wachtwoord beveiligde crypto-container laden.

     De crypto-container moet met een wachtwoord worden beveiligd. Het is niet mogelijk om een crypto-container toe te voegen met een leeg wachtwoord.

7. Klik op **OK**.
8. Voeg central node-servers toe. Hiertoe geeft u het serveradres (IPv4, IPv6) en de poort op om verbinding te maken met de server.
9. U kunt meerdere Central Node-serveradressen toevoegen. Kaspersky Endpoint Security probeert verbinding te maken met de server op het eerste IP-adres. Als er geen verbinding tot stand kan worden gebracht, probeert Kaspersky Endpoint Security verbinding te maken via het tweede IP-adres in de lijst, enzovoort.

10. Indien nodig, telemetrie configureren.

11. Sla uw wijzigingen op.

Een Kaspersky Endpoint Security-computer verbinden met Central Node via de webconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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 **Built-in Agents Configuration** → **Network Detection and Response (KATA)**.

5. Zet de schakelaar **Network Detection and Response (KATA) ENABLED** aan.

6. Klik op **Connection settings**.

7. Configureer de serververbinding:

   - **Timeout (sec)**. Maximale time-out voor de serverrespons van Central Node. Wanneer de time-out is verstreken, probeert Kaspersky Endpoint Security verbinding te maken met een andere Central Node-server.

   - **Server certificate**. TLS-certificaat voor het tot stand brengen van een vertrouwde verbinding met de Central Node-server. U kunt een TLS-certificaat verkrijgen in de Kaspersky Anti Targeted Attack Platform-console (zie de instructies in de Help van Kaspersky Anti Targeted Attack Platform).

   - **Use two-way authentication**. Tweerichtingsverificatie bij het tot stand brengen van een beveiligde verbinding tussen Kaspersky Endpoint Security en de Central Node-server. Om tweerichtingsverificatie te gebruiken, moet u tweerichtingsverificatie inschakelen in de Central Node-server instellingen, vervolgens een crypto-container ophalen en een wachtwoord instellen om de crypto-container te beschermen. Een *crypto-container* is een PFX-archief met een certificaat en een privésleutel. U kunt een crypto-container verkrijgen in de Kaspersky Anti Targeted Attack Platform-console (zie de instructies in de Help van Kaspersky Anti Targeted Attack Platform). Na het configureren van de Central Node-instellingen, moet u ook tweerichtingsverificatie inschakelen in de instellingen van Kaspersky Endpoint Security en een met een wachtwoord beveiligde crypto-container laden.

     De crypto-container moet met een wachtwoord worden beveiligd. Het is niet mogelijk om een crypto-container toe te voegen met een leeg wachtwoord.

8. Klik op **OK**.

9. Voeg central node-servers toe. Hiertoe geeft u het serveradres (IPv4, IPv6) en de poort op om verbinding te maken met de server.

10. U kunt meerdere Central Node-serveradressen toevoegen. Kaspersky Endpoint Security probeert verbinding te maken met de server op het eerste IP-adres. Als er geen verbinding tot stand kan worden gebracht, probeert Kaspersky Endpoint Security verbinding te maken via het tweede IP-adres in de lijst, enzovoort.

11. Indien nodig, telemetrie configureren.

12. Sla uw wijzigingen op.

Als resultaat wordt de computer toegevoegd aan de Kaspersky Anti Targeted Attack Platform-console. Controleer de werkingsstatus van het onderdeel door het *Report on status of application components* te bekijken. U kunt de werkingsstatus van een onderdeel ook in rapporten bekijken in de lokale interface van Kaspersky Endpoint Security. Het onderdeel **Network Detection and Response (KATA)** wordt toegevoegd aan de lijst met Kaspersky Endpoint Security-onderdelen.

EDR-agent integreren met EDR Expert (on-premises)

EDR-agent wordt geïnstalleerd op werkstations en servers in de IT-infrastructuur van de organisatie. Op deze computers controleert EDR-agent voortdurend processen, open netwerkverbindingen en bestanden die worden gewijzigd, en stuurt monitoringgegevens naar de EDR Expert (on-premises) server.

Om te integreren met EDR Expert (on-premises), moet u het onderdeel Endpoint Detection and Response Expert (on-premises) inschakelen en EDR-agent configureren.

De integratie met Endpoint Detection and Response Expert (on-premises) omvat de volgende stappen:

1. **Kaspersky Endpoint Detection and Response Expert (on-premises) activeren**

   U moet een afzonderlijke licentie kopen voor EDR Expert (on-premises) (Kaspersky Endpoint Detection and Response Expert (on-premises) add-on).

   De functie wordt beschikbaar na toevoeging van een afzonderlijke sleutel voor Kaspersky Endpoint Detection and Response Expert (on-premises). Licenties voor de zelfstandige Endpoint Detection and Response Expert (on-premises) functionaliteit is hetzelfde als de licentie van Kaspersky Endpoint Security.

   Zorg ervoor dat de EDR Export (on-premises)-functionaliteit is inbegrepen in de licentie en wordt uitgevoerd in de lokale interface van het programma.

2. **Verbinding maken met de server voor het verzamelen van telemetriegegevens en de responsserver**

   Kaspersky Endpoint Detection and Response Expert (on-premises) vereist een vertrouwde verbinding tussen Kaspersky Endpoint Security en twee servers:

   - Een *telemetrieverzamelingsserver* is een server die deel uitmaakt van een SIEM oplossing die informatie over gebeurtenissen op de computer verzamelt, normaliseert, correleert, analyseert en opslaat.
   - Een *responsservers* is een server voor het ontvangen en scannen van gegevens, het bestuderen van het gedrag van objecten en het publiceren van de resultaten van dergelijke onderzoeken.

   Gebruik een TLS-certificaat om een vertrouwde verbinding te configureren. U kunt een TLS-certificaat verkrijgen via het Open Single Management Platform (zie de instructies in de Help van Kaspersky Endpoint Detection and Response Expert (on-premises)). Vervolgens moet u het TLS-certificaat toevoegen aan Kaspersky Endpoint Security (zie onderstaande instructies).

   Standaard controleert Kaspersky Endpoint Security alleen het TLS-certificaat van de servers. Om de verbinding veiliger te maken, kunt u bovendien de verificatie van de computer op de server (twee-weg verificatie) inschakelen. Om deze verificatie in te schakelen, moet u twee-weg inschakelen in de server- en Kaspersky Endpoint Security-instellingen. Om twee-weg verificatie te gebruiken hebt u ook een crypto-container nodig. Een *crypto-container* is een PFX-archief met een certificaat en een privésleutel. U kunt een cryptocontainer verkrijgen op het Open Single Management Platform (zie de instructies in de Help van Kaspersky Endpoint Detection and Response Expert (on-premises)).

Een Kaspersky Endpoint Security-computer verbinden met EDR Expert (on-premises) via de webconsole

1. Selecteer in het hoofdvenster van de Webconsole het tabblad **Asset management** → **Policies**.
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 **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (on-premises)**.
5. Zet de schakelaar **Endpoint Detection and Response Expert (on-premises) ENABLED** aan.
6. Als u EDR Expert (on-premises) wilt configureren, selecteert u **Endpoint Detection and Response Expert (version 8.0 or later)** in de lijst met oplossingen.
7. Configureer de *servers voor het verzamelen van telemetriegegevens* verbinding:

   a. Klik in het blok **Connection to telemetry collection servers** op de koppeling **Connection settings**.

   b. Configureer de verbinding met de servers voor het verzamelen van telemetriegegevens:

   - **Timeout (sec)**. Maximale time-out voor de serverrespons. Wanneer de time-out is verstreken, probeert Kaspersky Endpoint Security verbinding te maken met een andere server.
   - **Server certificate**. TLS-certificaat voor het tot stand brengen van een vertrouwde verbinding met de server. U kunt een TLS-certificaat verkrijgen via het Open Single Management Platform (zie de instructies in de Help van Kaspersky Endpoint Detection and Response Expert (on-premises)).
   - **Use two-way authentication**. Tweerichtingsverificatie bij het tot stand brengen van een beveiligde verbinding tussen Kaspersky Endpoint Security en de server. Om tweerichtingsverificatie te gebruiken, moet u tweerichtingsverificatie inschakelen in de server instellingen, vervolgens een crypto-container ophalen en een wachtwoord instellen om de crypto-container te beschermen. Een *crypto-container* is een PFX-archief met een certificaat en een privésleutel. U kunt een cryptocontainer verkrijgen op het Open Single Management Platform (zie de instructies in de Help van Kaspersky Endpoint Detection and Response Expert (on-premises)). Na het configureren van de server instellingen, moet u ook tweerichtingsverificatie inschakelen in de instellingen van Kaspersky Endpoint Security en een met een wachtwoord beveiligde crypto-container laden.

     De crypto-container moet met een wachtwoord worden beveiligd. Het is niet mogelijk om een crypto-container toe te voegen met een leeg wachtwoord.

   c. Klik op **OK**.

   d. Voeg servers voor het verzamelen van telemetrie toe. Hiertoe geeft u het serveradres (IPv4, IPv6) en de poort op om verbinding te maken met de server.

      U kunt meerdere adressen van telemetrie-verzamelingsservers toevoegen. Kaspersky Endpoint Security probeert verbinding te maken met de server op het eerste IP-adres. Als er geen verbinding tot stand kan worden gebracht, probeert Kaspersky Endpoint Security verbinding te maken via het tweede IP-adres in de lijst, enzovoort.

   e. Indien nodig, telemetrie configureren.

8. Configureer de *responsservers* verbinding:

   a. Configureer in het blok **Connection to response servers** de instellingen **Send sync request to server every (min)**. Frequentie van synchronisatieverzoeken die naar de server worden verzonden. Tijdens de synchronisatie ontvangt Kaspersky Endpoint Security responstaken op dreigingen en verstuurt het de resultaten van de taken.

   b. Klik op de koppeling **Connection settings**.

   c. Configureer de responsservers verbinding:

      - **Timeout (sec)**. Maximale time-out voor de serverrespons. Wanneer de time-out is verstreken, probeert Kaspersky Endpoint Security verbinding te maken met een andere server.

      - **Server certificate**. TLS-certificaat voor het tot stand brengen van een vertrouwde verbinding met de server. U kunt een TLS-certificaat verkrijgen via het Open Single Management Platform (zie de instructies in de Help van Kaspersky Endpoint Detection and Response Expert (on-premises)).

      - **Use two-way authentication**. Tweerichtingsverificatie bij het tot stand brengen van een beveiligde verbinding tussen Kaspersky Endpoint Security en de server. Om tweerichtingsverificatie te gebruiken, moet u tweerichtingsverificatie inschakelen in de server instellingen, vervolgens een crypto-container ophalen en een wachtwoord instellen om de crypto-container te beschermen. Een *crypto-container* is een PFX-archief met een certificaat en een privésleutel. U kunt een cryptocontainer verkrijgen op het Open Single Management Platform (zie de instructies in de Help van Kaspersky Endpoint Detection and Response Expert (on-premises)). Na het configureren van de server instellingen, moet u ook tweerichtingsverificatie inschakelen in de instellingen van Kaspersky Endpoint Security en een met een wachtwoord beveiligde crypto-container laden.

        De crypto-container moet met een wachtwoord worden beveiligd. Het is niet mogelijk om een crypto-container toe te voegen met een leeg wachtwoord.

   d. Klik op **OK**.

   e. Voeg responsservers toe. Hiertoe geeft u het serveradres (IPv4, IPv6) en de poort op om verbinding te maken met de server.

      U kunt meerdere adressen van responsservers toevoegen. Kaspersky Endpoint Security probeert verbinding te maken met de server op het eerste IP-adres. Als er geen verbinding tot stand kan worden gebracht, probeert Kaspersky Endpoint Security verbinding te maken via het tweede IP-adres in de lijst, enzovoort.

9. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Als gevolg hiervan wordt de computer toegevoegd aan het Open Single Management Platform (OSMP). Controleer de werkingsstatus van het onderdeel door het *Report on status of application components* 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 Expert (on-premises)** wordt toegevoegd aan de lijst met Kaspersky Endpoint Security-onderdelen.

Compatibiliteit met toepassingen van derden EPP

EDR-agent ondersteunt de functionaliteit van Kaspersky Detection and Response-oplossingen. Beveiligings- en besturingscomponenten zijn niet beschikbaar voor EDR Agent. Met deze configuratie is het mogelijk EPP-programma's van derden te installeren en Kaspersky Detection and Response-oplossingen in de infrastructuur van de organisatie te implementeren. EDR Agent ondersteunt het werken met Kaspersky Managed Detection and Response, Kaspersky Anti Targeted Attack Platform (EDR), en Kaspersky Anti Targeted Attack Platform (NDR).

EDR-agent is compatibel met EPP-programma's van de volgende leveranciers:

- **Dr.Web**

  EDR-agent is compatibel met Dr.Web Agent voor Windows 13.0.1 of hoger en Dr.Web Server (x64) 13.0.0.10200.

- **Dallas Lock**

  EDR-agent is compatibel met Dallas Lock 8.0-C versie11.4.2.843 of hoger.

  > Om de EDR-agent te kunnen uitvoeren op een computer waarop de Dallas Lock-software is geïnstalleerd, moet u de verbinding met externe services van Kaspersky toestaan in de instellingen van de Firewall-module.

- **Secret Net Studio**

  EDR Agent is compatibel met Secret Net Studio versie 8.11 of later.

  > 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.

- **Trend Micro**

  EDR-agent is compatibel met Trend Micro Apex One versie 14.0.12994 of hoger (inclusief Security Agent).

  EDR-agent is compatibel met Trend Micro Deep Security versie 20.0.2-4960 of hoger (inclusief Security Agent).

- **Windows Defender**

- **Sophos**

  EDR Agent is compatibel met Sophos Intercept X versie 2024.1.2 of hoger (inclusief Endpoint Agent) en Sophos Core Agent versie 2024.3.2.3.

- **Bitdefender**

  EDR-agent is compatibel met Bitdefender Endpoint Security Tools versie 7.9.21.523 of hoger.

- **ESET**

  EDR Agent is compatibel met ESET Endpoint Security versie 12.0.2049.0 of hoger en ESET Management Agent versie 12.0 of hoger.

Op computers met Windows 11 voor Arm64 is EDR Agent niet compatibel met: Bitdefender Endpoint Security Tools.

De programma's moeten in de volgende volgorde worden geïnstalleerd: installeer eerst het EPP-programma, vervolgens Kaspersky Security Center Network Agent en vervolgens EDR Agent. Dit is nodig omdat het installatieprogramma van de EPP-programma EDR-agent en Networkagent mogelijk als incompatibele software detecteert en deze verwijdert. De werking van EDR-agent en Networkagent moet ook worden gecontroleerd na het updaten van de EPP-programma van derden, omdat het installatieprogramma de computer mogelijk opnieuw scant op incompatibele software en de programma's verwijdert.

Als u EDR-agent niet kunt installeren op een computer met een EPP-programma van derden omdat het installatieprogramma incompatibele software op de computer heeft aangetroffen, kunt u de controle op incompatibele software overslaan.

Managed Detection and Response



Kaspersky Endpoint Security voor Windows ondersteunt integratie met 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.

Configuraties van Kaspersky Endpoint Security voor integratie met MDR

De volgende configuraties kunnen worden gebruikt om met MDR te werken:

- **[KES+built-in agent]**. In deze configuratie fungeert Kaspersky Endpoint Security zowel als het programma dat de veiligheid van de computer garandeert, als het programma voor het werken met MDR. De ingebouwde agent is beschikbaar in Kaspersky Endpoint Security 11.6.0 voor Windows of hoger.

- **[EPP+EDR Agent van derden]**. In deze configuratie wordt de beveiliging van de IT-infrastructuur verzorgd door het Endpoint Protection Platform (EPP) van derden. De interactie met MDR wordt verzorgd door Kaspersky Endpoint Security in de configuratie Endpoint Detection and Response Agent (EDR Agent). In deze configuratie is EDR-agent compatibel met EPP-applicaties van derden. EDR-agent is beschikbaar in Kaspersky Endpoint Security 12.3 voor Windows of hoger.

Ondersteuning voor eerdere versies van Kaspersky Endpoint Security

Kaspersky Endpoint Security versie 11 en hoger ondersteunt de MDR-oplossing. Kaspersky Endpoint Security versies 11 – 11.5.0 verzendt alleen telemetriegegevens naar Kaspersky Managed Detection and Response 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.

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 Managed Detection and Response.

Integratie van de ingebouwde agent 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 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.

Een achtergrondverbinding tot stand brengen in Webconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Settings** → **Integration**.
2. Ga naar het gedeelte **Integration**.
3. Zet de schakelaar **Background connection for integration Enabled** aan.
4. Sla uw wijzigingen op.

Integratie met Kaspersky Managed Detection and Response bestaat uit de volgende stappen:

1. **Het onderdeel installeren Managed Detection and Response**

   U kunt het MDR-component selecteren tijdens: installatie of upgrade, alsook tijdens het gebruik van de taak *Programmaonderdelen wijzigen*.

   Om het Managed Detection and Response-onderdeel te installeren zonder de computer opnieuw op te starten, met gebruik van de *Programmaonderdelen wijzigen*-taak, moet u de optie **Controleer op incompatibele programma's van derden** in de taakinstellingen uitschakelen.

2 Kaspersky Private Security Network configureren

Sla deze stap over als u Kaspersky Security Center Cloud Console gebruikt. Kaspersky Security Center Cloud Console configureert automatisch Kaspersky Private Security Network bij het installeren van de MDR plug-in.

Kaspersky Private Security Network (KPSN) is een oplossing waarmee gebruikers van computers waarop Kaspersky Endpoint Security of andere Kaspersky-programma's worden gehost toegang krijgen tot reputatiedatabases van Kaspersky en tot andere statistische gegevens zonder gegevens naar Kaspersky te versturen vanaf hun eigen computers.

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 Managed Detection and Response-console. Raadpleeg de help van Kaspersky Security Center voor meer informatie over de configuratie van Kaspersky Private Security Network. U kunt ook een Kaspersky Security Network-configuratiebestand uploaden naar de computer vanaf de opdrachtregel (zie onderstaande instructies).

Het Kaspersky Private 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 <file name>
   ```

   Waarbij `<file name>` is de naam van het configuratiebestand met de Kaspersky Private Security Network-instellingen (PKCS7- of PEM-bestandsindeling).

   Voorbeeld:
   ```
   avp.com KSN /private C:\kpsn_config.pkcs7
   ```

Als gevolg hiervan zal Kaspersky Private Security Network gebruiken om de reputatie van bestanden, programma's en websites te bepalen. **Kaspersky Security Network** gedeelte van de beleidsinstellingen geeft de volgende bedrijfsstatus weer: *Infrastructuur: Kaspersky Private Security Network*.

U moet de uitgebreide KSN-modus inschakelen zodat Managed Detection and Response kan werken.

3 Kaspersky Managed Detection and Response activeren

Beginnend met Kaspersky Endpoint Security for Windows 12.10, activeer de functionaliteit Managed Detection and Response als alternatief voor een activatiecode, u kunt ook een licentiebestand gebruiken.

Kaspersky Managed Detection and Response ondersteunt de volgende licentiemethoden:

- Managed Detection and Response-functionaliteit is inbegrepen in de Kaspersky Endpoint Security for Windows-licentie.

  De functionaliteit is onmiddelijk beschikbaar na de activering van Kaspersky Endpoint Security voor Windows.

- Er wordt een aparte licentie voor MDR (Kaspersky Managed Detection and Response Add-on) gebruikt.

  De functie wordt functioneel beschikbaar na het toevoegen van een afzonderlijke sleutel voor Kaspersky Managed Detection and Response Add-on. Als resultaat worden er twee sleutels op de computer toegevoegd: een sleutel voor Kaspersky Endpoint Security en een sleutel voor Kaspersky Managed Detection and Response.

  Licenties voor de zelfstandige Managed Detection and Response-functionaliteit zijn hetzelfde als de licenties van Kaspersky Endpoint Security.

Zorg ervoor dat de MDR-functionaliteit is inbegrepen in de licentie en werkt in de lokale interface van het programma.

4. **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 Managed Detection and Response. Het BLOB-bestand bevindt zich in het ZIP-archief van het MDR-configuratiebestand. U kunt het Ziparchief verkrijgen in de Kaspersky Managed Detection and Response-console. Raadpleeg de Help van Kaspersky Managed Detection and Response voor gedetailleerde informatie over een BLOB-bestand.

Vanaf Kaspersky Endpoint Security 12.6 voor Windows is het toevoegen van een BLOB-bestand optioneel voor Kaspersky Managed Detection and Response zonder tenants als u een huidige licentie hebt.

Managed Detection and Response inschakelen in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)** in het beleidsvenster.
4. Selecteer het selectievakje **Managed Detection and Response (Industrial CyberSecurity)**.
5. Klik in het blok **Instellingen** op **Uploaden** en selecteer het BLOB-bestand ontvangen in de Kaspersky Managed Detection and Response-console. Het bestand heeft de extensie P7.

   Standaard mag de gebruiker de programma-instellingen beheren (het "hangslot" staat open). Om het beleid op computers toe te passen, sluit de hangsloten.

6. Sla uw wijzigingen op.

Managed Detection and Response activeren in de Webconsole en cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Built-in Agents Configuration** → **Managed Detection and Response**.
5. Zet de schakelaar **Managed Detection and Response ENABLED** aan.

6. Klik op **Upload** en selecteer het BLOB-bestand dat is verkregen in de Kaspersky Managed Detection and Response-console. Het bestand heeft de extensie P7.

   Standaard mag de gebruiker beleidsinstellingen beheren (het "hangslot" staat open). Om het beleid op computers toe te passen, sluit de hangsloten .

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 machtiging **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 downloaden en naar de computer sturen tijdens de volgende synchronisatie met Kaspersky Security Center. Controleer de werkingsstatus van het onderdeel door het *Report on status of application components* 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.

5. **Andere onderdelen van het programma configureren om telemetrie te ontvangen**

   U moet de volgende componenten inschakelen zodat Managed Detection and Response kan werken.

   - Kaspersky Security Network (uitgebreide modus).
   - Gedragsdetectie.
   - Exploit-preventie.
   - Web Threat Protection.
   - Mail Threat Protection.
   - File Threat Protection.
   - Network Threat Protection.
   - Firewall.
   - AMSI-bescherming.

- Achtergrondscan.

  1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
  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 **Built-in Agents Configuration** → **Managed Detection and Response**.
  5. Zet de schakelaar **Managed Detection and Response ENABLED** aan.
  6. Sla uw wijzigingen op.

  1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
  2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
  3. Selecteer **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)** in het beleidsvenster.
  4. Selecteer het selectievakje **Managed Detection and Response (Industrial CyberSecurity)**.
  5. Sla uw wijzigingen op.

Migratiegids van KEA naar KES voor MDR

Kaspersky Endpoint Security voor Windows bevat een ingebouwde agent voor de Kaspersky Managed Detection and Response-oplossing. U hebt geen apart Kaspersky Endpoint Agent-programma meer nodig om met MDR te werken. Alle functies van Kaspersky Endpoint Agent worden uitgevoerd door Kaspersky Endpoint Security.

Wanneer u Kaspersky Endpoint Security implementeert op computers waarop Kaspersky Endpoint Agent is geïnstalleerd, blijven Kaspersky Managed Detection and Response-oplossing werken met Kaspersky Endpoint Security. Daarnaast wordt Kaspersky Endpoint Agent van de computer verwijderd. Hetzelfde gedrag in het systeem zal optreden wanneer u Kaspersky Endpoint Security bijwerkt naar versie 11.6.0 of hoger.

> Kaspersky Endpoint Security is niet compatibel met Kaspersky Endpoint Agent. U kunt deze programma's niet beide op dezelfde computer installeren.

Kaspersky Endpoint Security moet aan de volgende voorwaarden voldoen om te werken als onderdeel van Kaspersky Managed Detection and Response:

- Kaspersky Security Center versie 13.2 of hoger (inclusief Network Agent). In eerdere versies van Kaspersky Security Center is het onmogelijk om de Managed Detection and Response-functie te activeren.
- Er is een achtergrondverbinding tot stand gebracht tussen Kaspersky Security Center Webconsole en Administration Server Om MDR te laten werken met Administration Server via Kaspersky Security Center Webconsole, moet u een nieuwe beveiligde verbinding tot stand brengen, een *achtergrondverbinding*.

Stappen voor het migreren van [KES +KEA] configuratie naar [KES +ingebouwde agent] voor MDR

1. **De beheerplug-in voor Kaspersky Endpoint Security upgraden**

   De MDR-component kan worden beheerd met de Kaspersky Endpoint Security Management Plug-in versie 11.6 of hoger. Afhankelijk van het type Kaspersky Security Center-console dat u gebruikt, werkt u de beheerplug-in in de Administration Console (MMC) of de webplug-in in de Web Console bij.

2. **Beleid en taken migreren**

   Zet Kaspersky Endpoint Agent-instellingen over naar Kaspersky Endpoint Security for Windows. De volgende opties zijn beschikbaar:

   - Een wizard voor het migreren van Kaspersky Endpoint Agent naar Kaspersky Endpoint Security. Een wizard voor het migreren van Kaspersky Endpoint Agent naar Kaspersky Endpoint Security werkt alleen in webconsole

     Zo migreert u beleids- en taakinstellingen van Kaspersky Endpoint Agent naar Kaspersky Endpoint Security in webconsole

Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Operations → Migration from Kaspersky Endpoint Agent**.

Hiermee wordt de wizard beleiden- en takenmigratie uitgevoerd. 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 het 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 ondersteunt geen MDR-taken. Sla deze stap over.

Stap 3. Voltooiing van wizard

Verlaat de wizard verlaten. Als gevolg van de wizard wordt een nieuw Kaspersky Endpoint Security-beleid gemaakt. Het beleid voegt instellingen van Kaspersky Endpoint Security en Kaspersky Endpoint Agent samen. Het beleid krijgt de naam *<Naam van Kaspersky Endpoint Security-beleid> & <Naam van Kaspersky Endpoint Agent-beleid>*. Het nieuwe beleid heeft de status *Inactive*. Wijzig nu de statussen van het Kaspersky Endpoint Agent-beleid en het Kaspersky Endpoint Security-beleid in *Inactive* en activeer het nieuwe samengevoegde beleid.

- Een standaard Batchconversiewizard voor beleid en taken De Batchconversiewizard van beleid en taken voor Kaspersky Security is alleen beschikbaar in de Beheerconsole (MMC). Voor meer informatie over beleiden en taken van de Batchconversiewizard raadpleegt u de Help van Kaspersky Security Center.

3. **Het licentiëren van de MDR-functionaliteit**

   Om Kaspersky Endpoint Security te activeren als onderdeel van de Kaspersky Managed Detection and Response-oplossing, hebt u een aparte licentie nodig voor de Add-on Kaspersky Managed Detection and Response. U kunt dan de sleutel toevoegen met de taak *Add key*. Als gevolg hiervan worden twee sleutels aan het programma toegevoegd: *Kaspersky Endpoint Security* en *Kaspersky Managed Detection and Response*.

4. **Het Kaspersky Endpoint Security-programma installeren/ upgraden**

   Om MDR-functionaliteit te migreren tijdens de installatie of upgrade van een applicatie, wordt aanbevolen om de installatietaak op afstand. Wanneer u een installatietaak op afstand maakt, moet u de MDR-component selecteren in de instellingen van het installatiepakket.

   U kunt het programma ook upgraden met behulp van de volgende methoden:

   - Met Kaspersky-updateservice.
   - Lokaal, met behulp van de Installatiewizard.

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 actuele licenties van Kaspersky-oplossingen. Als op de computer Kaspersky Endpoint Agent is geïnstalleerd en MDR-oplossing is geactiveerd, configureert het Kaspersky Endpoint Security-installatieprogramma automatisch de set onderdelen en selecteert het MDR-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 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 actuele licenties van Kaspersky-oplossingen. In dit geval selecteert Kaspersky Endpoint Security automatisch componenten op basis van een reeks componenten van Kaspersky Endpoint Agent. Hierna schakelt Kaspersky Endpoint Security over op het gebruik van de ingebouwde agent en wordt Kaspersky Endpoint Agent verwijderd.

Kaspersky Endpoint Security ondersteunt upgraden zonder de computer opnieuw op te starten. U kunt de toepassingsupgrademodus in beleidseigenschappen.

5. **De werking van het programma controleren**

   Als de computer na installatie of upgrade de status *Critical* heeft in de Kaspersky Security Center-console:

   - Zorg ervoor dat op de computer Netwerkagent versie 13.2 of hoger is geïnstalleerd.
   - Controleer de werkingsstatus van het ingebouwde agent door het *Report on status of application components* te bekijken. Als een onderdeel de status *Not installed* heeft, installeer dan de onderdeel met de taak *Change application components*. Als een onderdeel de *Geen onderdeel van licentie* toestand heeft, zorg er dan voor dat u de ingebouwde agent-functionaliteit heeft geactiveerd.
   - Zorg ervoor dat u akkoord gaat met de Kaspersky Security Network-verklaring in het nieuwe beleid van Kaspersky Endpoint Security voor Windows.

Endpoint Detection and Response

Kaspersky Endpoint Security for Windows heeft een ingebouwde agent voor de Kaspersky Endpoint Detection and Response Optimum-oplossing (hierna ook "EDR Optimum"). Vanaf versie 11.8.0 bevat Kaspersky Endpoint Security for Windows 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.

Tools voor dreigingsinformatie

Kaspersky Endpoint Detection and Response gebruikt de volgende Threat Intelligence-tools:

- De integratie met Kaspersky Threat Intelligence Portal dat informatie over de reputatie van bestanden en webadressen bevat en toont.
- Kaspersky Threats-database.
- 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.
- Cloud Sandbox-technologie waarmee u gedetecteerde bestanden in een geïsoleerde omgeving kunt uitvoeren en hun reputatie kunt controleren.

Werkingsprincipe van de oplossing

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. Een *Waarschuwing* is een gebeurtenis in de IT-infrastructuur van het bedrijf die door het programma is geïdentificeerd als ongebruikelijk of verdacht en die een beveiligingsrisico kan vormen voor de IT-infrastructuur van het bedrijf. *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.

Ondersteuning voor eerdere versies van Kaspersky Endpoint Security

Als u Kaspersky Endpoint Security 11.2.0–11.6.0 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-distributiepakket niet langer deel uit van de Kaspersky Endpoint Security-distributiekit.

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).

Integratie van de ingebouwde agent met EDR Optimum / EDR Expert

Om integratie met Kaspersky Endpoint Detection and Response in te stellen, moet u het onderdeel Endpoint Detection and Response Optimum of het onderdeel Endpoint Detection and Response Expert (cloud) toevoegen en Kaspersky Endpoint Security configureren.

De Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud), en Endpoint Detection and Response Expert (on-premises) onderdelen zijn niet compatibel met elkaar.

Aan de volgende voorwaarden moet worden voldaan om Endpoint Detection and Response te laten werken:

- Kaspersky Security Center versie 13.2 of hoger. In eerdere versies van Kaspersky Security Center is het onmogelijk om de Endpoint Detection and Response-functie te activeren.
- Kaspersky Endpoint Detection and Response beheerplug-in.

  Vanaf Kaspersky Endpoint Security versie 12.6 is de weergave van waarschuwingsdetails verplaatst van de beheerplug-in van Kaspersky Endpoint Security naar de beheerplug-in van EDR. De beheerplug-in van EDR is een enkele plug-in voor het werken met agents op Windows-, Mac- en Linux-besturingssystemen. Als u nu met EDR Optimum werkt, hebt u de beheerplug-in van Kaspersky Endpoint Security nodig om responstaken op bedreigingen te creëren en de beheerplug-in van EDR om waarschuwingsdetails te bekijken.
- Het Endpoint Detection and Response 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.
- 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 de component Endpoint Detection and Response Optimum of het onderdeel Endpoint Detection and Response Expert (cloud) selecteren tijdens installation of upgrade, en ook via de taak *Programmaonderdelen wijzigen*.

   > 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 functionaliteit is onmiddelijk beschikbaar na de activering van Kaspersky Endpoint Security voor Windows.

   - Een afzonderlijke licentie kpopen voor EDR Optimum of EDR Expert. (Kaspersky Endpoint Detection and Response add-on).

     De functionaliteit wordt beschikbaar na toevoeging van een afzonderlijke sleutel voor Kaspersky Endpoint Detection and Response. Als resultaat worden er twee sleutels op de computer toegevoegd: 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.

   Voor meer informatie over de EDR Optimum Gebruiksrechtovereenkomst raadpleeg de Help van Kaspersky Endpoint Detection and Response Optimum.

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 in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
   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 **Built-in Agents Configuration** → **Endpoint Detection and Response**.
   5. Zet de schakelaar **Endpoint Detection and Response ENABLED** aan.
   6. Sla uw wijzigingen op.

Het onderdeel Kaspersky Endpoint Detection and Response is ingeschakeld. Controleer de werkingsstatus van het onderdeel door het *Report on status of application components* 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 (cloud)** 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 in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
   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** → **KSC Integration**.
   5. Klik in het blok **Data transfer to Administration Server** op de koppeling **Advanced settings**.
   6. Selecteer in het venster dat opent de selectievakjes:
      - **About Quarantine files**.
      - **About a threat development chain**.
   7. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

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 Scan*-taak 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. *IOC-bestanden* 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 OpenIOC-norm.

IOC Scan -taak uitvoeren-modus

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.

DOWNLOAD HET BESTAND IOC_TERMS.XLSX

Kaspersky Endpoint Security ondersteunt ook alleenstaande IOC-scantasken wanneer het programma gebruikt wordt als onderdeel van de oplossing Kaspersky Sandbox.

IOC-bestand maken

Vanaf Kaspersky Endpoint Security 12.10 voor Windows kunt u IOC-bestanden rechtstreeks in de taakinstellingen maken. Om een IOC-bestand te maken, moet u een TXT-bestand voorbereiden met een lijst met Indicator of Compromise. U kunt lijsten met de volgende objecten toevoegen als indicatoren voor een compromis:

- Bestandshashes (MD5 / SHA256).

  Het programma bereidt een IOC-bestand voor met een FileItem/Md5sum of FileItem/Sha256sum scanbereik.

- IP-adressen (IPv4, IPv6).

  Het programma bereidt een IOC-bestand voor met een PortItem/RemoteIP scanbereik.

- DNS-namen.

  Het programma bereidt een IOC-bestand voor met een DnsEntryItem/RecordName scanbereik.

IOC-bestand maken in de Webconsole

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

   De lijst met taken wordt geopend.

2. Selecteer de taak **IOC Scan**.

   U ziet nu het venster met de taakeigenschappen. Maak indien nodig de **IOC Scan**-taak aan.

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

4. Ga naar het gedeelte **Threat Scan**.

5. Klik op **Redefine IOC files**.

6. Hiermee opent u het formulier voor het maken van een IOC-bestand:

   a. Onder **IOC files source**, selecteer **Generate from file**.

   b. Voer de naam van het IOC-bestand in.

   c. Selecteer een TXT-bestand met een lijst met indicatoren voor een compromis.

   d. Selecteer het type van het IOC-bestand: **DNS names**, **File hashes**, **IP addresses**.

   e. Klik op **Generate**.

   Kaspersky Endpoint Security voegt IOC-bestanden toe aan de IOC-verzameling. Indien nodig kunt u IOC-bestanden tijdelijk uitsluiten van het taakbereik.

7. Sla uw wijzigingen op.

Een IOC Scan-taak maken

U kunt *IOC Scan* taken 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.

Een taak IOC Scan maken:

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

   De lijst met taken wordt geopend.

2. Klik op **Add**.

   De wizard Taak wordt gestart.

3. Configureer de taakinstellingen:

   a. Selecteer in de vervolgkeuzelijst **Application** de optie **Kaspersky Endpoint Security for Windows 14.1.0**.

   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 **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. 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 Scan* taak 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. Voltooi de wizard.

   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 **Threat Scan**.

10. Upload de IOC-bestanden om Indicators of Compromise te zoeken.

    Nadat u de IOC-bestanden hebt geüpload, toont het programma beknopte informatie over het bestand, inclusief de lijst met indicatoren die de controle niet hebben doorstaan. Na het uploaden van IOC-bestanden kunt u de bestanden handmatig bewerken in de ingebouwde editor, rechtstreeks in de taakeigenschappen. Kaspersky Endpoint Security ondersteunt de bewerking van IOC-bestanden die voldoen aan de OpenIOC 1.1-standaard. Het is niet mogelijk om de inhoud van IOC-bestanden die compatibel zijn met OpenIOC versie 1.0 te wijzigen.

    Kaspersky Endpoint Security voegt IOC-bestanden toe aan de IOC-verzameling. Indien nodig kunt u IOC-bestanden tijdelijk uitsluiten van het taakbereik.

    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. Schakel indien nodig het selectievakje **Retrospective IOC Scan** in. *Retrospectieve IOC-scan* is een modus van de *IOC Scan* taak waarbij Kaspersky Endpoint Security gedurende een bepaalde periode scant op indicatoren van besmetting met behulp van gegevens. Deze modus is bedoeld voor het zoeken naar indicatoren van besmetting door de telemetrie van de beschermde computer, zoals netwerkactiviteit, processen, bestanden en andere telemetriegegevens. Kaspersky Endpoint Security analyseert gegevens in logboeken van het besturingssysteem en browserlogboeken op de computer. De Retrospective IOC Scan analyseert logboeken van de volgende browsers: Google Chrome, Mozilla Firefox, Microsoft Edge (versie 79 of hoger).

12. Configureer acties bij de detectie van IOC's:

- **Isolate device 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.

  Als dit selectievakje is uitgeschakeld, kunt u de computer van het netwerk isoleren nadat u de taak handmatig hebt uitgevoerd. Als de *IOC Scan*taak een IOC detecteert, kunt u de computer rechtstreeks van het netwerk isoleren van het IOC (eigenschappen van de taak *IOC Scan* → **Application settings** → **IOC Scan results**). Met Kaspersky Endpoint Security kunt u ook onmiddellijk extra instellingen beheren: Uitgeschakelde periode voor netwerkisolatie en uitzonderingen voor netwerkisolatie.

- **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.

  Als dit selectievakje is uitgeschakeld, kunt u het bestand handmatig in quarantaine plaatsen nadat u de taak handmatig hebt uitgevoerd. Als de *IOC Scan*taak een bestand detecteert dat gegevens kan compromitteren, kunt u dit bestand rechtstreeks vanuit IOC Scan-resultaten in quarantaine plaatsen (**Application settings** → **IOC Scan results**). Als gevolg hiervan start Kaspersky Endpoint Security de wizard voor het maken van taken met vooraf ingestelde gegevens van het gedetecteerde bestand. U hoeft alleen extra taakinstellingen te beheren, zoals het instellen van de taakplanning.

- **Run Critical Areas Scan**. Als deze optie is geselecteerd, start Kaspersky Endpoint Security de taak *Critical Areas Scan*. Standaard scant Kaspersky Endpoint Security het kernelgeheugen, actieve processen en de opstartsectoren van de schijf.

13. Ga naar het gedeelte **Advanced**.

14. Selecteer gegevenstypen (IOC-documenten) die als onderdeel van de taak moeten worden geanalyseerd.

> Kaspersky Endpoint Security selecteert automatisch gegevenstypen (IOC-documenten) voor de *IOC Scan*-taak op basis van 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 Log - 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.

- **Windows Registry - RegistryItem**. Configureer het bereik van de IOC-scan in het register.

  Kaspersky Endpoint Security scant standaard een set registersleutels.

15. Selecteer het tabblad **Schedule** in het venster met taakeigenschappen.

16. 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.

17. Sla uw wijzigingen op.

18. Schakel het selectievakje naast de taak in.

19. Klik op **Start**.

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: **Application settings** → **IOC Scan results**. In de resultaten van IOC-scan kunt u ook handmatig het gedetecteerde bestand in quarantaine plaatsen of isoleer de computer van het netwerk.

Kaspersky Endpoint Security zoekt naar duplicaten tussen records die voor hetzelfde IOC-bestand zijn gemaakt en bewaart alleen unieke records in de taakresultaten. Duplicaten zijn records van hetzelfde type met dezelfde waarden van alle vergeleken velden. Het programma maakt mogelijk ook geen record als een waarde in een of meer velden ontbreekt (zie de onderstaande tabel).

Type	Vergeleken velden	Voorwaarde voor het niet maken van een record
FileItem	• FullPath • Md5sum • Sha256sum • PID • UPID • ImagePath	• Ontbrekende waarde van de FullPath, Md5sum, Sha256sum velden. • Ontbrekende waarden van de FullPath veld en identieke waarden van de Md5sum, Sha256sum velden.
Registeritem	• Hive • KeyPath • ValueName • Text • Type	Ontbrekende waarde van ten minste een van de volgende velden: Hive, KeyPath, ValueName.
Procesitem	• startTime • PID	Ontbrekende waarden van de startTime of PID velden.

> De **Alert Details** kan het venster Registeritem-records met identieke veldwaarden worden weergegeven. Dergelijke records zijn geen duplicaten omdat ze verschillende waarden hebben in het tekstveld, dat niet wordt weergegeven in de interface.

> De resultaten van een IOC-scan worden 30 dagen bewaard. Na die tijd worden de oudste gegevens automatisch verwijderd door Kaspersky Endpoint Security.

Uitgebreide telemetrie voor IOC-scan

We raden aan om uitgebreide telemetrie op de computer in te schakelen voor retrospectieve IOC-scans. Uitgebreide telemetrie verbetert de nauwkeurigheid van IOC-detectie, maar gebruikt meer bronnen van de computer.

Uitgebreide telemetrie omvat de ondersteuning van de volgende aanvullende voorwaarden:

- FileItem/Md5sum
- FileItem/Sha256sum
- FileItem/SizeInBytes
- FileItem/Created
- FileItem/Modified
- FileItem/Changed
- FileItem/Accessed
- FileItem/FileAttributes

Als uitgebreide telemetrie is uitgeschakeld, kan Kaspersky Endpoint Security de informatie over gedetecteerde indicatoren van een besmetting rouleren.

Zo schakelt u uitgebreide telemetrie in:

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Built-in Agents Configuration** → **Endpoint Detection and Response**.
5. Selecteer het selectievakje **Enable advanced system activity logging**.
6. Sla uw wijzigingen op.

Bestand in Quarantaine plaatsen

Als reactie op een dreiging kunnen Kaspersky Endpoint Detection and Response *Move file to Quarantine*-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 wanneer het is geïntegreerd met Kaspersky Detection and Response-oplossingen. 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, Kaspersky Endpoint Detection and Response Expert Help, Kaspersky Anti Targeted Attack Platform Help, en Kaspersky Endpoint Detection and Response Expert (on-premises) Help.

U kun op de volgende manieren *Move file to Quarantine*-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.

- In de *IOC Scan*taak instellingen.

  Als de *IOC Scan*taak een bestand detecteert dat gegevens kan compromitteren, kunt u dit bestand rechtstreeks vanuit IOC Scan-resultaten in quarantaine plaatsen (**Application settings** → **IOC Scan results**). Als gevolg hiervan start Kaspersky Endpoint Security de wizard voor het maken van taken met vooraf ingestelde gegevens van het gedetecteerde bestand. U hoeft alleen extra taakinstellingen te beheren, zoals het instellen van de taakplanning.

De taak *Move file to Quarantine* 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.
4. U kunt geen objecten scannen die in quarantaine zijn geplaatst met de taak *Move file to Quarantine*.

Een taak Move file to Quarantine maken:

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

   De lijst met taken wordt geopend.

2. Klik op **Add**.

   De wizard Taak wordt gestart.

3. Configureer de taakinstellingen:

   a. Selecteer in de vervolgkeuzelijst **Application** de optie **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. Selecteer in de vervolgkeuzelijst **Task type** de optie **Move file to Quarantine**.

   c. Typ in het veld **Task name** een korte omschrijving.

   d. Selecteer in het gedeelte **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 **Next**.

5. Voer de accountgegevens in van de gebruiker wiens rechten u wilt gebruiken om de taak uit te voeren. Klik op **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 **Add**.

   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 **Schedule** 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. Sla uw wijzigingen op.

14. Schakel het selectievakje naast de taak in.

15. Klik op **Start**.

    Kaspersky Endpoint Security verplaatst nu het bestand naar Quarantaine.

Als het bestand is vergrendeld door een ander proces, wordt de taak weergegeven als *Completed*, maar het bestand wordt pas verwijderd nadat de computer opnieuw is opgestart. Controleer na het opnieuw opstarten van de computer of het bestand is verwijderd.

De taak *Move file to Quarantine* kan worden afgebroken met de foutmelding *Toegang geweigerd* wanneer u probeert een uitvoerbaar bestand dat momenteel wordt uitgevoerd in quarantaine te plaatsen. Maak een Proces beëindigd-taak voor het bestand en probeer het opnieuw.

De taak *Move file to Quarantine* kan worden afgebroken met de foutmelding *Onvoldoende ruimte in Quarantaine* wanneer u probeert een te groot bestand in quarantaine te plaatsen. 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. Na het uitvoeren van de taak wordt het bestand opgeslagen in Quarantaine. *Quarantaine* is een speciale lokale opslagplaats op de computer. Met Webconsole kunt u dit bestand vanuit Quarantaine downloaden naar uw computer (**Handelingen** → **Opslag** → **Quarantaine**). 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.

Een taak Bestand ophalen maken:

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

   De lijst met taken wordt geopend.

2. Klik op **Add**.

   De wizard Taak wordt gestart.

3. Configureer de taakinstellingen:

   a. Selecteer in de vervolgkeuzelijst **Application** de optie **Kaspersky Endpoint Security for Windows 14.1.0**.

   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 **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 **Next**.

5. Voer de accountgegevens in van de gebruiker wiens rechten u wilt gebruiken om de taak uit te voeren. Klik op **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 **Add**.

   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 **Schedule** 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. Sla uw wijzigingen op.
14. Schakel het selectievakje naast de taak in.
15. Klik op **Start**.

    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 *Delete file* kunt u op afstand bestanden verwijderen. bijvoorbeeld wanneer er sprake is van een dreiging.

De taak *Delete file* heeft de volgende beperkingen:

- System Critical Object (SCO) kan niet worden verwijderd. SCO's zijn bestanden die het besturingssysteem en Kaspersky Endpoint Security 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.

Een taak Delete file maken:

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

   De lijst met taken wordt geopend.
2. Klik op **Add**.

   De wizard Taak wordt gestart.

3. Configureer de taakinstellingen:

   a. Selecteer in de vervolgkeuzelijst **Application** de optie **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. Selecteer in de vervolgkeuzelijst **Task type** de optie **Delete file**.

   c. Typ in het veld **Task name** een korte omschrijving.

   d. Selecteer in het gedeelte **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 **Next**.

5. Voer de accountgegevens in van de gebruiker wiens rechten u wilt gebruiken om de taak uit te voeren. Klik op **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 **Add**.

   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 **Schedule** 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. Sla uw wijzigingen op.

14. Schakel het selectievakje naast de taak in.

15. Klik op **Start**.

Kaspersky Endpoint Security verwijdert nu het bestand van de computer. Als het bestand is vergrendeld

vanwege een ander proces, wordt de taak weergegeven als *Done*. 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 *Delete file* wordt mogelijk afgebroken na de foutmelding *Access denied or file not found* 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 *Process start* 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 *Receive file from device* 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.

Een taak Process start maken:

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

   De lijst met taken wordt geopend.

2. Klik op **Add**.

   De wizard Taak wordt gestart.

3. Configureer de taakinstellingen:

   a. Selecteer in de vervolgkeuzelijst **Application** de optie **Kaspersky Endpoint Security for Windows 14.1.0**.

   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 **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 **Next**.

5. Voer de accountgegevens in van de gebruiker wiens rechten u wilt gebruiken om de taak uit te voeren. Klik op **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.

    Stel dat u een hulpprogramma (`utility.exe`) wilt uitvoeren dat de informatie over de configuratie van een computer opslaat in een bestand met de naam `conf.txt` in de huidige map (standaard). Het hulpprogramma is in de `C:\Users\admin\Diagnostic\` map. U moet het configuratiebestand opslaan in de `C:\Users\admin\Documents\Configuration` map. Voer de volgende waarden in:

    - **Executable command** – `C:\Users\admin\Diagnostic\utility.exe`
    - **Command line arguments (optional)** – `/R conf.txt`
    - **Path to the working folder (optional)** – `C:\Users\admin\Documents\Configuration`

11. Selecteer het tabblad **Schedule** 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. Sla uw wijzigingen op.

14. Schakel het selectievakje naast de taak in.

15. Klik op **Start**.

    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 **Execution results**.

Proces beëindigen

Met de taak *Terminate process* 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 *Terminate process* 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 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.

Een taak Terminate process maken:

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

   De lijst met taken wordt geopend.

2. Klik op **Add**.

   De wizard Taak wordt gestart.

3. Configureer de taakinstellingen:

   a. Selecteer in de vervolgkeuzelijst **Application** de optie **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. Selecteer in de vervolgkeuzelijst **Task type** de optie **Terminate process**.

   c. Typ in het veld **Task name** een korte omschrijving.

   d. Selecteer in het gedeelte **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 **Next**.

5. Voer de accountgegevens in van de gebruiker wiens rechten u wilt gebruiken om de taak uit te voeren. Klik op **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 **Save**.

13. Schakel het selectievakje naast de taak in.

14. Klik op **Start**.

    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.

Preventie van uitvoering heeft de volgende beperkingen:

1. 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.

2. Het is onmogelijk om het opstarten van systeemkritische objecten (SCO) te blokkeren. SCO's zijn bestanden die het besturingssysteem en Kaspersky Endpoint Security nodig hebben om te kunnen werken.

3. Het is niet aanbevolen om meer dan 5000 regels voor runpreventie te maken, omdat dit systeeminstabiliteit kan veroorzaken.

Regelmodi voor preventie van uitvoering

Het component voor preventie van uitvoering kan werken in twee modi:

- **Alleen statistieken**

  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 in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Built-in Agents Configuration** → **Endpoint Detection and Response**.
5. Selecteer het tabblad **Execution Prevention**.
6. Zet de schakelaar **Execution Prevention ENABLED** aan.
7. Selecteer in het blok **Action on execution or opening of forbidden object** de uitvoermodus voor het onderdeel:

   - **Block and add to event log**. 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.

   - **Add to event log**. 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.

8. Maak een lijst met regels voor de preventie van uitvoering:

   a. Klik op **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.

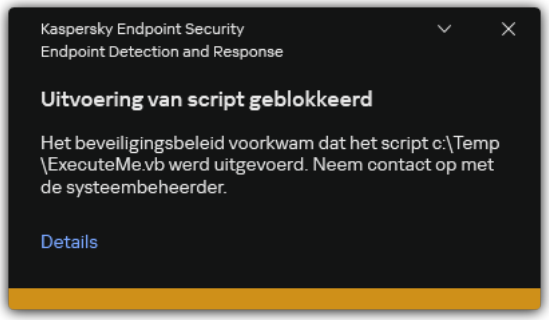
   d. Om het bestand toe te voegen, moet u de hash van het bestand (SHA256 of MD5), het volledige pad naar het bestand of zowel de hash als het pad invoeren.

   > 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.

   Preventie van uitvoering ondersteunt een reeks office-bestandsextensies en een reeks scriptinterpreters.

9. 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.
- Verbindingen met de SVM en de Integration Server als het programma in de Light Agent-modus wordt gebruikt.
- Verbindingen met KSN bij integratie van het programma met Kaspersky Managed Detection and Response.

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 **Asset management** → **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 de automatische netwerkisolatie zo configureren dat deze na een bepaalde tijd wordt uitgeschakeld. 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 **Asset management** → **Policies**.
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 **Built-in Agents Configuration** → **Endpoint Detection and Response**.
5. Selecteer het tabblad **Network Isolation**.
6. Selecteer de vertraging voor het 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
- In de *IOC Scan*taak instellingen.

  Als de *IOC Scan*taak een IOC detecteert, kunt u de computer rechtstreeks van het netwerk isoleren van het IOC (eigenschappen van de taak *IOC Scan* → **Application settings** → **IOC Scan results**). Met Kaspersky Endpoint Security kunt u ook onmiddellijk extra instellingen beheren: Uitgeschakelde periode voor netwerkisolatie en uitzonderingen voor netwerkisolatie.

Netwerkisolatie van een computer handmatig inschakelen

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Assets (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 de automatische netwerkisolatie zo configureren dat deze na een bepaalde tijd wordt uitgeschakeld. 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 **Asset management → Assets (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 **Asset management → Assets (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.

Vanaf Kaspersky Endpoint Security 12.10 voor Windows kunt u Netwerkisolatie beheren in de details van de waarschuwing. Bovendien kunt u in de details van de waarschuwing de periode voor computer isoleren van netwerk opgeven. 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.

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 **Asset management** → **Policies**.
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 **Built-in Agents Configuration** → **Endpoint Detection and Response**.
5. Selecteer het tabblad **Network Isolation**.
6. Klik in het blok **Network isolation exclusions Exclusions**.
7. Dit opent een venster. Klik in dit venster op **Add** → **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 netwerkverbindingsinstellingen wijzigen.
8. Voeg indien nodig handmatig een uitzondering voor netwerkisolatie toe. Klik hiervoor in het venster met de lijst met uitzonderingen op **Add** → **Add** en bewerk de instellingen van netwerkverbindingen handmatig.
9. Sla uw wijzigingen op.

Uitzondering netwerkisolatie toevoegen in handmatige modus

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Assets (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 netwerkverbindingsinstellingen 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.

Vanaf Kaspersky Endpoint Security 12.10 voor Windows kunt u de uitzonderingen voor Netwerkisolatie toevoegen in de details van de waarschuwing. 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.

Cloud Sandbox

Cloud Sandbox is een technologie waarmee u geavanceerde bedreigingen op een computer kunt detecteren. Kaspersky Endpoint Security stuurt gedetecteerde bestanden automatisch door naar Cloud Sandbox voor analyse. Cloud Sandbox voert deze bestanden uit in een geïsoleerde omgeving om kwaadaardige activiteiten te identificeren en over hun reputatie te beslissen. Gegevens over deze bestanden worden vervolgens naar Kaspersky Security Network verzonden. Als Cloud Sandbox daarom een kwaadaardig bestand heeft gedetecteerd, zal Kaspersky Endpoint Security de juiste actie ondernemen om deze bedreiging te elimineren op alle computers waarop dit bestand wordt gedetecteerd.

Voor de werking van Cloud Sandbox, moet u het gebruik van Kaspersky Security Network inschakelen.

Als u Kaspersky Private Security Network gebruikt, is Cloud Sandbox-technologie niet beschikbaar.

Cloud Sandbox-technologie is permanent ingeschakeld en is beschikbaar voor alle gebruikers van Kaspersky Security Network, ongeacht het type licentie dat ze gebruiken. Als u Endpoint Detection and Response Optimum-oplossingen al heeft geïmplementeerd, kunt u een aparte teller inschakelen voor door Cloud Sandbox gedetecteerde dreigingen. U kunt deze teller gebruiken om statistieken te compileren bij de analyse van gedetecteerde bedreigingen. Kaspersky Endpoint Security geeft Cloud Sandbox-technologie aan in het *Report on threats* in de Kaspersky Security Center-console.



Tellers van bedreigingen

De Cloud Sandbox-teller inschakelen:

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Built-in Agents Configuration** → **Endpoint Detection and Response**.
5. Selecteer het tabblad **Cloud Sandbox**.
6. Zet de schakelaar **Cloud Sandbox ENABLED** aan.
7. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Telkens wanneer er een bedreiging is, activeert Kaspersky Endpoint Security de teller voor dreigingen gedetecteerd met Cloud Sandbox in het hoofdvenster van het programma onder **Technologieën voor detectie van dreigingen**. Kaspersky Endpoint Security zal ook Cloud Sandbox-technologie aangeven in het *Report on threats* in de Kaspersky Security Center-console.

Migratiegids van KEA naar KES voor EDR Optimum

Kaspersky Endpoint Security voor Windows bevat een ingebouwde agent voor de Kaspersky Endpoint Detection and Response Optimum-oplossing. U hebt geen apart Kaspersky Endpoint Agent-programma meer nodig om met EDR Optimum te werken. Alle functies van Kaspersky Endpoint Agent worden uitgevoerd door Kaspersky Endpoint Security.

Wanneer u Kaspersky Endpoint Security implementeert op computers waarop Kaspersky Endpoint Agent is geïnstalleerd, blijven Kaspersky Endpoint Detection and Response Optimum-oplossingen werken met Kaspersky Endpoint Security. Daarnaast wordt Kaspersky Endpoint Agent van de computer verwijderd. Hetzelfde gedrag in het systeem zal optreden wanneer u Kaspersky Endpoint Security bijwerkt naar versie 11.7.0 of hoger.

Kaspersky Endpoint Security is niet compatibel met Kaspersky Endpoint Agent. U kunt deze programma's niet beide op dezelfde computer installeren.

Kaspersky Endpoint Security moet aan de volgende voorwaarden voldoen om te werken als onderdeel van Kaspersky Endpoint Detection and Response Optimum:

- Kaspersky Endpoint Detection and Response Optimum 2.0 of hoger.
- Kaspersky Security Center versie 13.2 of hoger (inclusief Network Agent). In eerdere versies van Kaspersky Security Center is het onmogelijk om de EDR Optimum-functie te activeren.
- EDR Optimum kan alleen worden beheerd met behulp van Kaspersky Security Center Web Console.
- Gegevensoverdracht naar Administration Server is ingeschakeld. De gegevens zijn nodig om via Webconsole informatie te verkrijgen over bestanden die op een computer in quarantaine zijn geplaatst.
- Er is een achtergrondverbinding tot stand gebracht tussen Kaspersky Security Center Webconsole en Administration Server Om EDR Optimum te laten werken met Administration Server via Kaspersky Security Center Web Console, moet u een nieuwe beveiligde verbinding tot stand brengen, een *achtergrondverbinding*.

Stappen voor het migreren van [KES+KEA] configuratie naar [KES + ingebouwde agent] voor EDR Optimum

1. **De webplug-in voor Kaspersky Endpoint Security upgraden**

   De EDR Optimum-component kan worden beheerd met de Kaspersky Endpoint Security-webplug-in versie 11.7.0 of hoger.

2. **Beleid en taken migreren**

   Zet Kaspersky Endpoint Agent-instellingen over naar Kaspersky Endpoint Security for Windows. Gebruik hiervoor de wizard voor migreren vanuit Kaspersky Endpoint Agent in de webconsole.

   Zo migreert u beleids- en taakinstellingen van Kaspersky Endpoint Agent naar Kaspersky Endpoint Security in webconsole

   Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Operations → Migration from Kaspersky Endpoint Agent**.

Hiermee wordt de wizard beleiden- en takenmigratie uitgevoerd. 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 het 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. In de takenlijst selecteert u de Kaspersky Endpoint Agent-taken die u wilt maken voor het Kaspersky Endpoint Security-beleid. Ga naar de volgende stap.

Stap 3. Voltooiing van wizard

Verlaat de wizard verlaten. Als gevolg hiervan doet de wizard het volgende:

- Maakt een nieuw Kaspersky Endpoint Security-beleid.

  Het beleid voegt instellingen van Kaspersky Endpoint Security en Kaspersky Endpoint Agent samen. Het beleid krijgt de naam *<Naam van Kaspersky Endpoint Security-beleid> & <Naam van Kaspersky Endpoint Agent-beleid>*. Het nieuwe beleid heeft de status *Inactive*. Wijzig nu de statussen van het Kaspersky Endpoint Agent-beleid en het Kaspersky Endpoint Security-beleid in *Inactive* 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. De taken van Kaspersky Endpoint Agent worden door de wizard niet gewijzigd.

3 Het licentiëren van de EDR Optimum-functionaliteit

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 of hoger. 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 of hoger, 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 *Add key*.

4. **Het Kaspersky Endpoint Security-programma installeren/ upgraden**

Om EDR Optimum-functionaliteit te migreren tijdens de installatie of upgrade van een applicatie, wordt aanbevolen om de installatietaak op afstand. Wanneer u een installatietaak op afstand maakt, moet u het EDR Optimum-component selecteren in de instellingen van het installatiepakket.

U kunt het programma ook upgraden met behulp van de volgende methoden:

- Met Kaspersky-updateservice.
- Lokaal, met behulp van de Installatiewizard.

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 actuele 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 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 actuele licenties van Kaspersky-oplossingen. In dit geval selecteert Kaspersky Endpoint Security automatisch onderdelen op basis van de Kaspersky Endpoint Agent-configuratie: Hierna schakelt Kaspersky Endpoint Security over op het gebruik van de ingebouwde agent en wordt Kaspersky Endpoint Agent verwijderd.

Kaspersky Endpoint Security ondersteunt upgraden zonder de computer opnieuw op te starten. U kunt de toepassingsupgrademodus in beleidseigenschappen.

5. **De werking van het programma controleren**

Als de computer na installatie of upgrade de status *Critical* heeft in de Kaspersky Security Center-console:

- Zorg ervoor dat op de computer Netwerkagent versie 13.2 of hoger is geïnstalleerd.
- Controleer de werkingsstatus van het ingebouwde agent door het *Report on status of application components* te bekijken. Als een onderdeel de status *Not installed* heeft, installeer dan de onderdeel met de taak *Change application components*. Als een onderdeel de *Geen onderdeel van licentie* toestand heeft, zorg er dan voor dat u de ingebouwde agent-functionaliteit heeft geactiveerd.
- Zorg ervoor dat u akkoord gaat met de Kaspersky Security Network-verklaring in het nieuwe beleid van Kaspersky Endpoint Security voor Windows.

Kaspersky Sandbox

Kaspersky Endpoint Security for Windows heeft een ingebouwde agent voor integratie met de Kaspersky Sandbox-oplossing. Het *Sandbox*-onderdeel detecteert en blokkeert automatisch geavanceerde dreigingen op computers. Sandbox analyseert het gedrag van objecten om schadelijke activiteit en activiteit kenmerkend voor doelgerichte aanvallen op de IT-infrastructuur van het bedrijf te detecteren. Sandbox analyseert en scant objecten op speciale servers met geïmplementeerde virtuele kopieën van Microsoft Windows-besturingssystemen (Sandbox-servers). Voor informatie over de oplossing raadpleeg de Help van Kaspersky Sandbox en Help van Kaspersky Anti Targeted Attack Platform.

Integratie van de ingebouwde agent met Kaspersky Sandbox

Het toevoegen van de Kaspersky Sandbox-component is vereist voor integratie met Kaspersky Sandbox. U kunt het Sandbox-component selecteren tijdens: installatie of upgrade, alsook tijdens het gebruik van de taak *Programmaonderdelen wijzigen*.

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 is ingeschakeld.

  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 in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
  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** → **KSC Integration**.
  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 achtereenvolgens **Settings** → **Integration**.
2. Ga naar het gedeelte **Integration**.
3. Zet de schakelaar **Background connection for integration Enabled** 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.

- Om een vertrouwde verbinding met de Sandbox-server te configureren, moet u een TLS-certificaat voorbereiden. Vervolgens moet u het certificaat met behulp van een beleid aan de computer toevoegen. U moet het certificaat ook toevoegen aan de Sandbox-server.

  Tweerichtingsverificatie met behulp van een crypto-container is niet beschikbaar voor Kaspersky Sandbox.

  U kunt in webconsole of ook lokaal een TLS-certificaat aan de computer toevoegen met behulp van de opdrachtregel.

- Het onderdeel Kaspersky Sandbox wordt ingeschakeld.
- Programmaonderdelen die zorgen voor de werking van Sandbox zijn ingeschakeld en operationeel. De volgende onderdelen zorgen voor de werking van Sandbox:
  - File Threat Protection.
  - Host Intrusion Prevention.
  - Firewall.
  - AMSI-bescherming.
  - Achtergrondscan.

De integratie met Kaspersky Sandbox in- of uitschakelen:

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Built-in Agents Configuration** → **Sandbox**.
5. Gebruik de schakelaar **Integration with Sandbox ENABLED** om de component in of uit te schakelen.

6. Selecteer in het blok **Integration mode** de uitvoermodus voor het onderdeel: **Kaspersky Sandbox**.

7. Klik op de koppeling **Connection settings**.

   Dit opent het venster Sandbox-serververbindingsinstellingen.

8. Klik in het blok **Server TLS certificate** op **Upload** en selecteer het TLS-certificaatbestand.

   Kaspersky Endpoint Security kan slechts één TLS-certificaat hebben voor een Sandbox-server. Als u al eerder een TLS-certificaat hebt toegevoegd, dan wordt dat certificaat ingetrokken. Alleen het laatst toegevoegde certificaat wordt gebruikt.

9. Configureer geavanceerde verbindingsinstellingen voor Sandbox-servers:

   - **Timeout (msec)**. Verbindingstime-out voor de 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 de server verlengen als uw verbindingssnelheid laag is of als de verbinding onstabiel is. De aanbevolen timeout voor een aanvraag is 0,5 seconden of minder.

   - **Request queue**. Grootte van de verzoekwachtrijmap. Bij het verzenden van meerdere objecten om te scannen in Sandbox, maakt Kaspersky Endpoint Security een wachtrij voor aanvragen. Standaard is de grootte van de verzoekwachtrijmap beperkt tot 100 MB. Nadat de maximale grootte is bereikt, stopt 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.

10. In het blok **Connection to Sandbox servers**, klikt u op de knop **Add**.

11. Dit opent een venster; voer in dat venster het Sandbox-serveradres (IPv4, IPv6, DNS) en de poort in.

    Raadpleeg voor details over het inzetten van virtuele afbeeldingen en het configureren van Sandbox-servers de Kaspersky Sandbox Help.

12. 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. Controleer de werkingsstatus van het onderdeel door het *Report on status of application components* te bekijken. U kunt de werkingsstatus van een onderdeel ook in rapporten bekijken in de lokale interface van Kaspersky Endpoint Security. Het onderdeel **Sandbox** wordt toegevoegd aan de lijst met Kaspersky Endpoint Security-onderdelen.

U kunt de integratie met Kaspersky Sandbox in webonsole of lokaal in- of uitschakelen met de opdrachtregel.

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 `Error code: XXX` indeling (bijvoorbeeld, `0xa67b01f4`), neem dan contact op met de Technische Support.

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 Scan*-taak 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. *IOC-bestanden* 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 OpenIOC-norm. Kaspersky Endpoint Security genereert automatisch IOC-bestanden voor Kaspersky Sandbox.

IOC Scan -taak uitvoeren-modus

Het programma maakt zelfstandige IOC-scantaken voor Kaspersky Sandbox. De *zelfstandige IOC-scantaak* 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 van IOC Scan-taak

Kaspersky Sandbox kan automatisch *IOC Scan* taken 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 Scan-taak wijzigen:

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **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.

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 Critical Areas Scan**. Als deze optie is geselecteerd, start Kaspersky Endpoint Security de taak *Critical Areas Scan*. Standaard scant Kaspersky Endpoint Security het kernelgeheugen, actieve processen en de opstartsectoren van de schijf.

   - **Run only when the computer is idle**. Uitgestelde start van de taak 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. Met deze planningsoptie kunt u computervermogen besparen wanneer de computer wordt gebruikt.

6. 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: **Application settings** → **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.

Migratiegids van KEA naar KES voor Kaspersky Sandbox

Kaspersky Endpoint Security voor Windows bevat een ingebouwde agent voor de Kaspersky Sandbox-oplossing. U hebt geen apart Kaspersky Endpoint Agent-programma meer nodig om te werken met Kaspersky Sandbox. Alle functies van Kaspersky Endpoint Agent worden uitgevoerd door Kaspersky Endpoint Security.

Wanneer u Kaspersky Endpoint Security implementeert op computers waarop Kaspersky Endpoint Agent is geïnstalleerd, blijvt de Kaspersky Sandbox-oplossing werken met Kaspersky Endpoint Security. Daarnaast wordt Kaspersky Endpoint Agent van de computer verwijderd. Hetzelfde gedrag in het systeem zal optreden wanneer u Kaspersky Endpoint Security bijwerkt naar versie 11.7.0 of hoger.

Kaspersky Endpoint Security is niet compatibel met Kaspersky Endpoint Agent. U kunt deze programma's niet beide op dezelfde computer installeren.

Kaspersky Endpoint Security moet aan de volgende voorwaarden voldoen om te werken als onderdeel van Kaspersky Sandbox:

- Kaspersky Sandbox versie 2.0 of hoger.
- Kaspersky Security Center versie 13.2 of hoger (inclusief Network Agent). In eerdere versies van Kaspersky Security Center is het onmogelijk om de Kaspersky Sandbox-functie te activeren.
- Kaspersky Sandbox kan alleen worden beheerd met behulp van de Kaspersky Security Center Web Console.

- Gegevensoverdracht naar Administration Server is ingeschakeld. De gegevens zijn nodig om via Webconsole informatie te verkrijgen over bestanden die op een computer in quarantaine zijn geplaatst.
- 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*.

Stappen voor het migreren van [KES + KEA] configuratie naar [KES+ingebouwde agent] voor Kaspersky Sandbox

1. **De webplug-in voor Kaspersky Endpoint Security upgraden**

   Kaspersky Sandbox kan worden beheerd met de Kaspersky Endpoint Security-webplug-in versie 11.7.0 of hoger.

2. **Beleid en taken migreren**

   Zet Kaspersky Endpoint Agent-instellingen over naar Kaspersky Endpoint Security for Windows. Gebruik hiervoor de wizard voor migreren vanuit Kaspersky Endpoint Agent in de webconsole.

   Zo migreert u beleids- en taakinstellingen van Kaspersky Endpoint Agent naar Kaspersky Endpoint Security in webconsole

   Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Operations** → **Migration from Kaspersky Endpoint Agent**.

   Hiermee wordt de wizard beleiden- en takenmigratie uitgevoerd. 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 het 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. In de takenlijst selecteert u de Kaspersky Endpoint Agent-taken die u wilt maken voor het Kaspersky Endpoint Security-beleid. Ga naar de volgende stap.

Stap 3. Voltooiing van wizard

Verlaat de wizard verlaten. Als gevolg hiervan doet de wizard het volgende:

- Maakt een nieuw Kaspersky Endpoint Security-beleid.

  Het beleid voegt instellingen van Kaspersky Endpoint Security en Kaspersky Endpoint Agent samen. Het beleid krijgt de naam *<Naam van Kaspersky Endpoint Security-beleid> & <Naam van Kaspersky Endpoint Agent-beleid>*. Het nieuwe beleid heeft de status *Inactive*. Wijzig nu de statussen van het Kaspersky Endpoint Agent-beleid en het Kaspersky Endpoint Security-beleid in *Inactive* 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. De taken van Kaspersky Endpoint Agent worden door de wizard niet gewijzigd.

3 Licentieverlening voor de Kaspersky Sandbox-functionaliteit

Om Kaspersky Endpoint Security te activeren als onderdeel van de Kaspersky Sandbox-oplossing, hebt u een aparte licentie nodig voor Kaspersky Sandbox Add-on. U kunt dan de sleutel toevoegen met de taak *Add key*. Als gevolg hiervan worden twee sleutels aan programma toegevoegd: *Kaspersky Endpoint Security* en *Kaspersky Sandbox*.

4 Het Kaspersky Endpoint Security-programma installeren/ upgraden

Om Kaspersky Sandbox te migreren tijdens de installatie of upgrade van een applicatie, wordt aanbevolen om de installatietaak op afstand. Wanneer u een installatietaak op afstand maakt, moet u de Kaspersky Sandbox selecteren in de instellingen van het installatiepakket.

U kunt het programma ook upgraden met behulp van de volgende methoden:

- Met Kaspersky-updateservice.
- Lokaal, met behulp van de Installatiewizard.

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 actuele licenties van Kaspersky-oplossingen. Als op de computer bijvoorbeeld Kaspersky Endpoint Agent is geïnstalleerd en de Kaspersky Sandbox-oplossing is geactiveerd, configureert het Kaspersky Endpoint Security-installatieprogramma automatisch de set onderdelen en selecteert het Kaspersky Sandbox-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 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 actuele licenties van Kaspersky-oplossingen. In dit geval selecteert Kaspersky Endpoint Security automatisch onderdelen op basis van de Kaspersky Endpoint Agent-configuratie: Hierna schakelt Kaspersky Endpoint Security over op het gebruik van de ingebouwde agent en wordt Kaspersky Endpoint Agent verwijderd.

Kaspersky Endpoint Security ondersteunt upgraden zonder de computer opnieuw op te starten. U kunt de toepassingsupgrademodus in beleidseigenschappen.

5. **De werking van het programma controleren**

   Als de computer na installatie of upgrade de status *Critical* heeft in de Kaspersky Security Center-console:

   - Zorg ervoor dat op de computer Netwerkagent versie 13.2 of hoger is geïnstalleerd.
   - Controleer de werkingsstatus van het ingebouwde agent door het *Report on status of application components* te bekijken. Als een onderdeel de status *Not installed* heeft, installeer dan de onderdeel met de taak *Change application components*. Als een onderdeel de *Geen onderdeel van licentie* toestand heeft, zorg er dan voor dat u de ingebouwde agent-functionaliteit heeft geactiveerd.
   - Zorg ervoor dat u akkoord gaat met de Kaspersky Security Network-verklaring in het nieuwe beleid van Kaspersky Endpoint Security voor Windows.

Kaspersky Anti Targeted Attack Platform



Kaspersky Endpoint Security for Windows ondersteunt het werken met de Kaspersky Anti Targeted Attack Platform (EDR (KATA))-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 drie functionele eenheden:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

U kunt alle functionele eenheden of afzonderlijke functionele eenheden afzonderlijk kopen. Voor informatie over de oplossing raadpleegt u de Help van Kaspersky Anti Targeted Attack Platform. Het programma bevat ingebouwde agents voor EDR, NDR-onderdelen. Het programma ondersteunt ook het werken met het Sandbox-onderdeel dat is onderdeel van KATA.

Tools voor dreigingsinformatie

Kaspersky Endpoint Detection and Response gebruikt de volgende Threat Intelligence-tools:

- De integratie met Kaspersky Threat Intelligence Portal dat informatie over de reputatie van bestanden en webadressen bevat en toont.
- Kaspersky Threats-database.
- 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.

Werkingsprincipe van de oplossing

Het programma Kaspersky Endpoint Security 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 (telemetriegegevens) wordt verzonden naar de Kaspersky Anti Targeted Attack Platform-server. In dit geval verzendt Kaspersky Endpoint Security ook informatie naar de Kaspersky Anti Targeted Attack Platform-server over dreigingen gevonden door het programma, evenals informatie over verwerkingsresultaten voor deze dreigingen.

De EDR (KATA) en NDR (KATA)-integratie wordt geconfigureerd op de Kaspersky Security Center-console. De ingebouwde agent wordt vervolgens beheerd met behulp van de Kaspersky Anti Targeted Attack Platform-console, inclusief het uitvoeren van taken, het beheren van in quarantaine geplaatste objecten, het bekijken van rapporten en andere acties.

Kaspersky Endpoint Security-configuraties voor het werken met EDR / NDR (KATA)

Voor het werken met EDR/NDR (KATA) kunnen de volgende configuraties worden gebruikt:

- **[KES+built-in agent]**. In deze configuratie fungeert Kaspersky Endpoint Security zowel als het programma dat de veiligheid van de computer garandeert, als het programma voor het werken met EDR / NDR (KATA). De ingebouwde agent voor EDR (KATA) is beschikbaar in Kaspersky Endpoint Security 12.1 voor Windows of hoger. De ingebouwde agent voor NDR (KATA) is beschikbaar in Kaspersky Endpoint Security 12.7 voor Windows of hoger.
- **[EPP+EDR Agent van derden]**. In deze configuratie wordt de beveiliging van de IT-infrastructuur verzorgd door het Endpoint Protection Platform (EPP) van derden. De interactie met EDR/ NDR (KATA) wordt verzorgd door Kaspersky Endpoint Security in de configuratie Endpoint Detection and Response Agent (EDR Agent). In deze configuratie is EDR-agent compatibel met EPP-applicaties van derden. EDR-agent voor EDR (KATA) is beschikbaar in Kaspersky Endpoint Security 12.3 voor Windows of hoger. EDR-agent voor NDR (KATA) is beschikbaar in Kaspersky Endpoint Security 12.7 voor Windows of hoger.

Ondersteuning voor eerdere versies van Kaspersky Endpoint Security

Als u Kaspersky Endpoint Security 11.2.0–11.8.0 gebruikt voor interoperabiliteit met Kaspersky Anti Targeted Attack Platform (EDR), bevat het programma ook Kaspersky Endpoint Agent. U kunt Kaspersky Endpoint Agent samen met Kaspersky Endpoint Security installeren.

Als u Kaspersky Endpoint Security 11.9.0 – 12.0 gebruikt, moet u Kaspersky Endpoint Agent afzonderlijk installeren, vanaf Kaspersky Endpoint Security 11.9.0 maakt het Kaspersky Endpoint Agent-distributiepakket geen deel meer uit van de Kaspersky Endpoint Security-distributiekit.

Integratie van de ingebouwde agent met EDR / NDR (KATA)

Voor integratie met EDR/NDR (KATA) moet u de relevante onderdelen toevoegen: Endpoint Detection and Response (KATA) of Network Detection and Response (KATA). U kunt het onderdeel selecteren voor integratie met EDR / NDR (KATA) tijdens: installeren of upgraden van het programma, alsook tijdens het gebruik van de taak *Programmaonderdelen wijzigen*.

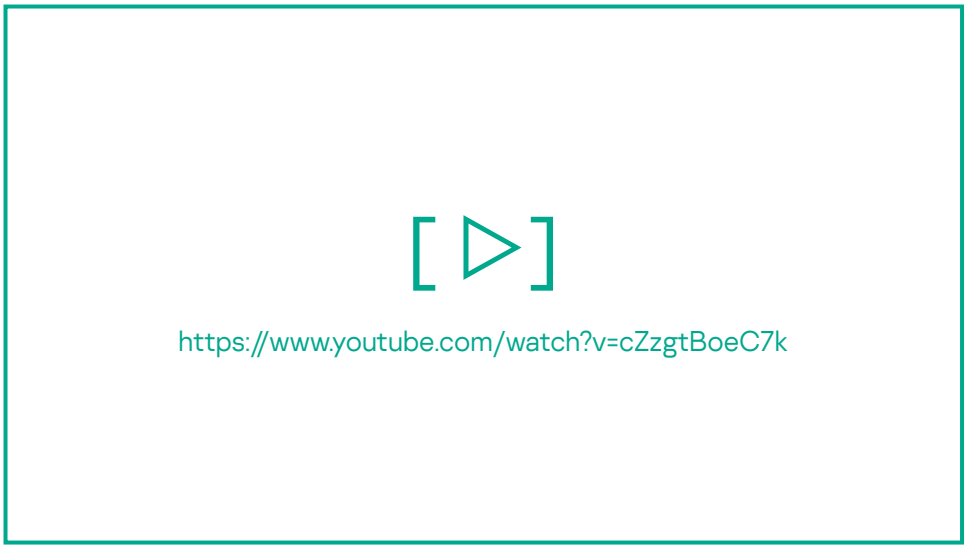
Vanaf versie 12.11 van Kaspersky Endpoint Security voor Windows is de naam van het onderdeel EDR (KATA) gewijzigd in **Endpoint Detection and Response Expert (version 8.0 or later)**. In deze versie van het programma is het onderdeel compatibel met Kaspersky Anti Targeted Attack Platform 7.1 en eerdere versies, evenals Kaspersky Endpoint Detection and Response Expert (on-premises).

De Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud), en Endpoint Detection and Response Expert (on-premises) onderdelen zijn niet compatibel met elkaar.

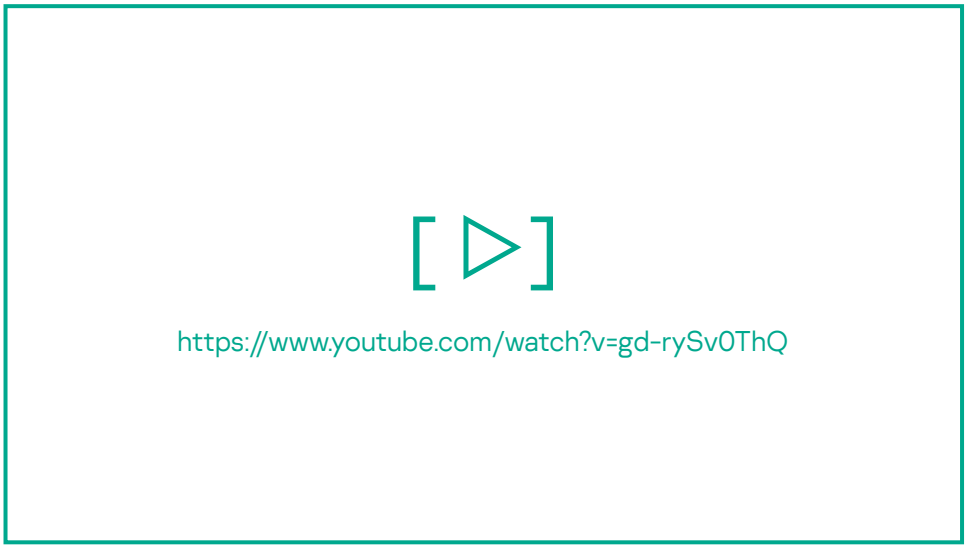
Voor het gebruik van EDR / NDR (KATA) moet aan de volgende voorwaarden worden voldaan:

- EDR (KATA): Kaspersky Anti Targeted Attack Platform versie 5.0-7.1.
- NDR (KATA): Kaspersky Anti Targeted Attack Platform versie 7.0 of hoger.
- EDR (KATA): Kaspersky Endpoint Security for Windows 12.1 of hoger. Voor meer informatie over de compatibiliteit van KATA met verschillende versies van Kaspersky Endpoint Security raadpleegt u de Help voor Kaspersky Anti Targeted Attack Platform.
- NDR (KATA): Kaspersky Endpoint Security for Windows 12.7 of hoger.
- Kaspersky Security Center versie 14.2 of hoger. In eerdere versies van Kaspersky Security Center is het onmogelijk om de EDR / NDR (KATA)-functionaliteit te activeren.
- Het programma is geactiveerd en de functionaliteit valt onder de licentie.
- De onderdelen Endpoint Detection and Response (KATA) en Network Detection and Response (KATA) zijn ingeschakeld.

- Programmaonderdelen die zorgen voor de werking van EDR/NDR (KATA) zijn ingeschakeld en operationeel. De volgende onderdelen zorgen voor de werking van EDR / NDR (KATA):
  - File Threat Protection.
  - Web Threat Protection.
  - Mail Threat Protection.
  - Exploit-preventie.
  - Gedragsdetectie.
  - Host Intrusion Prevention.
  - AMSI-bescherming.
  - Achtergrondscan.
  - Kaspersky Security Network.



https://www.youtube.com/watch?v=cZzgtBoeC7k



https://www.youtube.com/watch?v=gd-rySv0ThQ

De integratie met Endpoint Detection and Response (KATA) omvat de volgende stappen:

1. **De onderdelen Endpoint Detection and Response (KATA) en Network Detection and Response (KATA) installeren**

   U kunt EDR (KATA) en NDR (KATA) onderdelen selecteren tijdens: installatie of upgrade, alsook tijdens het gebruik van de taak *Programmaonderdelen wijzigen*.

   U moet uw computer opnieuw opstarten om de upgrade van het programma met de nieuwe componenten te voltooien.

2. **Activeren van Endpoint Detection and Response (KATA) en Network Detection and Response (KATA)**

   U moet een afzonderlijke licentie kopen voor EDR (KATA) en NDR (KATA) (bijvoorbeeld, Kaspersky Endpoint Detection and Response (KATA) add-on).

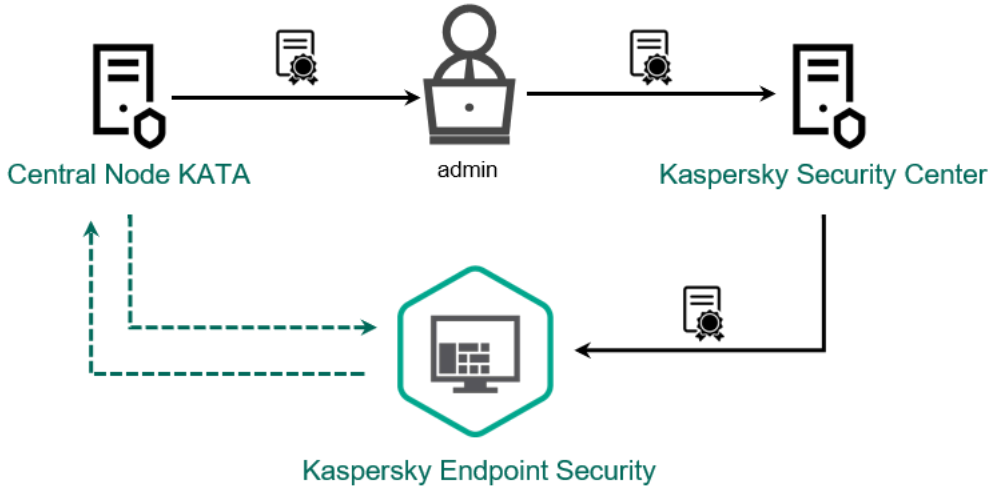
   De functionaliteit komt beschikbaar na het toevoegen van een aparte sleutel die EDR (KATA) en NDR (KATA) functionaliteit dekt. Als resultaat worden er verschillende sleutels op de computer toegevoegd: een sleutel voor Kaspersky Endpoint Security en sleutels voor Kaspersky Endpoint Detection and Response (KATA) en Network Detection and Response (KATA).

   Licenties voor de zelfstandige EDR (KATA) en NDR (KATA)-functionaliteit zijn hetzelfde als de licenties van Kaspersky Endpoint Security.

   Zorg ervoor dat zowel de EDR (KATA) als en de NDR (KATA)-functionaliteit is inbegrepen in de licentie en wordt uitgevoerd in de lokale interface van het programma.

3. **Verbinden met Central Node**

   Kaspersky Anti Targeted Attack Platform heeft een vertrouwde verbinding nodig tussen Kaspersky Endpoint Security en het onderdeel Central Node. Gebruik een TLS-certificaat om een vertrouwde verbinding te configureren. U kunt een TLS-certificaat verkrijgen in de Kaspersky Anti Targeted Attack Platform-console (zie de instructies in de Help van Kaspersky Anti Targeted Attack Platform). Vervolgens moet u het TLS-certificaat toevoegen aan Kaspersky Endpoint Security (zie onderstaande instructies).



Een TLS-certificaat toevoegen aan Kaspersky Endpoint Security

   Standaard controleert Kaspersky Endpoint Security alleen het TLS-certificaat van Central Node. Om de verbinding veiliger te maken, kunt u bovendien de verificatie van de computer op Central Node (twee-weg verificatie) inschakelen. Als u deze verificatie wilt inschakelen, moet u twee-weg verificatie inschakelen in de instellingen Central Node en Kaspersky Endpoint Security. Om twee-weg verificatie te gebruiken hebt u ook een crypto-container nodig. Een *crypto-container* is een PFX-archief met een certificaat en een privésleutel. U kunt een crypto-container verkrijgen in de Kaspersky Anti Targeted Attack Platform-console (zie de instructies in de Help van Kaspersky Anti Targeted Attack Platform).

Een Kaspersky Endpoint Security-computer verbinden met Central Node via de Beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de beheerconsole **Policies**.
3. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
4. Selecteer in het beleidsvenster **Detection and Response** en selecteer het onderdeel dat u wilt configureren: **Endpoint Detection and Response Expert (on-premises)** of **Network Detection and Response (KATA)**.
5. Selecteer het bijbehorende selectievakje: **Endpoint Detection and Response Expert (Versie 7.1 of ouder)** of **Network Detection and Response (KATA)**.
6. Klik op **Serververbindingsinstellingen**.
7. Configureer de serververbinding:
   - **Time-out (sec.)**. Maximale time-out voor de serverrespons van Central Node. Wanneer de time-out is verstreken, probeert Kaspersky Endpoint Security verbinding te maken met een andere Central Node-server.
   - **Server TLS certificaat**. TLS-certificaat voor het tot stand brengen van een vertrouwde verbinding met de Central Node-server. U kunt een TLS-certificaat verkrijgen in de Kaspersky Anti Targeted Attack Platform-console (zie de instructies in de Help van Kaspersky Anti Targeted Attack Platform).
   - **Gebruik twee-weg verificatie**. Tweerichtingsverificatie bij het tot stand brengen van een beveiligde verbinding tussen Kaspersky Endpoint Security en de Central Node-server. Om tweerichtingsverificatie te gebruiken, moet u tweerichtingsverificatie inschakelen in de Central Node-server instellingen, vervolgens een crypto-container ophalen en een wachtwoord instellen om de crypto-container te beschermen. Een *crypto-container* is een PFX-archief met een certificaat en een privésleutel. U kunt een crypto-container verkrijgen in de Kaspersky Anti Targeted Attack Platform-console (zie de instructies in de Help van Kaspersky Anti Targeted Attack Platform). Na het configureren van de Central Node-instellingen, moet u ook tweerichtingsverificatie inschakelen in de instellingen van Kaspersky Endpoint Security en een met een wachtwoord beveiligde crypto-container laden.

     De crypto-container moet met een wachtwoord worden beveiligd. Het is niet mogelijk om een crypto-container toe te voegen met een leeg wachtwoord.
8. Klik op **OK**.
9. Voeg central node-servers toe. Hiertoe geeft u het serveradres (IPv4, IPv6) en de poort op om verbinding te maken met de server.

   U kunt meerdere Central Node-serveradressen toevoegen. Kaspersky Endpoint Security probeert verbinding te maken met de server op het eerste IP-adres. Als er geen verbinding tot stand kan worden gebracht, probeert Kaspersky Endpoint Security verbinding te maken via het tweede IP-adres in de lijst, enzovoort.
10. Indien nodig, telemetrie configureren.
11. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Een Kaspersky Endpoint Security-computer verbinden met Central Node via de webconsole

1. Selecteer in het hoofdvenster van de Webconsole het tabblad **Asset management** → **Policies**.
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 de **Built-in Agents Configuration** sectie en selecteer het onderdeel dat u wilt configureren: **Endpoint Detection and Response Expert (on-premises)** of **Network Detection and Response (KATA)**.
5. Zet de bijbehorende schakelaar aan: **Endpoint Detection and Response Expert (on-premises) ENABLED** of **Network Detection and Response (KATA) ENABLED**.
6. Als u EDR (KATA) wilt configureren, selecteert u **Endpoint Detection and Response Expert (version 7.1 or earlier)** in de lijst met oplossingen.
7. Klik op **Connection settings**.
8. Configureer de serververbinding:

   - **Timeout (sec)**. Maximale time-out voor de serverrespons van Central Node. Wanneer de time-out is verstreken, probeert Kaspersky Endpoint Security verbinding te maken met een andere Central Node-server.
   - **Server certificate**. TLS-certificaat voor het tot stand brengen van een vertrouwde verbinding met de Central Node-server. U kunt een TLS-certificaat verkrijgen in de Kaspersky Anti Targeted Attack Platform-console (zie de instructies in de Help van Kaspersky Anti Targeted Attack Platform).
   - **Use two-way authentication**. Tweerichtingsverificatie bij het tot stand brengen van een beveiligde verbinding tussen Kaspersky Endpoint Security en de Central Node-server. Om tweerichtingsverificatie te gebruiken, moet u tweerichtingsverificatie inschakelen in de Central Node-server instellingen, vervolgens een crypto-container ophalen en een wachtwoord instellen om de crypto-container te beschermen. Een *crypto-container* is een PFX-archief met een certificaat en een privésleutel. U kunt een crypto-container verkrijgen in de Kaspersky Anti Targeted Attack Platform-console (zie de instructies in de Help van Kaspersky Anti Targeted Attack Platform). Na het configureren van de Central Node-instellingen, moet u ook tweerichtingsverificatie inschakelen in de instellingen van Kaspersky Endpoint Security en een met een wachtwoord beveiligde crypto-container laden.

     De crypto-container moet met een wachtwoord worden beveiligd. Het is niet mogelijk om een crypto-container toe te voegen met een leeg wachtwoord.
9. Klik op **OK**.
10. Voeg central node-servers toe. Hiertoe geeft u het serveradres (IPv4, IPv6) en de poort op om verbinding te maken met de server.

    U kunt meerdere Central Node-serveradressen toevoegen. Kaspersky Endpoint Security probeert verbinding te maken met de server op het eerste IP-adres. Als er geen verbinding tot stand kan worden gebracht, probeert Kaspersky Endpoint Security verbinding te maken via het tweede IP-adres in de lijst, enzovoort.

11. Indien nodig, telemetrie configureren.

12. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

U kunt ook lokaal een TLS-certificaat aan de computer toevoegen met behulp van de opdrachtregel.

Als resultaat wordt de computer toegevoegd aan de Kaspersky Anti Targeted Attack Platform-console. Controleer de werkingsstatus van de onderdelen door het *Report on status of application components* te bekijken. U kunt de werkingsstatus van de onderdelen ook in rapporten bekijken in de lokale interface van Kaspersky Endpoint Security. De onderdelen **Endpoint Detection and Response Expert (version 8.0 or later)** en **Network Detection and Response (KATA)** wordt toegevoegd aan de lijst met Kaspersky Endpoint Security-onderdelen.

U kunt de status van onderdelen in de Kaspersky Security Center console controleren in de eigenschappen van de computer in het **Components** sectie. Houd rekening met het volgende wanneer u de status van het onderdeel in de console controleert. Als het onderdeel niet is geïnstalleerd en de functionaliteit wordt niet gedekt door uw licentie, toont de console het volgende: **Not supported by license** status in plaats van **Not installed**.

Vanaf Kaspersky Endpoint Security 12.6 voor Windows kunt u de status van het EDR (KATA)-onderdeel controleren in de Kaspersky Security Center Beheerconsole (MMC). De huidige status van het onderdeel wordt weergegeven in computereigenschappen in de **Endpoint Sensor status** kolom (*Running*, *Starting*, *Stopped*, *Paused*, *Failed*, *Unknown*). De Webconsole geeft de status van de Endpoint Sensor niet weer.

EDR (KATA)-telemetrie configureren

Telemetrie is een lijst met gebeurtenissen die hebben plaatsgevonden op de beveiligde computer. Kaspersky Endpoint Security analyseert telemetriegegevens en verzendt deze tijdens de synchronisatie naar Kaspersky Anti Targeted Attack Platform. Telemetriegebeurtenissen komen bijna continu op de server aan. Kaspersky Endpoint Security start de synchronisatie met de server wanneer aan een van de volgende voorwaarden is voldaan:

- Het synchronisatie-interval is vervallen.
- Het aantal gebeurtenissen in de buffer overschrijdt de bovengrens.

Daarom synchroniseert het programma standaard elke 30 seconden of wanneer de buffer 1024 gebeurtenissen bevat. U kunt het synchronisatiegedrag configureren in het Kaspersky Endpoint Security-beleid en optimale waarden selecteren die overeenkomen met uw netwerkbelasting (zie onderstaande instructies).

Als er geen verbinding is tussen Kaspersky Endpoint Security en de server, plaatst het programma nieuwe gebeurtenissen in de wachtrij. Wanneer de verbinding hersteld is, stuurt Kaspersky Endpoint Security gebeurtenissen in de wachtrij in de juiste volgorde naar de server. Om overbelasting van de server te voorkomen, kan Kaspersky Endpoint Security bepaalde gebeurtenissen overslaan. Hiervoor kunt u de instellingen voor gebeurtenisoverdracht optimaliseren zoals een maximale waarde voor gebeurtenissen per uur (zie onderstaande instructies).

Als u Kaspersky Anti Targeted Attack Platform gebruikt in combinatie met een andere oplossing die ook telemetrie gebruikt, kunt u telemetrie voor KATA (EDR) uitschakelen (zie instructies beneden). Hiermee kunt u de serverbelasting voor deze oplossingen optimaliseren. Als u bijvoorbeeld de Managed Detection and Response-oplossing en KATA (EDR) hebt geïmplementeerd, kunt u MDR-telemetrie gebruiken en Threat Response-taken maken in KATA (EDR).

Telemetrie configureren in de Beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de beheerconsole **Policies**.
3. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
4. Selecteer in het beleidsvenster **Detection and Response** en selecteer het onderdeel dat u wilt configureren: **Endpoint Detection and Response Expert (on-premises)** of **Network Detection and Response (KATA)**.
5. Configureer de instelling **Stuur sync-verzoek naar KATA-server elke (min)**. Frequentie van synchronisatieverzoeken die naar de server worden verzonden. Tijdens de synchronisatie verzendt Kaspersky Endpoint Security informatie over gewijzigde programma-instellingen en -taken.
6. Zorg ervoor dat het selectievakje **Telemetrie versturen naar KATA** ingeschakeld is.
7. Configureer indien nodig de synchronisatie met de serverinstellingen in het blok **Data-overdrachtsinstellingen**:
   - **Maximale vertraging gebeurtenisoverdracht (sec)**. Het programma synchroniseert met de server om gebeurtenissen te verzenden nadat het synchronisatie-interval is verlopen. De standaardinstelling is 30 seconden.
   - **Maximum aantal evenementenpakketten**. Het programma synchroniseert met de server wanneer de buffer gevuld is met gebeurtenissen. De standaardinstelling is 1024 gebeurtenissen.
8. Schakel indien nodig het selectievakje in naast **Afremmen van verzoeken inschakelen** in het blok **Afremmen verzoeken**.

   Dit helpt de belasting op de server te optimaliseren. Als deze functionaliteit is ingeschakeld, beperkt het programma de verzending van gebeurtenissen. Als het aantal gebeurtenissen de ingestelde limieten overschrijdt, stopt Kaspersky Endpoint Security met het verzenden van gebeurtenissen.
9. Configureer optimalisatie-instellingen voor het verzenden van gebeurtenissen naar de server:
   - **Maximum aantal gebeurtenissen per uur**. Het programma analyseert de telemetriegegevensstroom en beperkt het verzenden van gebeurtenissen als de gebeurtenisstroom de geconfigureerde limiet voor gebeurtenissen per uur overschrijdt. Kaspersky Endpoint Security hervat het verzenden van gebeurtenissen na een uur. De standaardinstelling is 3000 gebeurtenissen per uur. Als het programma op een server is geïnstalleerd, is de telemetrie gegevensstroom hoger. Voor servers wordt aanbevolen om de waarde te verhogen tot 60 000 gebeurtenissen per uur.
   - **Percentage van de limietoverschrijding**. Het programma sorteert gebeurtenissen op type (bijvoorbeeld 'wijzigingen in het register'-gebeurtenissen) en beperkt de overdracht van gebeurtenissen als de verhouding tussen gebeurtenissen van hetzelfde type en het totale aantal gebeurtenissen de geconfigureerde limiet overschrijdt. Kaspersky Endpoint Security hervat het verzenden van gebeurtenissen wanneer de verhouding tussen andere gebeurtenissen en het totale aantal gebeurtenissen opnieuw groot genoeg is. De standaardinstelling is 15 %.
10. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Telemetrie configureren in de webconsole

1. Selecteer in het hoofdvenster van de Webconsole het tabblad **Asset management** → **Policies**.
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 **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (on-premises)**.

5. Als u EDR (KATA) wilt configureren, selecteert u **Endpoint Detection and Response Expert (version 7.1 or earlier)** in de lijst met oplossingen.

6. Zorg ervoor dat de **Send telemetry to KATA servers** selectievakje is ingeschakeld in het **Data transmission settings** blok.

7. Configureer de instelling **Send sync request to server every (min)**. Frequentie van synchronisatieverzoeken die naar de server worden verzonden. Tijdens de synchronisatie verzendt Kaspersky Endpoint Security informatie over gewijzigde programma-instellingen en -taken.

8. Zorg ervoor dat het selectievakje **Send telemetry to KATA servers** ingeschakeld is.

9. Configureer indien nodig de synchronisatie met de serverinstellingen in het blok **Data transmission settings**:

   - **Maximum event transmission delay (sec)**. Het programma synchroniseert met de server om gebeurtenissen te verzenden nadat het synchronisatie-interval is verlopen. De standaardinstelling is 30 seconden.

   - **Maximum number of event packages**. Het programma synchroniseert met de server wanneer de buffer gevuld is met gebeurtenissen. De standaardinstelling is 1024 gebeurtenissen.

10. Schakel indien nodig het selectievakje in naast **Enable request throttling** in het blok **Request throttling**.

    Dit helpt de belasting op de server te optimaliseren. Als deze functionaliteit is ingeschakeld, beperkt het programma de verzending van gebeurtenissen. Als het aantal gebeurtenissen de ingestelde limieten overschrijdt, stopt Kaspersky Endpoint Security met het verzenden van gebeurtenissen.

11. Configureer optimalisatie-instellingen voor het verzenden van gebeurtenissen naar de server:

    - **Maximum number of events per hour**. Het programma analyseert de telemetriegegevensstroom en beperkt het verzenden van gebeurtenissen als de gebeurtenisstroom de geconfigureerde limiet voor gebeurtenissen per uur overschrijdt. Kaspersky Endpoint Security hervat het verzenden van gebeurtenissen na een uur. De standaardinstelling is 3000 gebeurtenissen per uur. Als het programma op een server is geïnstalleerd, is de telemetrie gegevensstroom hoger. Voor servers wordt aanbevolen om de waarde te verhogen tot 60 000 gebeurtenissen per uur.

    - **Percentage of event limit excess**. Het programma sorteert gebeurtenissen op type (bijvoorbeeld 'wijzigingen in het register'-gebeurtenissen) en beperkt de overdracht van gebeurtenissen als de verhouding tussen gebeurtenissen van hetzelfde type en het totale aantal gebeurtenissen de geconfigureerde limiet overschrijdt. Kaspersky Endpoint Security hervat het verzenden van gebeurtenissen wanneer de verhouding tussen andere gebeurtenissen en het totale aantal gebeurtenissen opnieuw groot genoeg is. De standaardinstelling is 15 %.

12. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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 het gedeelte **KATA-integratie → Telemetrie uitsluitingen**.
5. Schakel onder **Data overdracht instellingen** het selectievakje in voor **Uitsluitingen gebruiken**.
6. Klik op **Toevoegen** en configureer de uitzonderingen:

   Criteria worden gecombineerd met de logische *AND*.

   - **Pad**. Volledig pad naar het bestand inclusief de naam en extensie. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de `*` en `?`-tekens bij het invoeren van een masker. Om de uitzondering te laten werken, moet het pad naar het bestand worden opgegeven.
   - **Opdrachtregel**. Opdracht gebruikt om het object uit te voeren.
   - **Beschrijving**. Waarde van de parameter FileDescription van een RT_VERSION bron (VersionInfo).

     Voor meer informatie over bron VersionInfo gaat u naar de website van Microsoft.
   - **Oorspronkelijke bestandsnaam**. Waarde van de parameter OriginalFilename van een RT_VERSION bron (VersionInfo).
   - **Versie**. Waarde van de parameter FileVersion van een RT_VERSION bron (VersionInfo).
   - **MD5**. MD5-hash van het bestand.
   - **SHA256**. SHA256-hash van het bestand.
   - **Type gebeurtenis**. Selecteer minstens één type gebeurtenis om de uitzondering te laten werken.
7. Sla uw wijzigingen op.

1. Selecteer **Tasks** in de structuur van de Beheerconsole van Kaspersky Security Center.

   De lijst met taken wordt geopend.
2. Klik op **New task**.

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

Stap 1. Een taaktype selecteren

1. Selecteer **Kaspersky Endpoint Security voor Windows 14.1. → Update terugdraaien**.

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 het taakschema bijvoorbeeld handmatig.

Stap 4. Taaknaam definiëren

Voer een naam voor de taak in.

Stap 7. Aanmaak van de taak voltooien

Verlaat de wizard verlaten. Schakel indien nodig het selectievakje **Run the task after the wizard finishes** in. U kunt de voortgang van de taak volgen in de taakeigenschappen.

EDR (KATA) telemetrie-uitzonderingen

Om de prestaties te verbeteren en de gegevensoverdracht naar de telemetrieserver te optimaliseren, kunt u uitzonderingen voor telemetrie configureren. U kunt er bijvoorbeeld voor kiezen om geen gegevens voor netwerkcommunicaties voor individuele programma's te verzenden.

Een telemetrie-uitzondering in de Beheerconsole (MMC) maken

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Algemene instellingen** → **Uitzonderingen en objecttypen** in het beleidsvenster.
4. In het blok **Telemetrie-instellingen** → **EDR (KATA) / NDR (KATA) telemetrie**, klikt u op de knop **Instellingen**.

5. Configureer in het geopende venster telemetrie-uitzonderingen (zie onderstaande tabel).

   Het programma combineert uitzonderingsvoorwaarden met de logische AND. Als u een regel wilt maken, moet u een waarde opgeven in de **Volledig pad** en selecteer ten minste één type gebeurtenis in het veld **Gebruik voor de volgende gebeurtenistypen** lijst.

6. Sla uw wijzigingen op.

Een telemetrie-uitzondering maken in de webconsole en de cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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** → **Telemetry Settings**.
5. Selecteer het tabblad **EDR (KATA) / NDR (KATA) telemetry**.
6. Configureer in het geopende venster telemetrie-uitzonderingen (zie onderstaande tabel).

   Het programma combineert uitzonderingsvoorwaarden met de logische AND. Als u een regel wilt maken, moet u een waarde opgeven in de **Full path** en selecteer ten minste één type gebeurtenis.

7. Sla uw wijzigingen op.

Parameter	Beschrijving
Uitgesloten processen	**Formaat van telemetrie optimaliseren voor verzending**. Met Kaspersky Endpoint Security kunt u de hoeveelheid verzonden gegevens optimaliseren en gebeurtenissen met bepaalde codes uitsluiten van telemetrie: code 102 (basiscommunicatie) en 8 (netwerkactiviteit van het proces) voor het Microsoft SMB-protocol, de WinRM-service en het klnagent.exe-proces van de Netwerkagent, evenals uitgebreide informatie over de soorten netwerkpakketten voor alle soorten netwerkprotocollen. Kaspersky Endpoint Security combineert activeringscriteria van regel met een logische EN. **Process** en **Parent process**: • **Full path**. Volledig pad naar het bestand inclusief de naam en extensie. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de `*` en `?`-tekens bij het invoeren van een masker. • **Command line text**. Opdracht gebruikt om het bestand uit te voeren. • **Description**. Waarde van de parameter FileDescription van een RT_VERSION bron (VersionInfo). • **Original file name**. Waarde van de parameter OriginalFilename van een RT_VERSION bron (VersionInfo). • **Version**. Waarde van de parameter FileVersion van een RT_VERSION bron (VersionInfo). • **File checksums**. MD5 en SHA256. U kunt ook handmatig een bestand selecteren, waarna het programma automatisch de velden van het geselecteerde bestand invult. In 64-bits besturingssystemen moet u de parameters van de 64-bits versie van het uitvoerbare bestand van een proces uit de map `C:\windows\system32` handmatig invoeren, omdat het programma de parametervelden van het uitvoerbare bestand vult met gegevens uit de eigenschappen van de 32-bits versie van hetzelfde uitvoerbare bestand in de map `C:\windows\syswow64`. Als u bijvoorbeeld `C:\windows\system32\cmd.exe` selecteert, geeft de plug-in de parameters van `C:\windows\syswow64\cmd.exe` weer. Dergelijk gedrag wordt gedicteerd door eigenaardigheden van het besturingssysteem. **Gebruik voor de volgende gebeurtenistypen** • **Bestandswijziging**. • **Netwerk gebeurtenissen**. • **Proces: console interactieve invoer**. • **Module laden**. • **Register gewijzigd**. • **DNS-logboeken**. • **Procestoegang**. • **Code-injectie**. • **WMI-query**. • **Pipe**. • **LDAP**. • **AMSI**.
Uitgesloten netwerkcommunicaties	**Regelnaam**. **Richting**. **Protocol**. **Raw socket**. **Protocolnummer**. **TLS-certificaat**. **Lokale poort of bereik**. **Externe poort of bereik**. **Lokaal adres**. Het netwerkadres van de computer waarvoor Kaspersky Endpoint Security telemetrie uitsluit van netwerkverkeer. **Extern adres**. Het netwerkadres van de computer waarvoor Kaspersky Endpoint Security telemetrie uitsluit van netwerkverkeer. Alleen het IPv4-formaat wordt ondersteund voor IP-adressen. **Programma's**. Lijst met uitvoerbare bestanden van programma's waarvoor Kaspersky Endpoint Security EDR-telemetrie uitsluit van netwerkverkeer.

Parameter	Beschrijving
Uitgesloten bestandsbewerkingen	**Regelnaam**. **Bestandsnaam of masker**. Naam of masker van een bestand of map; Kaspersky Endpoint Security past de uitzonderingsregel toe wanneer dit bestand of deze map wordt geopend. Kaspersky Endpoint Security biedt geen ondersteuning voor de tekens `*` en `?` bij de invoer van een masker. **Bewerkingstype**. **Vorig pad**. Kaspersky Endpoint Security combineert activeringscriteria van regel met een logische EN. **Process** en **Parent process**: • **Full path**. Volledig pad naar het bestand inclusief de naam en extensie. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de `*` en `?`-tekens bij het invoeren van een masker. • **Command line text**. Opdracht gebruikt om het bestand uit te voeren. • **Description**. Waarde van de parameter FileDescription van een RT_VERSION bron (VersionInfo). • **Original file name**. Waarde van de parameter OriginalFilename van een RT_VERSION bron (VersionInfo). • **Version**. Waarde van de parameter FileVersion van een RT_VERSION bron (VersionInfo). • **File checksums**. MD5 en SHA256. U kunt ook handmatig een bestand selecteren, waarna het programma automatisch de velden van het geselecteerde bestand invult. In 64-bits besturingssystemen moet u de parameters van de 64-bits versie van het uitvoerbare bestand van een proces uit de map `C:\windows\system32` handmatig invoeren, omdat het programma de parametervelden van het uitvoerbare bestand vult met gegevens uit de eigenschappen van de 32-bits versie van hetzelfde uitvoerbare bestand in de map `C:\windows\syswow64`. Als u bijvoorbeeld `C:\windows\system32\cmd.exe` selecteert, geeft de plug-in de parameters van `C:\windows\syswow64\cmd.exe` weer. Dergelijk gedrag wordt gedicteerd door eigenaardigheden van het besturingssysteem.
Uitgesloten DNS-bewerkingen	**Regelnaam**. Kaspersky Endpoint Security combineert activeringscriteria van regel met een logische EN. **Process** en **Parent process**: • **Full path**. Volledig pad naar het bestand inclusief de naam en extensie. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de `*` en `?`-tekens bij het invoeren van een masker. • **Command line text**. Opdracht gebruikt om het bestand uit te voeren. • **Description**. Waarde van de parameter FileDescription van een RT_VERSION bron (VersionInfo). • **Original file name**. Waarde van de parameter OriginalFilename van een RT_VERSION bron (VersionInfo). • **Version**. Waarde van de parameter FileVersion van een RT_VERSION bron (VersionInfo). • **File checksums**. MD5 en SHA256. U kunt ook handmatig een bestand selecteren, waarna het programma automatisch de velden van het geselecteerde bestand invult. In 64-bits besturingssystemen moet u de parameters van de 64-bits versie van het uitvoerbare bestand van een proces uit de map `C:\windows\system32` handmatig invoeren, omdat het programma de parametervelden van het uitvoerbare bestand vult met gegevens uit de eigenschappen van de 32-bits versie van hetzelfde uitvoerbare bestand in de map `C:\windows\syswow64`. Als u bijvoorbeeld `C:\windows\system32\cmd.exe` selecteert, geeft de plug-in de parameters van `C:\windows\syswow64\cmd.exe` weer. Dergelijk gedrag wordt gedicteerd door eigenaardigheden van het besturingssysteem. **DNS** • **IP-adres DNS-server**. • **Query opties**. • **Status**. • **Domeinnaam**. • **Instellingen type ID**. • **Response data**.

Parameter	Beschrijving
Uitgesloten LDAP-bewerkingen	**Regelnaam**. **LDAP Zoekbereik**. **Filter**. **Onderscheidende naam voor het zoeken naar LDAP-objecten**. **Objectkenmerken**. Kaspersky Endpoint Security combineert activeringscriteria van regel met een logische EN. **Process** en **Parent process**: • **Full path**. Volledig pad naar het bestand inclusief de naam en extensie. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de `*` en `?`-tekens bij het invoeren van een masker. • **Command line text**. Opdracht gebruikt om het bestand uit te voeren. • **Description**. Waarde van de parameter FileDescription van een RT_VERSION bron (VersionInfo). • **Original file name**. Waarde van de parameter OriginalFilename van een RT_VERSION bron (VersionInfo). • **Version**. Waarde van de parameter FileVersion van een RT_VERSION bron (VersionInfo). • **File checksums**. MD5 en SHA256. U kunt ook handmatig een bestand selecteren, waarna het programma automatisch de velden van het geselecteerde bestand invult. In 64-bits besturingssystemen moet u de parameters van de 64-bits versie van het uitvoerbare bestand van een proces uit de map `C:\windows\system32` handmatig invoeren, omdat het programma de parametervelden van het uitvoerbare bestand vult met gegevens uit de eigenschappen van de 32-bits versie van hetzelfde uitvoerbare bestand in de map `C:\windows\syswow64`. Als u bijvoorbeeld `C:\windows\system32\cmd.exe` selecteert, geeft de plug-in de parameters van `C:\windows\syswow64\cmd.exe` weer. Dergelijk gedrag wordt gedicteerd door eigenaardigheden van het besturingssysteem.
Uitgesloten verzoeken voor procestoegang	**Regelnaam**. **Bewerkingstype**. **Toegang tot het proces aangevraagd**. **Stack trace oproepen**. Kaspersky Endpoint Security combineert activeringscriteria van regel met een logische EN. **Process**, **Parent process**, **File of the target process**, **Handle to the source process** en **Handle to the target process**. • **Volledig pad**. Volledig pad naar het bestand inclusief de naam en extensie. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de `*` en `?`-tekens bij het invoeren van een masker. • **Opdrachtregeltekst**. Opdracht gebruikt om het bestand uit te voeren. • **Geef de criteria voor het activeren van regels op en de gebeurtenistypen waarvoor u deze regel wilt gebruiken**. Waarde van de parameter FileDescription van een RT_VERSION bron (VersionInfo). • **Oorspronkelijke bestandsnaam**. Waarde van de parameter OriginalFilename van een RT_VERSION bron (VersionInfo). • **Versie**. Waarde van de parameter FileVersion van een RT_VERSION bron (VersionInfo). • **Bestands-controlesommen**. MD5 en SHA256. U kunt ook handmatig een bestand selecteren, waarna het programma automatisch de velden van het geselecteerde bestand invult. In 64-bits besturingssystemen moet u de parameters van de 64-bits versie van het uitvoerbare bestand van een proces uit de map `C:\windows\system32` handmatig invoeren, omdat het programma de parametervelden van het uitvoerbare bestand vult met gegevens uit de eigenschappen van de 32-bits versie van hetzelfde uitvoerbare bestand in de map `C:\windows\syswow64`. Als u bijvoorbeeld `C:\windows\system32\cmd.exe` selecteert, geeft de plug-in de parameters van `C:\windows\syswow64\cmd.exe` weer. Dergelijk gedrag wordt gedicteerd door eigenaardigheden van het besturingssysteem.

Parameter	Beschrijving
Uitgesloten code-injecties	**Regelnaam**. **Toegangsmethode**. **Stack oproepen**. **Gewijzigde opdrachtregel**. **Injectieadres**. **Geïnjecteerde DLL-naam**. Kaspersky Endpoint Security combineert activeringscriteria van regel met een logische EN. **Process** en **Parent process**: • **Full path**. Volledig pad naar het bestand inclusief de naam en extensie. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de `*` en `?`-tekens bij het invoeren van een masker. • **Command line text**. Opdracht gebruikt om het bestand uit te voeren. • **Description**. Waarde van de parameter FileDescription van een RT_VERSION bron (VersionInfo). • **Original file name**. Waarde van de parameter OriginalFilename van een RT_VERSION bron (VersionInfo). • **Version**. Waarde van de parameter FileVersion van een RT_VERSION bron (VersionInfo). • **File checksums**. MD5 en SHA256. U kunt ook handmatig een bestand selecteren, waarna het programma automatisch de velden van het geselecteerde bestand invult. In 64-bits besturingssystemen moet u de parameters van de 64-bits versie van het uitvoerbare bestand van een proces uit de map `C:\windows\system32` handmatig invoeren, omdat het programma de parametervelden van het uitvoerbare bestand vult met gegevens uit de eigenschappen van de 32-bits versie van hetzelfde uitvoerbare bestand in de map `C:\windows\syswow64`. Als u bijvoorbeeld `C:\windows\system32\cmd.exe` selecteert, geeft de plug-in de parameters van `C:\windows\syswow64\cmd.exe` weer. Dergelijk gedrag wordt gedicteerd door eigenaardigheden van het besturingssysteem.

Parameter	Beschrijving
Uitgesloten WMI-verzoeken	**Regelnaam**. **WMI-bewerkingstype**. **Query op afstand**. **Naam van een computer die een WMI-opdracht heeft uitgevoerd**. **WMI gebruikersaccount**. **Uitgevoerd WMI-opdracht**. **WMI-naamruimte**. **WMI-gebeurtenis consumentfilter**. **Naam van de gemaakte WMI-gebeurtenisconsument**. **Broncode van een WMI-gebeurtenisconsument**. Kaspersky Endpoint Security combineert activeringscriteria van regel met een logische EN. **Process** en **Parent process**: • **Full path**. Volledig pad naar het bestand inclusief de naam en extensie. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de `*` en `?`-tekens bij het invoeren van een masker. • **Command line text**. Opdracht gebruikt om het bestand uit te voeren. • **Description**. Waarde van de parameter FileDescription van een RT_VERSION bron (VersionInfo). • **Original file name**. Waarde van de parameter OriginalFilename van een RT_VERSION bron (VersionInfo). • **Version**. Waarde van de parameter FileVersion van een RT_VERSION bron (VersionInfo). • **File checksums**. MD5 en SHA256. U kunt ook handmatig een bestand selecteren, waarna het programma automatisch de velden van het geselecteerde bestand invult. In 64-bits besturingssystemen moet u de parameters van de 64-bits versie van het uitvoerbare bestand van een proces uit de map `C:\windows\system32` handmatig invoeren, omdat het programma de parametervelden van het uitvoerbare bestand vult met gegevens uit de eigenschappen van de 32-bits versie van hetzelfde uitvoerbare bestand in de map `C:\windows\syswow64`. Als u bijvoorbeeld `C:\windows\system32\cmd.exe` selecteert, geeft de plug-in de parameters van `C:\windows\syswow64\cmd.exe` weer. Dergelijk gedrag wordt gedicteerd door eigenaardigheden van het besturingssysteem.
Uitgesloten pijpbewerkingen	**Regelnaam**. **Naam van pipe**. **Bewerkingstype**. Kaspersky Endpoint Security combineert activeringscriteria van regel met een logische EN. **Process** en **Parent process**: • **Full path**. Volledig pad naar het bestand inclusief de naam en extensie. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de `*` en `?`-tekens bij het invoeren van een masker. • **Command line text**. Opdracht gebruikt om het bestand uit te voeren. • **Description**. Waarde van de parameter FileDescription van een RT_VERSION bron (VersionInfo). • **Original file name**. Waarde van de parameter OriginalFilename van een RT_VERSION bron (VersionInfo). • **Version**. Waarde van de parameter FileVersion van een RT_VERSION bron (VersionInfo). • **File checksums**. MD5 en SHA256. U kunt ook handmatig een bestand selecteren, waarna het programma automatisch de velden van het geselecteerde bestand invult. In 64-bits besturingssystemen moet u de parameters van de 64-bits versie van het uitvoerbare bestand van een proces uit de map `C:\windows\system32` handmatig invoeren, omdat het programma de parametervelden van het uitvoerbare bestand vult met gegevens uit de eigenschappen van de 32-bits versie van hetzelfde uitvoerbare bestand in de map `C:\windows\syswow64`. Als u bijvoorbeeld `C:\windows\system32\cmd.exe` selecteert, geeft de plug-in de parameters van `C:\windows\syswow64\cmd.exe` weer. Dergelijk gedrag wordt gedicteerd door eigenaardigheden van het besturingssysteem.

Parameter	Beschrijving
Registerwijzigingen uitsluiten	**Regelnaam**. **Bewerkingstype**. **Pad**. **Naam van waarde**. **Waarde**. **Volledige naam van een registerbestand**. Kaspersky Endpoint Security combineert activeringscriteria van regel met een logische EN. **Process** en **Parent process**: • **Full path**. Volledig pad naar het bestand inclusief de naam en extensie. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de `*` en `?`-tekens bij het invoeren van een masker. • **Command line text**. Opdracht gebruikt om het bestand uit te voeren. • **Description**. Waarde van de parameter FileDescription van een RT_VERSION bron (VersionInfo). • **Original file name**. Waarde van de parameter OriginalFilename van een RT_VERSION bron (VersionInfo). • **Version**. Waarde van de parameter FileVersion van een RT_VERSION bron (VersionInfo). • **File checksums**. MD5 en SHA256. U kunt ook handmatig een bestand selecteren, waarna het programma automatisch de velden van het geselecteerde bestand invult. In 64-bits besturingssystemen moet u de parameters van de 64-bits versie van het uitvoerbare bestand van een proces uit de map `C:\windows\system32` handmatig invoeren, omdat het programma de parametervelden van het uitvoerbare bestand vult met gegevens uit de eigenschappen van de 32-bits versie van hetzelfde uitvoerbare bestand in de map `C:\windows\syswow64`. Als u bijvoorbeeld `C:\windows\system32\cmd.exe` selecteert, geeft de plug-in de parameters van `C:\windows\syswow64\cmd.exe` weer. Dergelijk gedrag wordt gedicteerd door eigenaardigheden van het besturingssysteem.
Uitgesloten bewerkingen met apparaten	**Regelnaam**. **Apparaattype**. **Apparaat-ID**. **Apparaatnaam**.

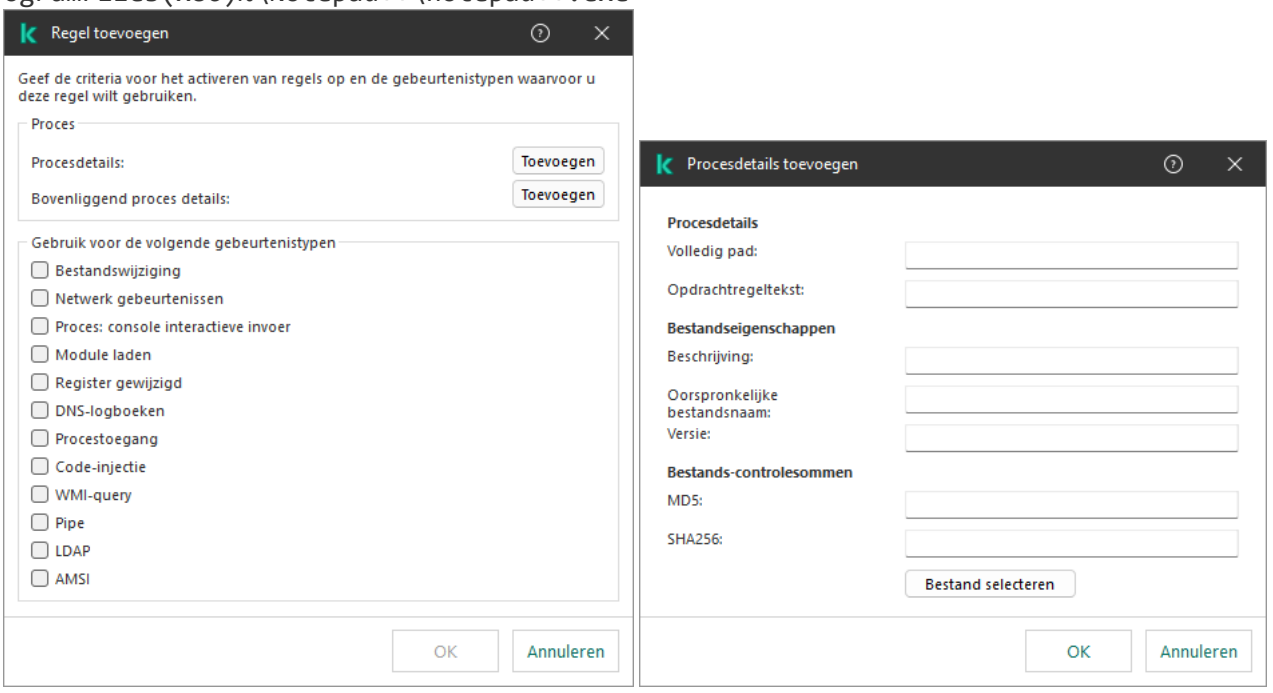
Voorbeeld 1. Uitgesloten processen

Als u gebeurtenissen van programma's (proces) van derden wilt uitsluiten van telemetrie, het venster Uitzonderingen voor EDR-telemetrie openen op de **Uitgesloten processen** en voeg het uitvoerbare bestand van het programma toe.

Kaspersky Endpoint Security combineert activeringscriteria van regel met een logische EN.

Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de `*` en `?`-tekens bij het invoeren van een masker. Bijvoorbeeld:

- `C:\Program Files\*\notepad++.exe`
- `%ProgramFiles(x86)%\Notepad++\notepad++.exe`



Een proces uitsluiten

Voorbeeld 1. Bestandswijziging

Als u vaak scripts bewerkt in het Notepad++-programma en u de wijzigingsgebeurtenissen voor de overeenkomstige scripts wilt uitsluiten, voeg de Notepad++ uitvoerbaar bestand naar telemetrie-uitzonderingen.

Geef de instellingen als volgt op:

- **Volledig pad**: `C:\Program Files\Notepad++\notepad++.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.
- **Gebruik voor de volgende gebeurtenistypen**: Bestandswijziging.

Voorbeeld 2. Netwerkgebeurtenissen

Als u het WinSCP-programma gebruikt om bestanden op een externe server te beheren en u netwerkgebeurtenissen wilt uitsluiten, voeg het uitvoerbare WinSCP-bestand toe aan de telemetrie-uitzonderingen.

Geef de instellingen als volgt op:

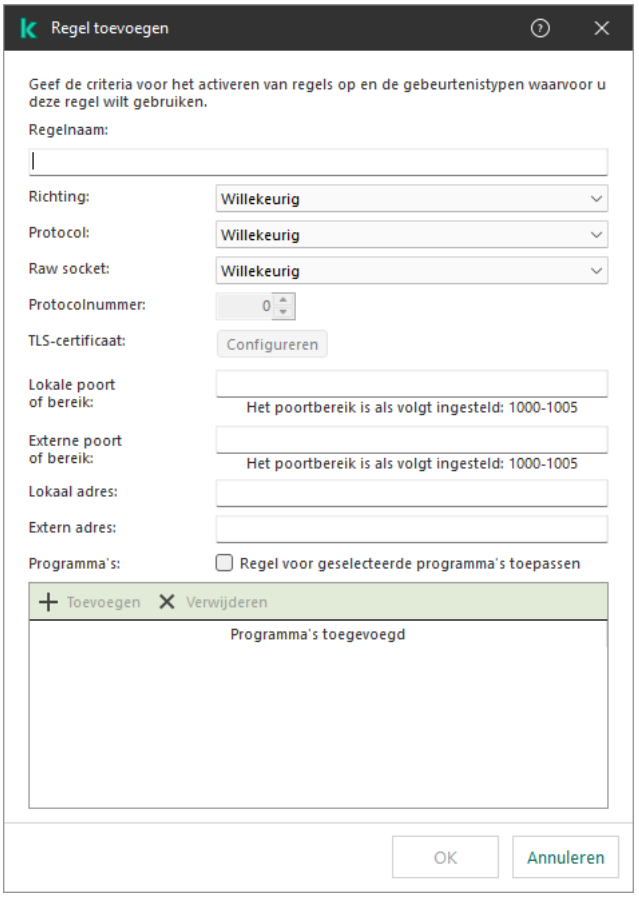
- **Volledig pad**: `C:\Program Files (x86)\WinSCP\WinSCP.exe`.
- **SHA256**: 47204338f0e092057024c9186f228c02417e917777f3e841d52b58251a956a74 (optioneel).
- **Gebruik voor de volgende gebeurtenistypen**: Netwerk gebeurtenissen.

Voorbeeld 2. Uitgesloten netwerkcommunicaties

Als u verbindingsgebeurtenissen van externe services wilt uitsluiten van telemetrie, het venster Uitzonderingen voor EDR-telemetrie openen op de **Uitgesloten netwerkcommunicaties** en voeg verbindingsinstellingen toe: protocol, poort, richting, IP-adres, TLS-certificaat en andere.

Kaspersky Endpoint Security combineert activeringscriteria van regel met een logische EN.

U kunt geen subnetadres opgeven (bijvoorbeeld 10.28.0.0/24). Het programma staat het opgeven van slechts één IP-adres toe (bijvoorbeeld 10.28.0.105).



Uitzondering voor netwerkcommunicatie

Als u een zakelijke webserver gebruikt en u wilt browsergebeurtenissen uitsluiten wanneer u verbinding maakt met die webserver, voeg dan het IP-adres van de riool en het uitvoerbare bestand van de browser toe aan de telemetrie-uitzonderingen.

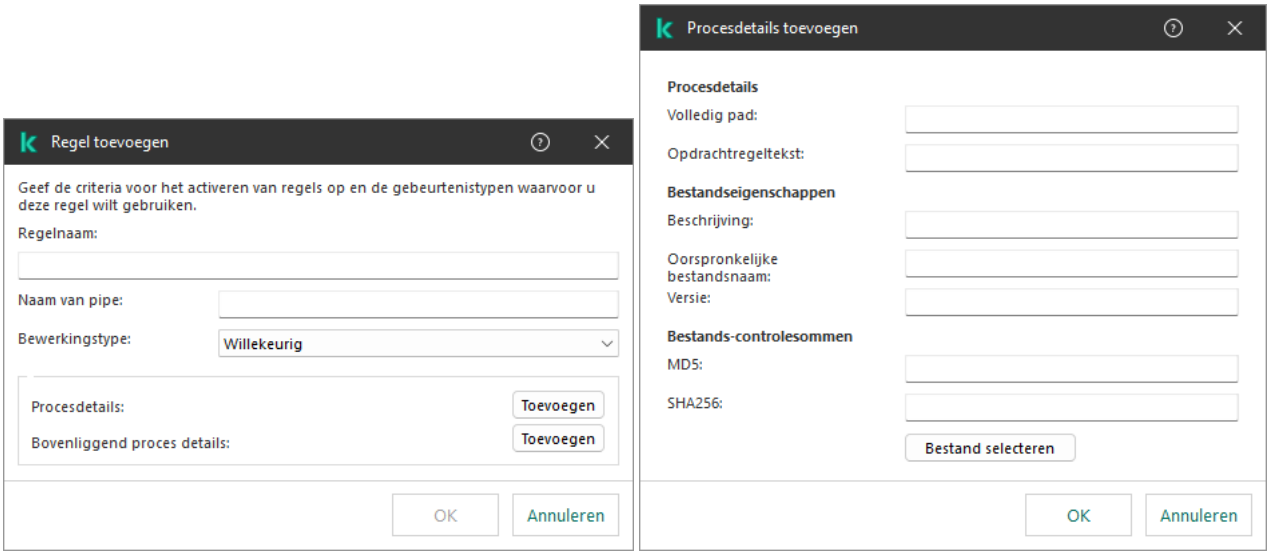
Geef de instellingen als volgt op:

- **Protocol**: TCP.
- **Externe poort of bereik**: 443.
- **Extern adres**: 10.28.0.105.
- **Programma's**: `C:\Program Files (x86)\Google\Chrome\Application\chrome.exe`; `C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe`.

Voorbeeld 3. Uitgesloten bestandsbewerkingen

Als u gebeurtenissen met betrekking tot bewerkingen met vertrouwde bestanden wilt uitsluiten van telemetrie, het venster Uitzonderingen voor EDR-telemetrie openen op de **Uitgesloten bestandsbewerkingen** en voeg het vertrouwde bestand toe.

Kaspersky Endpoint Security combineert activeringscriteria van regel met een logische EN.



Bestandsbewerkingen uitsluiten

Als een programma naar een logboek schrijft en u wijzigingen in het logboekbestand wilt uitsluiten, voeg het logboekbestand en het uitvoerbare bestand van het programma toe vanuit telemetrie.

Geef de instellingen als volgt op:

- **Bestandsnaam of masker**: `C:\Apache24\logs\error.log`.
- **Bewerkingstype**: Bestandswijziging.
- **Volledig pad**: `C:\Apache24\bin\httpd.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.

Voorbeeld 4. Uitgesloten registerwijzigingen

Als u gebeurtenissen van registerwijzigingen wilt uitsluiten van telemetrie, het venster Uitzonderingen voor EDR-telemetrie openen op de **Registerwijzigingen uitsluiten** tabblad en voeg een registersleutel toe.

Kaspersky Endpoint Security combineert activeringscriteria van regel met een logische EN.

Als een programma regelmatig de registerwaarden wijzigt en u deze wijzigingen in het register wilt uitsluiten van telemetrie, voegt u de registersleutel en het uitvoerbare bestand van het programma toe aan de telemetrie-uitzonderingen.

Geef de instellingen als volgt op:

- **Bewerkingstype**: Wijzigen.
- **Pad**: HKEY_LOCAL_MACHINE\SOFTWARE\SimonTatham\PuTTY64.
- **Volledig pad**: `C:\Program Files\PuTTY\putty.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.

KATA Sandbox

Kaspersky Anti Targeted Attack Platform bevat het onderdeel Sandbox (KATA Sandbox). *Sandbox* is een technologie waarmee u geavanceerde bedreigingen op een computer kunt detecteren. Sandbox analyseert het gedrag van objecten om schadelijke activiteit en activiteit kenmerkend voor doelgerichte aanvallen op de IT-infrastructuur van het bedrijf te detecteren. Sandbox analyseert en scant objecten op speciale servers met geïmplementeerde virtuele kopieën van Microsoft Windows-besturingssystemen (Sandbox-servers). Voor informatie over de oplossing raadpleegt u de Help van Kaspersky Anti Targeted Attack Platform.

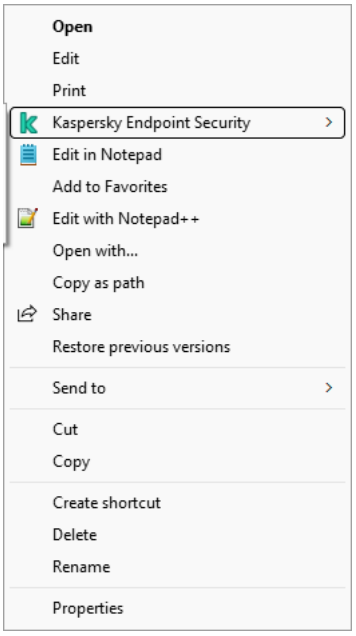
Om KATA Sandbox te activeren, hebt u een licentiesleutel nodig die KATA- of KEDR-functionaliteit omvat. Voor informatie over de beschikbare oplossingen raadpleegt u de Help van Kaspersky Anti Targeted Attack Platform.

KATA Sandbox staat het scannen van bestanden toe in de volgende modussen:

- *Handmatig*. De gebruiker stuurt het bestand handmatig in voor scannen vanuit het contextmenu (**Verzenden naar Sandbox**). Wanneer een bestand naar Sandbox wordt gestuurd, scant het programma het bestand ook met behulp van antivirusdatabases.
- *Automatisch*. Het programma detecteert automatisch objecten en stuurt ze in naar Sandbox om ze te scannen.

Nadat het bestand naar Sandbox is verzonden, blijft het bestand toegankelijk voor de gebruiker. Kaspersky Endpoint Security registreert de bijbehorende gebeurtenis en stuurt de gebeurtenis naar Kaspersky Security Center en de Kaspersky Anti Targeted Attack Platform-console. Als Sandbox kwaadaardige activiteit detecteert, voert Kaspersky Endpoint Security een Thread Response automatisch (het verwijdert bijvoorbeeld het object en start een scan van kritieke gebieden).

Om KATA Sandbox in de handmatige modus te laten werken, moet Kaspersky Anti Targeted Attack Platform 7.0 of hoger zijn geïmplementeerd. Om KATA Sandbox in de automatische modus te laten werken, moet Kaspersky Anti Targeted Attack Platform 8.0 of hoger zijn geïmplementeerd.



Scannen in KATA Sandbox vanuit het contextmenu

Integratie van de ingebouwde agent met KATA Sandbox

Het toevoegen van het onderdeel Sandbox is vereist voor integratie met KATA Sandbox. U kunt het Sandbox-component selecteren tijdens: installatie of upgrade, alsook tijdens het gebruik van de taak *Programmaonderdelen wijzigen*.

Om bestanden voor scannen te verzenden, moet u de integratie met KATA Sandbox inschakelen en een Central Node-server toevoegen die in de oplossing wordt geïmplementeerd. Het onderdeel kan alleen worden beheerd met behulp van de Kaspersky Security Center-webconsole. U kunt dit onderdeel niet beheren met de Beheerconsole (MMC).

De integratie met KATA Sandbox in- of uitschakelen:

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Built-in Agents Configuration** → **Sandbox**.
5. Gebruik de schakelaar **Integration with Sandbox ENABLED** om de component in of uit te schakelen.

6. Selecteer de KATA Sandbox-uitvoermodus:

   - **Manually**. De gebruiker stuurt het bestand handmatig in voor scannen vanuit het contextmenu (**Verzenden naar Sandbox**).

   - **Automatically**. Het programma detecteert automatisch objecten en stuurt ze in naar Sandbox om ze te scannen.

   - **Combined**.

7. Klik op de koppeling **Connection settings**.

8. Configureer de verbindingsinstellingen van de Central Node-server:

   - **Timeout (msec)**. Verbindingstime-out voor de Central Node-server. Nadat de geconfigureerde time-out is verstreken, stuurt Kaspersky Endpoint Security een verzoek naar de volgende server. U kunt de verbindingstime-out voor de server verlengen als uw verbindingssnelheid laag is of als de verbinding onstabiel is. De aanbevolen timeout voor een aanvraag is 0,5 seconden of minder.

   - **Request queue**. Grootte van de verzoekwachtrijmap. Bij het verzenden van meerdere objecten om te scannen in Sandbox, maakt Kaspersky Endpoint Security een wachtrij voor aanvragen. Standaard is de grootte van de verzoekwachtrijmap beperkt tot 100 MB. Nadat de maximale grootte is bereikt, stopt 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.

   - **Server TLS certificate**. Om een vertrouwde verbinding met de Central Node-server te configureren, moet u een TLS-certificaat voorbereiden. Vervolgens moet u het certificaat met behulp van een beleid aan de computer toevoegen. U moet het certificaat ook toevoegen aan de Central Node-server.

   - **Use two-way authentication**. Tweerichtingsverificatie bij het tot stand brengen van een beveiligde verbinding tussen Kaspersky Endpoint Security en de Central Node-server. Om tweerichtingsverificatie te gebruiken, moet u tweerichtingsverificatie inschakelen in de Central Node-server instellingen, vervolgens een crypto-container ophalen en een wachtwoord instellen om de crypto-container te beschermen. Een *crypto-container* is een PFX-archief met een certificaat en een privésleutel. U kunt een crypto-container verkrijgen in de Kaspersky Anti Targeted Attack Platform-console (zie de instructies in de Help van Kaspersky Anti Targeted Attack Platform). Na het configureren van de Central Node-instellingen, moet u ook tweerichtingsverificatie inschakelen in de instellingen van Kaspersky Endpoint Security en een met een wachtwoord beveiligde crypto-container laden.

9. In het blok **Connection to Sandbox servers**, klikt u op de knop **Add**.

10. Dit opent een venster; voer in dat venster het Central Node-serveradres (IPv4, IPv6, DNS) en de poort in.

    Raadpleeg de Help van Kaspersky Anti Targeted Attack Platform voor meer informatie over het implementeren van virtuele images en het configureren van Central Node-servers.

11. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Het onderdeel Sandbox wordt hierdoor ingeschakeld. Controleer de werkingsstatus van het onderdeel door het *Report on status of application components* te bekijken. U kunt de werkingsstatus van een onderdeel ook in rapporten bekijken in de lokale interface van Kaspersky Endpoint Security. Het onderdeel **Sandbox** wordt toegevoegd aan de lijst met Kaspersky Endpoint Security-onderdelen.

Threat Response-acties configureren

Als Sandbox schadelijke activiteiten detecteert, voert Kaspersky Endpoint Security automatisch een Threat Response-actie uit (het verwijdert bijvoorbeeld het object en start een scan van kritieke gebieden).

Threat Response-acties configureren:

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Built-in Agents Configuration** → **Sandbox**.
5. Selecteer de relevante actie in het blok **Action on threat detection**:

   - **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 Critical Areas Scan**. Als deze optie is geselecteerd, start Kaspersky Endpoint Security de taak *Critical Areas Scan*. Standaard scant Kaspersky Endpoint Security het kernelgeheugen, actieve processen en de opstartsectoren van de schijf.
   - **Create IOC Scan task**. Als deze optie is geselecteerd, maakt Kaspersky Endpoint Security automatisch de *IOC Scan (autonome IOC-scantaak)*. Voor deze taak kunt u de uitvoermodus, het scanbereik en de actie voor IOC-detectie configureren (*Move copy to Quarantine, delete object* of *Run Critical Areas Scan*). Om andere instellingen van de *IOC Scan* taak te wijzigen, gaat u naar de taakinstellingen.
6. Configureer indien nodig de instelling *IOC-scan* taakinstellingen in het blok **IOC Scan scope**.

   - **Critical file areas**. Als deze optie geselecteerd is, voert Kaspersky Endpoint Security alleen een IOC-scan uit in kritieke bestandsgebieden van de computer: kernelgeheugen en opstartsectoren.
   - **File areas on system drive of the computer**. Als deze optie geselecteerd is, voert Kaspersky Endpoint Security een IOC-scan uit op het systeemstation van de computer.
7. Configureer indien nodig de instelling *IOC-scan* taakinstellingen in het blok **Run IOC Scan task**.

   - **Manually**. Uitvoeringsmodus waarin u de *IOC Scan* handmatig kunt starten op een moment dat u uitkomt.
   - **Automatically**. Uitvoermodus waarin Kaspersky Endpoint Security de *IOC Scan* taak automatisch wordt uitgevoerd nadat een dreiging wordt gedetecteerd.
   - **Run only when the computer is idle**. Uitvoermodus waarin Kaspersky Endpoint Security de *IOC-scan* taak uitvoert als de screensaver actief is of het scherm wordt vergrendeld. Als de gebruiker de computer ontgrendelt, pauzeert Kaspersky Endpoint Security de scantaak. Dit betekent dat de taak enkele dagen in beslag kan nemen.

8. Geavanceerde taakinstellingen configureren voor: *IOC-scan*.

9. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Migratiegids van KEA naar KES voor EDR (KATA)

Vanaf versie 12.1 bevat Kaspersky Endpoint Security voor Windows nu een ingebouwde agent voor het beheer van de Kaspersky Endpoint Detection and Response-component als onderdeel van de Kaspersky Anti Targeted Attack Platform-oplossing. U hebt geen apart Kaspersky Endpoint Agent-programma meer nodig om met EDR (KATA) te werken. Alle functies van Kaspersky Endpoint Agent worden uitgevoerd door Kaspersky Endpoint Security. De belasting op Kaspersky Anti Targeted Attack Platform-servers blijft hetzelfde.

Wanneer u Kaspersky Endpoint Security implementeert op computers waarop Kaspersky Endpoint Agent is geïnstalleerd, blijft de oplossing Kaspersky Anti Targeted Attack Platform (EDR) werken met Kaspersky Endpoint Security. Daarnaast wordt Kaspersky Endpoint Agent van de computer verwijderd. Hetzelfde gedrag in het systeem zal optreden wanneer u Kaspersky Endpoint Security bijwerkt naar versie 12.1 of hoger.

> Kaspersky Endpoint Security is niet compatibel met Kaspersky Endpoint Agent. U kunt deze programma's niet beide op dezelfde computer installeren.

Kaspersky Endpoint Security moet aan de volgende voorwaarden voldoen om te werken als onderdeel van Endpoint Detection and Response (KATA):

- Kaspersky Anti Targeted Attack Platform versie 5.0 of hoger.
- Kaspersky Security Center versie 14.2 of hoger (inclusief Network Agent). In eerdere versies van Kaspersky Security Center is het onmogelijk om de Endpoint Detection and Response (KATA)-functie te activeren.

Stappen voor het migreren van [KES KEA] configuratie naar [KES ingebouwde agent] voor EDR (KATA)

1. **De beheerplug-in voor Kaspersky Endpoint Security upgraden**

   De EDR (KATA)-onderdeel kan worden beheerd met de Kaspersky Endpoint Security Management Plug-in versie 12.1 of hoger. Afhankelijk van het type Kaspersky Security Center-console dat u gebruikt, werkt u de beheerplug-in in de Administration Console (MMC) of de webplug-in in de Web Console bij.

2. **Beleid en taken migreren**

   Zet Kaspersky Endpoint Agent-instellingen over naar Kaspersky Endpoint Security for Windows. De volgende opties zijn beschikbaar:

   - Een wizard voor het migreren van Kaspersky Endpoint Agent naar Kaspersky Endpoint Security. Een wizard voor het migreren van Kaspersky Endpoint Agent naar Kaspersky Endpoint Security werkt alleen in webconsole

     Zo migreert u beleids- en taakinstellingen van Kaspersky Endpoint Agent naar Kaspersky Endpoint Security in webconsole

     Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Operations** → **Migration from Kaspersky Endpoint Agent**.

     Hiermee wordt de wizard beleiden- en takenmigratie uitgevoerd. 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 het 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 ondersteunt geen EDR (KATA)-taken. Sla deze stap over.

Stap 3. Voltooiing van wizard

Verlaat de wizard verlaten. Als gevolg van de wizard wordt een nieuw Kaspersky Endpoint Security-beleid gemaakt. Het beleid voegt instellingen van Kaspersky Endpoint Security en Kaspersky Endpoint Agent samen. Het beleid krijgt de naam *<Naam van Kaspersky Endpoint Security-beleid> & <Naam van Kaspersky Endpoint Agent-beleid>*. Het nieuwe beleid heeft de status *Inactive*. Wijzig nu de statussen van het Kaspersky Endpoint Agent-beleid en het Kaspersky Endpoint Security-beleid in *Inactive* en activeer het nieuwe samengevoegde beleid.

De migratiewizard in Web Console de volgende beleidsinstellingen overslaat en deze niet migreert:

- Verbod op wijzigen van de instellingen **Connection settings** ("hangslot").

  Standaard kunnen de instellingen gewijzigd worden (het “hangslot” is open). De instellingen zijn daarom niet toegepast op de computer. U zult de wijziging van de instellingen moeten verbieden en het "hangslot" sluiten.

- Crypto-container.

  Als u twee-weg verificatie gebruikt om contact te maken met de Central Node servers, moet u de crypto-container opnieuw toevoegen.

Aangezien de migratiewizard deze instellingen niet migreert, kunt u fouten tegenkomen wanneer u de computer verbindt met Central Node-servers. Om de fouten op te lossen, moet u naar de beleidseigenschappen gaan en de verbindingsinstellingen configureren.

- Een standaard Batchconversiewizard voor beleid en taken De Batchconversiewizard van beleid en taken voor Kaspersky Security is alleen beschikbaar in de Beheerconsole (MMC). Voor meer informatie over beleiden en taken van de Batchconversiewizard raadpleegt u de Help van Kaspersky Security Center.

Om ervoor te zorgen dat Kaspersky Endpoint Security correct werkt op servers, wordt aanbevolen om bestanden die belangrijk zijn voor het functioneren van de server toe te voegen aan de vertrouwde zone. Voor SQL-servers moet u MDF- en LDF-databasebestanden toevoegen. Voor Microsoft Exchange-servers moet u CHK-, EDB-, JRS-, LOG- en JSL-bestanden toevoegen. U kunt bijvoorbeeld maskers gebruiken, bijvoorbeeld `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

Beginnend met Kaspersky Endpoint Security 12.6 voor Windows, uitzonderingen scannen en vertrouwde programma's worden toegevoegd aan de vertrouwde zone. Vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's helpen bij het snel configureren van Kaspersky Endpoint Security op SQL-servers, Microsoft Exchange-servers en System Center Configuration Manager. Dit betekent dat u niet handmatig een vertrouwde zone voor het programma op servers hoeft in te stellen.

EDR-telemetrie-uitsluitingsinstellingen migreren niet van het Kaspersky Endpoint Agent-beleid naar het Kaspersky Endpoint Security-beleid. Kaspersky Endpoint Security heeft zijn eigen uitsluitingstools - vertrouwde applicaties. De werking van Kaspersky Endpoint Security is geoptimaliseerd, zodat de afwezigheid van individuele EDR-telemetrie-uitsluitingen uw computer niet extra belast in vergelijking met Kaspersky Endpoint Agent. Kaspersky Endpoint Security gebruikt telemetrie niet alleen voor EDR (KATA), maar ook voor de werking van de onderdelen voor programmabeveiliging. Daarom is het niet nodig om afzonderlijke EDR-telemetrie-uitzonderingen over te dragen. Als de prestaties van de computer afnemen, controleer dan de werking van het programma (zie stap 7 De werking controleren).

3 Het licentiëren van de EDR (KATA) functionaliteit

Om Kaspersky Endpoint Security te activeren als onderdeel van de Kaspersky Anti Targeted Attack Platform-oplossing, hebt u een aparte licentie nodig voor Kaspersky Endpoint Detection and Response (KATA) Add-on. U kunt dan de sleutel toevoegen met de taak *Add key*. Als gevolg hiervan worden twee sleutels aan het programma toegevoegd: *Kaspersky Endpoint Security* en *Kaspersky Endpoint Detection and Response (KATA)*.

Licentiebeheer van Kaspersky Endpoint Detection and Response (KATA) Add-on op computers met eerder geactiveerde EDR Optimum- of EDR Expert-functies houdt de volgende speciale overwegingen in:

- Als u een *licentiebestand* gebruikt voor het licentiebeheer van Kaspersky Endpoint Security met EDR Optimum- of EDR Expert-functies, kunt u geen afzonderlijke sleutel toevoegen voor Kaspersky Endpoint Detection and Response (KATA) Add-on. U kunt overschakelen op het gebruik van een activatiecode voor licentiebeheer of contact opnemen met uw serviceprovider om een nieuw licentiebestand te verkrijgen voor het activeren van Kaspersky Endpoint Security- en EDR-functies. De serviceprovider levert een of meer sleutelbestanden voor licentiebeheer.

- Als u een *licentiebestand* gebruikt voor het licentiebeheer van Kaspersky Endpoint Security zonder EDR Optimum- of EDR Expert-functies, dan kunt u een afzonderlijke sleutel toevoegen voor Kaspersky Endpoint Detection and Response (KATA) Add-on zonder een nieuw licentiebestand.

- Als u een *activatiecode* gebruikt voor licentiebeheer, zal de Kaspersky-activeringsserver de code automatisch opnieuw uitgeven en worden EDR (KATA)-functies automatisch beschikbaar. In dit geval worden EDR Optimum en EDR Expert uitgeschakeld.

- Met Kaspersky Endpoint Security kunt u maximaal twee actieve codes toevoegen: Kaspersky Endpoint Security-code en een code voor de Add-on. U kunt ook maximaal twee reservecodes toevoegen. Eén reservecode van Kaspersky Endpoint Security en één reservecode van het add-on-type.

4 Het Kaspersky Endpoint Security-programma installeren/ upgraden

Om EDR (KATA)-functionaliteit te migreren tijdens de installatie of upgrade van een applicatie, wordt aanbevolen om de installatietaak op afstand. Wanneer u een installatietaak op afstand maakt, moet u de EDR (KATA)-component selecteren in de instellingen van het installatiepakket.

U kunt het programma ook upgraden met behulp van de volgende methoden:

- Met Kaspersky-updateservice.

- Lokaal, met behulp van de Installatiewizard.

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 actuele licenties van Kaspersky-oplossingen. Als op de computer Kaspersky Endpoint Agent is geïnstalleerd en EDR (KATA)-oplossing is geactiveerd, configureert het Kaspersky Endpoint Security-installatieprogramma automatisch de set onderdelen en selecteert het EDR (KATA)-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 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 actuele licenties van Kaspersky-oplossingen. In dit geval selecteert Kaspersky Endpoint Security automatisch componenten op basis van een reeks componenten van Kaspersky Endpoint Agent. Hierna schakelt Kaspersky Endpoint Security over op het gebruik van de ingebouwde agent en wordt Kaspersky Endpoint Agent verwijderd.

Kaspersky Endpoint Security ondersteunt upgraden zonder de computer opnieuw op te starten. U kunt de toepassingsupgrademodus in beleidseigenschappen.

5 De werking van het programma controleren

Als de computer na installatie of upgrade de status *Critical* heeft in de Kaspersky Security Center-console:

- Zorg ervoor dat op de computer Netwerkagent versie 13.2 of hoger is geïnstalleerd.
- Controleer de werkingsstatus van het ingebouwde agent door het *Report on status of application components* te bekijken. Als een onderdeel de status *Not installed* heeft, installeer dan de onderdeel met de taak *Change application components*. Als een onderdeel de *Geen onderdeel van licentie* toestand heeft, zorg er dan voor dat u de ingebouwde agent-functionaliteit heeft geactiveerd.
- Zorg ervoor dat u akkoord gaat met de Kaspersky Security Network-verklaring in het nieuwe beleid van Kaspersky Endpoint Security voor Windows.

6 Controleer de verbinding met Kaspersky Anti Targeted Attack Platform-servers

Controleer de verbinding met Kaspersky Anti Targeted Attack Platform-servers. Hiertoe doet u het volgende:

1. Controleer of u een geldig certificaat heeft.
2. Controleer de serververbindingsinstellingen.
3. Controleer het gebeurtenislogboek.

   Als er een verbinding met de server tot stand is gebracht, verzendt het programma de gebeurtenis *Successful connection to the EDR Expert server*. Als er geen geslaagde verbindingsgebeurtenis is en er geen gebeurtenissen zijn met verbindingsfouten, controleer de instellingen van het gebeurtenislogboek en schakel het verzenden van gebeurtenissen in voor Endpoint Detection and Response (KATA).

De verbindingsstatus van de server heeft geen invloed op de computerstatus in de Kaspersky Security Center-console. Daarom kan de computer, als er geen verbinding met de server is, nog steeds het *OK* toestand. Controleer het gebeurtenislogboek om de verbinding met de server te verifiëren.

7 Prestaties controleren

Als de prestaties van uw computer vertragen na het installeren of bijwerken van een programma, kunt u de gegevensoverdracht optimaliseren. Hiertoe doet u het volgende:

1. Schakel het EDR (KATA)-onderdeel uit en controleer of de prestatievermindering te wijten is aan EDR (KATA).
2. Voor vertrouwde programma's, schakelt u telemetrieverzameling uit bij console-invoerbewerkingen (standaard ingeschakeld).
3. Voeg programma's die de computerprestaties verminderen toe aan de lijst met vertrouwde programma's.
4. Neem contact op met de technische klantenondersteuning van Kaspersky. Ondersteuningsexperts helpen u bij het configureren van telemetriefilters in Kaspersky Anti Targeted Attack Platform. Dit zal de hoeveelheid verkeer verminderen. Als uw computerprestaties beïnvloed worden door een bepaald programma, voegt u het distributiepakket van dat programma toe aan het verzoek.

Endpoint Detection and Response Expert (on-premises)



Kaspersky Endpoint Security voor Windows ondersteunt integratie met de Kaspersky Endpoint Detection and Response Expert (on-premises)-oplossing. *Kaspersky Endpoint Detection and Response Expert (on-premises)* is een enterprise-cyberbeveiligingsoplossing die Kaspersky-programma's bevat waarmee een organisatie zich kan verdedigen tegen de meeste soorten cyberrisico's en die de belangrijkste scenario's voor de verspreiding van dreigingen dekt. Onderdelen van EDR Expert (on-premises) worden geïmplementeerd op het Open Single Management Platform (OSMP). Dit platform voert cross-platformscenario's uit in één enkele interface en maakt het mogelijk om Kaspersky-programma's te integreren met programma's van derden in een uitgebreid beveiligingssysteem.

Een van de centrale elementen van de oplossing is: *SIEM*. SIEM houdt gebeurtenissen bij die afkomstig zijn van alle onderdelen en correleert deze gebeurtenissen met elkaar met behulp van door de leverancier en door de gebruiker gedefinieerde regels. EDR Expert (on-premises) bekijkt logboeken en telemetriegegevens die worden ontvangen van de bedrijfsinfrastructuur om aanvallen automatisch te detecteren en maakt het onderzoek van incidenten mogelijk met behulp van een uniforme onderzoeksgrafiek die alle gebeurtenissen combineert die in EDR Expert (on-premises) zijn verzameld, inclusief gebeurtenissen van Kaspersky-programma's en informatiebeveiligingsproducten van derden.

Voor de reactie op geavanceerde incidenten gebruikt EDR Expert (on-premises) vooraf ingestelde en door de gebruiker gedefinieerde scenario's. U kunt ook responsacties van programma's van derden en responsscenario's waarbij meerdere programma's zijn betrokken, gebruiken.

Tools voor dreigingsinformatie

Kaspersky Endpoint Detection and Response gebruikt de volgende Threat Intelligence-tools:

- De integratie met Kaspersky Threat Intelligence Portal dat informatie over de reputatie van bestanden en webadressen bevat en toont.
- Kaspersky Threats-database.
- 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.

Werkingsprincipe van de oplossing

Het programma Kaspersky Endpoint Security wordt op individuele computers op de IT-infrastructuur van het bedrijf geïnstalleerd en bewaakt continu processen, open netwerkverbindingen en bestanden die worden gewijzigd.

Bij installatie in de standaardmodus in de VDI -infrastructuur ondersteunt Kaspersky Endpoint Security integratie met EDR Expert (on-premises). De bruikbaarheid van de andere functies van het programma is echter niet gegarandeerd. Voor de bescherming van virtuele machines in de VDI-infrastructuur raden we aan dat u Kaspersky Endpoint Security in Light Agent-modus.

Informatie over gebeurtenissen op de computer (telemetrie) wordt verzonden naar de EDR Expert (on-premises) server. In dit geval verzendt Kaspersky Endpoint Security ook informatie over dreigingen gevonden door het programma, evenals informatie over verwerkingsresultaten voor deze dreigingen naar de servers voor het verzamelen van telemetriegegevens.

De EDR Expert (on-premises) integratie wordt geconfigureerd op de Kaspersky Security Center-console. De ingebouwde agent wordt vervolgens beheerd met behulp van de Open Single Management Platform (OSMP), inclusief het uitvoeren van taken, het beheren van in quarantaine geplaatste objecten, het bekijken van rapporten en andere acties.

Kaspersky Endpoint Security-configuraties voor het werken met EDR Expert (on-premises)

Voor het werken met EDR Expert (on-premises) kunnen de volgende configuraties worden gebruikt:

- **[KES+built-in agent]**. In deze configuratie fungeert Kaspersky Endpoint Security zowel als het programma dat de veiligheid van de computer garandeert, als het programma voor het werken met EDR Expert (on-premises). De ingebouwde agent voor EDR Expert (on-premises) is beschikbaar in Kaspersky Endpoint Security 12.11 voor Windows of hoger.

- **[EPP+EDR Agent van derden]**. In deze configuratie wordt de beveiliging van de IT-infrastructuur verzorgd door het Endpoint Protection Platform (EPP) van derden. De interactie met EDR Expert (on-premises) wordt verzorgd door Kaspersky Endpoint Security in de configuratie Endpoint Detection and Response Agent (EDR Agent). In deze configuratie is EDR-agent compatibel met EPP-applicaties van derden. EDR-agent voor EDR Expert (on-premises) is beschikbaar in Kaspersky Endpoint Security 12.11 voor Windows of hoger.

Integratie van de ingebouwde agent met EDR Expert (on-premises)

Voor integratie met de oplossing van Kaspersky Endpoint Detection and Response Expert (on-premises), moet u het onderdeel Endpoint Detection and Response Expert (on-premises) toevoegen en Kaspersky Endpoint Security configureren.

De Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud), en Endpoint Detection and Response Expert (on-premises) onderdelen zijn niet compatibel met elkaar.

Aan de volgende voorwaarden moet worden voldaan om Endpoint Detection and Response (on-premises) te laten werken:

- OSMP (Open Single Management Platform) is geïnstalleerd.
- Het programma is geactiveerd en de functionaliteit valt onder de licentie.
- Het onderdeel Endpoint Detection and Response Expert (on-premises) is ingeschakeld.
- Programmaonderdelen die zorgen voor de werking van EDR Expert (on-premises) zijn ingeschakeld en operationeel. De volgende onderdelen zorgen voor de werking van EDR Expert (on-premises):
  - File Threat Protection.
  - Web Threat Protection.
  - Mail Threat Protection.
  - Exploit-preventie.
  - Gedragsdetectie.
  - Host Intrusion Prevention.
  - Remediation Engine.
  - Adaptieve controle op afwijkingen.

Het opzetten van de EDR Expert (on-premises) integratie omvat de volgende stappen:

1. **Het onderdeel EDR Expert (on-premises) installeren**

   U kunt het onderdeel EDR Expert (on-premises) selecteren tijdens: installatie of upgrade, alsook tijdens het gebruik van de taak *Programmaonderdelen wijzigen*.

   > U moet uw computer opnieuw opstarten om de upgrade van het programma met het nieuwe onderdeel te voltooien.

2. **Kaspersky Endpoint Detection and Response Expert (on-premises) activeren**

   U moet een afzonderlijke licentie kopen voor EDR Expert (on-premises) (Kaspersky Endpoint Detection and Response Expert (on-premises) add-on).

   De functie wordt beschikbaar na toevoeging van een afzonderlijke sleutel voor Kaspersky Endpoint Detection and Response Expert (on-premises). Als resultaat worden er twee sleutels op de computer toegevoegd: een sleutel voor Kaspersky Endpoint Security en een sleutel voor Kaspersky Endpoint Detection and Response Expert (on-premises).

   Licenties voor de zelfstandige Endpoint Detection and Response Expert (on-premises) functionaliteit is hetzelfde als de licentie van Kaspersky Endpoint Security.

   Zorg ervoor dat de EDR Export (on-premises)-functionaliteit is inbegrepen in de licentie en wordt uitgevoerd in de lokale interface van het programma.

3. **Verbinding maken met de server voor het verzamelen van telemetriegegevens en de responsserver**

Kaspersky Endpoint Detection and Response Expert (on-premises) vereist een vertrouwde verbinding tussen Kaspersky Endpoint Security en twee servers:

- Een *telemetrieverzamelingsserver* is een server die deel uitmaakt van een SIEM oplossing die informatie over gebeurtenissen op de computer verzamelt, normaliseert, correleert, analyseert en opslaat.
- Een *responsservers* is een server voor het ontvangen en scannen van gegevens, het bestuderen van het gedrag van objecten en het publiceren van de resultaten van dergelijke onderzoeken.

Gebruik een TLS-certificaat om een vertrouwde verbinding te configureren. U kunt een TLS-certificaat verkrijgen via het Open Single Management Platform (zie de instructies in de Help van Kaspersky Endpoint Detection and Response Expert (on-premises)). Vervolgens moet u het TLS-certificaat toevoegen aan Kaspersky Endpoint Security (zie onderstaande instructies).

Standaard controleert Kaspersky Endpoint Security alleen het TLS-certificaat van de servers. Om de verbinding veiliger te maken, kunt u bovendien de verificatie van de computer op de server (twee-weg verificatie) inschakelen. Om deze verificatie in te schakelen, moet u twee-weg inschakelen in de server- en Kaspersky Endpoint Security-instellingen. Om twee-weg verificatie te gebruiken hebt u ook een crypto-container nodig. Een *crypto-container* is een PFX-archief met een certificaat en een privésleutel. U kunt een cryptocontainer verkrijgen op het Open Single Management Platform (zie de instructies in de Help van Kaspersky Endpoint Detection and Response Expert (on-premises)).

Een Kaspersky Endpoint Security-computer verbinden met EDR Expert (on-premises) via de webconsole

1. Selecteer in het hoofdvenster van de Webconsole het tabblad **Asset management** → **Policies**.
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 **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (on-premises)**.
5. Zet de schakelaar **Endpoint Detection and Response Expert (on-premises) ENABLED** aan.
6. Als u EDR Expert (on-premises) wilt configureren, selecteert u **Endpoint Detection and Response Expert (version 8.0 or later)** in de lijst met oplossingen.
7. Configureer de *servers voor het verzamelen van telemetriegegevens* verbinding:

   a. Klik in het blok **Connection to telemetry collection servers** op de koppeling **Connection settings**.

   b. Configureer de verbinding met de servers voor het verzamelen van telemetriegegevens:

   - **Timeout (sec)**. Maximale time-out voor de serverrespons. Wanneer de time-out is verstreken, probeert Kaspersky Endpoint Security verbinding te maken met een andere server.
   - **Server certificate**. TLS-certificaat voor het tot stand brengen van een vertrouwde verbinding met de server. U kunt een TLS-certificaat verkrijgen via het Open Single Management Platform (zie de instructies in de Help van Kaspersky Endpoint Detection and Response Expert (on-premises)).

- **Use two-way authentication**. Tweerichtingsverificatie bij het tot stand brengen van een beveiligde verbinding tussen Kaspersky Endpoint Security en de server. Om tweerichtingsverificatie te gebruiken, moet u tweerichtingsverificatie inschakelen in de server instellingen, vervolgens een crypto-container ophalen en een wachtwoord instellen om de crypto-container te beschermen. Een *crypto-container* is een PFX-archief met een certificaat en een privésleutel. U kunt een cryptocontainer verkrijgen op het Open Single Management Platform (zie de instructies in de Help van Kaspersky Endpoint Detection and Response Expert (on-premises)). Na het configureren van de server instellingen, moet u ook tweerichtingsverificatie inschakelen in de instellingen van Kaspersky Endpoint Security en een met een wachtwoord beveiligde crypto-container laden.

  > De crypto-container moet met een wachtwoord worden beveiligd. Het is niet mogelijk om een crypto-container toe te voegen met een leeg wachtwoord.

c. Klik op **OK**.

d. Voeg servers voor het verzamelen van telemetrie toe. Hiertoe geeft u het serveradres (IPv4, IPv6) en de poort op om verbinding te maken met de server.

U kunt meerdere adressen van telemetrie-verzamelingsservers toevoegen. Kaspersky Endpoint Security probeert verbinding te maken met de server op het eerste IP-adres. Als er geen verbinding tot stand kan worden gebracht, probeert Kaspersky Endpoint Security verbinding te maken via het tweede IP-adres in de lijst, enzovoort.

e. Indien nodig, telemetrie configureren.

8. Configureer de *responsservers* verbinding:

a. Configureer in het blok **Connection to response servers** de instellingen **Send sync request to server every (min)**. Frequentie van synchronisatieverzoeken die naar de server worden verzonden. Tijdens de synchronisatie ontvangt Kaspersky Endpoint Security responstaken op dreigingen en verstuurt het de resultaten van de taken.

b. Klik op de koppeling **Connection settings**.

c. Configureer de responsservers verbinding:

- **Timeout (sec)**. Maximale time-out voor de serverrespons. Wanneer de time-out is verstreken, probeert Kaspersky Endpoint Security verbinding te maken met een andere server.

- **Server certificate**. TLS-certificaat voor het tot stand brengen van een vertrouwde verbinding met de server. U kunt een TLS-certificaat verkrijgen via het Open Single Management Platform (zie de instructies in de Help van Kaspersky Endpoint Detection and Response Expert (on-premises)).

- **Use two-way authentication**. Tweerichtingsverificatie bij het tot stand brengen van een beveiligde verbinding tussen Kaspersky Endpoint Security en de server. Om tweerichtingsverificatie te gebruiken, moet u tweerichtingsverificatie inschakelen in de server instellingen, vervolgens een crypto-container ophalen en een wachtwoord instellen om de crypto-container te beschermen. Een *crypto-container* is een PFX-archief met een certificaat en een privésleutel. U kunt een cryptocontainer verkrijgen op het Open Single Management Platform (zie de instructies in de Help van Kaspersky Endpoint Detection and Response Expert (on-premises)). Na het configureren van de server instellingen, moet u ook tweerichtingsverificatie inschakelen in de instellingen van Kaspersky Endpoint Security en een met een wachtwoord beveiligde crypto-container laden.

  > De crypto-container moet met een wachtwoord worden beveiligd. Het is niet mogelijk om een crypto-container toe te voegen met een leeg wachtwoord.

d. Klik op **OK**.

e. Voeg responsservers toe. Hiertoe geeft u het serveradres (IPv4, IPv6) en de poort op om verbinding te maken met de server.

   U kunt meerdere adressen van responsservers toevoegen. Kaspersky Endpoint Security probeert verbinding te maken met de server op het eerste IP-adres. Als er geen verbinding tot stand kan worden gebracht, probeert Kaspersky Endpoint Security verbinding te maken via het tweede IP-adres in de lijst, enzovoort.

9. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Als gevolg hiervan wordt de computer toegevoegd aan de lijst met beheerde apparaten op het Open Single Management Platform (OSMP). Controleer de werkingsstatus van het onderdeel door het *Report on status of application components* 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 Expert (on-premises)** wordt toegevoegd aan de lijst met Kaspersky Endpoint Security-onderdelen.

Instellingen voor EDR Expert (on-premises) telemetrie configureren

Telemetrie is een lijst met gebeurtenissen die hebben plaatsgevonden op de beveiligde computer. Kaspersky Endpoint Security analyseert telemetriegegevens en verzendt deze tijdens synchronisatie naar telemetrieverzamelservers. Telemetriegebeurtenissen komen bijna continu op de server aan. Kaspersky Endpoint Security start de synchronisatie met de server wanneer aan een van de volgende voorwaarden is voldaan:

- Het synchronisatie-interval is vervallen.
- Het aantal gebeurtenissen in de buffer overschrijdt de bovengrens.

Daarom synchroniseert het programma standaard elke 30 seconden of wanneer de buffer 1024 gebeurtenissen bevat. U kunt het synchronisatiegedrag configureren in het Kaspersky Endpoint Security-beleid en optimale waarden selecteren die overeenkomen met uw netwerkbelasting (zie onderstaande instructies).

Als er geen verbinding is tussen Kaspersky Endpoint Security en de server, plaatst het programma nieuwe gebeurtenissen in de wachtrij. Wanneer de verbinding hersteld is, stuurt Kaspersky Endpoint Security gebeurtenissen in de wachtrij in de juiste volgorde naar de server. Om overbelasting van de server te voorkomen, kan Kaspersky Endpoint Security bepaalde gebeurtenissen overslaan. Hiervoor kunt u de instellingen voor gebeurtenisoverdracht optimaliseren zoals een maximale waarde voor gebeurtenissen per uur (zie onderstaande instructies).

Voer de volgende stappen uit om telemetrie-instellingen te configureren.

1. Selecteer in het hoofdvenster van de Webconsole het tabblad **Asset management → Policies**.
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 **Built-in Agents Configuration → Endpoint Detection and Response Expert (on-premises)**.
5. Als u EDR Expert (on-premises) wilt configureren, selecteert u **Endpoint Detection and Response Expert (version 8.0 or later)** in de lijst met oplossingen.
6. Zorg ervoor dat de **Send telemetry to telemetry collection servers** selectievakje is ingeschakeld in het **Data transmission settings** blok.
7. Schakel indien nodig het selectievakje **Send telemetry with IOA only** in. *Indicator van aanval (IOA)* is een regel die een beschrijving bevat van verdacht gedrag in het systeem dat kan wijzen op een gerichte aanval. Het programma vergelijkt het gedrag in het systeem met deze regels en registreert gebeurtenissen die wijzen op een gerichte aanval. Het programma gebruikt de *streaming scan*technologie die het mogelijk maakt om dergelijke gebeurtenissen in realtime bij te houden.
8. Configureer indien nodig de synchronisatie met de serverinstellingen in het blok **Data transmission settings**:

   - **Maximum event transmission delay (sec)**. Het programma synchroniseert met de server om gebeurtenissen te verzenden nadat het synchronisatie-interval is verlopen. De standaardinstelling is 30 seconden.
   - **Maximum number of event packages**. Het programma synchroniseert met de server wanneer de buffer gevuld is met gebeurtenissen. De standaardinstelling is 1024 gebeurtenissen.
9. Schakel indien nodig het selectievakje **Enable request throttling** uit in het blok **Request throttling**.

   Dit helpt de belasting op de server te optimaliseren. Als deze functionaliteit is ingeschakeld, beperkt het programma de verzending van gebeurtenissen. Als het aantal gebeurtenissen de ingestelde limieten overschrijdt, stopt Kaspersky Endpoint Security met het verzenden van gebeurtenissen. Deze optie is standaard ingeschakeld.
10. Configureer optimalisatie-instellingen voor het verzenden van gebeurtenissen naar de server:

    - **Maximum number of events per hour**. Het programma analyseert de telemetriegegevensstroom en beperkt het verzenden van gebeurtenissen als de gebeurtenisstroom de geconfigureerde limiet voor gebeurtenissen per uur overschrijdt. Kaspersky Endpoint Security hervat het verzenden van gebeurtenissen na een uur. De standaardinstelling is 3000 gebeurtenissen per uur. Als het programma op een server is geïnstalleerd, is de telemetrie gegevensstroom hoger. Voor servers wordt aanbevolen om de waarde te verhogen tot 60 000 gebeurtenissen per uur.
    - **Percentage of event limit excess**. Het programma sorteert gebeurtenissen op type (bijvoorbeeld 'wijzigingen in het register'-gebeurtenissen) en beperkt de overdracht van gebeurtenissen als de verhouding tussen gebeurtenissen van hetzelfde type en het totale aantal gebeurtenissen de geconfigureerde limiet overschrijdt. Kaspersky Endpoint Security hervat het verzenden van gebeurtenissen wanneer de verhouding tussen andere gebeurtenissen en het totale aantal gebeurtenissen opnieuw groot genoeg is. De standaardinstelling is 15 %.
11. In de **Connection to response servers** blok, voer een waarde in voor de **Send sync request to server every (min)** parameter.

12. Frequentie van synchronisatieverzoeken die naar de server worden verzonden. Tijdens de synchronisatie verzendt Kaspersky Endpoint Security informatie over gewijzigde programma-instellingen en -taken.

13. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Uitzonderingen voor telemetrie van EDR Expert (on-premises)

Om de prestaties te verbeteren en de gegevensoverdracht naar de telemetrieverzamelingsservers te optimaliseren, kunt u uitzonderingen voor telemetrie toevoegen. U kunt er bijvoorbeeld voor kiezen om geen gegevens voor netwerkcommunicaties voor individuele programma's te verzenden.

> Het gebruik van te veel regels kan de belasting van de telemetrieverzamelingsserver verhogen en de prestaties van de computer verminderen. We raden u aan om alleen noodzakelijke regels toe te voegen.

Een telemetrie-uitzondering maken in de Webconsole en de Cloudconsole:

1. Selecteer in het hoofdvenster van de Webconsole het tabblad **Asset management** → **Policies**.

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** → **Telemetry Settings**.

5. Selecteer het tabblad **EDR Expert (on-premises) telemetry**.

6. In het blok **General exclusions**, klikt u op de knop **Add**.

   Het venster **Add exclusion rule** wordt geopend.

7. Wijzig indien nodig de status van de regel. De regel is standaard ingeschakeld.

8. Voer een naam voor de regel in.

9. Selecteer de actie die moet worden uitgevoerd wanneer de regel wordt geactiveerd:

   - **Do not collect**. De gefilterde gebeurtenis wordt uitgesloten van de verzonden telemetrie.
   - **Exclude IOA**. De gebeurtenis die de IOA-regel activeert, wordt uitgezonderd van de verzonden telemetrie.

10. Als de **Exclude IOA** optie is geselecteerd, geeft u de IOA-regels op die aan uitzonderingen moeten worden toegevoegd:

    - **Exclude all**. Wanneer aan de opgegeven voorwaarde is voldaan, sluit het programma gebeurtenissen uit die zijn gegenereerd op basis van alle IOA-regels van de telemetrie.
    - **Exclude by GUID**. Geef de GUID van de IOA-regel op. U kunt meerdere GUID's opgeven met `,`. Voor meer informatie over de IOA-regels raadpleeg de Help van EDR Expert (on-premises).

11. Geef de filtervoorwaarde op:

    a. Selecteer de veldnaam die moet worden gebruikt voor het filteren.

    b. Selecteer een operator (zie de tabel hieronder) en geef de waarde op waarmee de veldwaarde van de gebeurtenis wordt vergeleken.

Lijst met voorwaardelijke operators

Operator	Beschrijving
<	Als de veldwaarde kleiner is dan de waarde die is opgegeven in de voorwaarde, wordt de gebeurtenis uitgefilterd.
≤	Als de veldwaarde kleiner is dan of gelijk is aan de waarde die is opgegeven in de voorwaarde, wordt de gebeurtenis uitgefilterd.
=	Als de waarde van het veld gelijk is aan de waarde die is opgegeven in de voorwaarde, wordt de gebeurtenis uitgefilterd.
≥	Als de waarde van het veld groter is dan of gelijk is aan de waarde die is opgegeven in de voorwaarde, wordt de gebeurtenis uitgefilterd.
>	Als de veldwaarde groter is dan de waarde die is opgegeven in de voorwaarde, wordt de gebeurtenis uitgefilterd.
≠	Als de waarde van het veld niet gelijk is aan de waarde die is opgegeven in de voorwaarde, wordt de gebeurtenis uitgefilterd.
is like	Als de veldwaarde overeenkomt met het masker dat is opgegeven in de voorwaarde, wordt de gebeurtenis uitgefilterd. Het programma ondersteunt de `*` en `?` tekens bij het invoeren van een masker:
is not like	Als de veldwaarde niet overeenkomt met het masker dat is opgegeven in de voorwaarde, wordt de gebeurtenis uitgefilterd. Het programma ondersteunt de `*` en `?` tekens bij het invoeren van een masker:
one of	Als de veldwaarde overeenkomt met een van de waarden in de lijst die is opgegeven in de voorwaarde, wordt de gebeurtenis uitgefilterd.
none of	Als de veldwaarde niet overeenkomt met een van de waarden in de lijst die in de voorwaarde is opgegeven, wordt de gebeurtenis uitgefilterd.
is like one of	Als de veldwaarde overeenkomt met een van de opgegeven maskers in de voorwaarde, wordt de gebeurtenis uitgefilterd. Het programma ondersteunt de * en ? tekens wanneer u een masker invoert.
is not like one of	Als de veldwaarde niet overeenkomt met een van de opgegeven maskers in de voorwaarde, wordt de gebeurtenis uitgefilterd. Het programma ondersteunt de * en ? tekens wanneer u een masker invoert.
exists	Als het opgegeven veld in de voorwaarde aanwezig is in de gebeurtenis, wordt de gebeurtenis uitgefilterd.
not exists	Als het opgegeven veld in de voorwaarde niet aanwezig is in de gebeurtenis, wordt de gebeurtenis uitgefilterd.
contains	Als de opgegeven waarde in de voorwaarde aanwezig is in de veldwaarde, wordt de gebeurtenis uitgefilterd.
is equal to	Als de waarde van het veld gelijk is aan de waarde die is opgegeven in de voorwaarde, wordt de gebeurtenis uitgefilterd. De scan is niet hoofdlettergevoelig.
bitwise AND	Als het resultaat van de Bitwise AND (&)-bewerking tussen de veldwaarde en de opgegeven waarde in de voorwaarde 1 is, wordt de gebeurtenis uitgefilterd.

12. Indien nodig kunt u complexe filtercriteria maken door meerdere filtervoorwaarden en groepen voorwaarden toe te voegen. U kunt ook geneste voorwaarden en voorwaardegroepen toevoegen aan een voorwaardegroep. U kunt de volgende operators gebruiken:

    - **AND** betekent dat het filter gebeurtenissen selecteert die aan alle opgegeven voorwaarden voldoen.
    - **OR** betekent dat het filter gebeurtenissen selecteert die aan een van de opgegeven voorwaarden voldoen.
    - **NOT** (om deze operator te gebruiken, selecteer de optie **Add NOT before**) betekent dat de filter gebeurtenissen selecteert die niet aan een van de opgegeven voorwaarden voldoen.

    Voorwaarden en voorwaardegroepen op het eerste niveau worden gecombineerd met de **AND** operator.

13. Als op uw computer Open Single Management Platform (OSMP) wordt uitgevoerd, kunt u de gemaakte filterregel scannen. Om de scan uit te voeren, klik op de knop **Check rule**.

    In het geopende venster wordt een tabel met gebeurtenissen weergegeven die zijn gefilterd op de gemaakte regel. Voor meer details, raadpleeg de Help van EDR Expert (on-premises).

14. Indien nodig, onder **All event types**, voeg telemetrie-uitzonderingen toe op de type gebeurtenis.

    a. Klik op de naam van het gebeurtenistype.

    b. Klik in het venster op de knop **Set up manually**.

    c. Configureer indien nodig de verzending van telemetrie voor het geselecteerde type gebeurtenis met de **Send event** schakelaar. Standaard is verzending van telemetrie ingeschakeld voor alle gebeurtenistypen.

    d. In het blok **Exclusion rules**, klikt u op de knop **Add**.

    Het venster **Add exclusion rule** wordt geopend.

    e. Voer de acties uit die worden beschreven in stap 7–13 voor elke regel die u toevoegt.

15. Voor sommige gebeurtenistypen kunt u ook opnameregels toevoegen om de verzamelde telemetrie uit te breiden:

    a. In het blok **Inclusion rules**, klikt u op de knop **Add**.

    Het venster **Add inclusion rules** wordt geopend.

    b. Voer een naam voor de regel in.

    c. Onder **Condition**, voert u waarden voor de weergegeven velden in. Het type beschikbare velden hangt af van de geselecteerde gebeurtenis.

> Uitzonderingsregels krijgen voorrang op opnameregels.

16. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

EDR Expert (on-premises) gebeurtenisfilters exporteren en importeren

U kunt de lijst met uitzonderingen exporteren naar een JSON-bestand. Vervolgens kunt u het bestand aanpassen om bijvoorbeeld een groot aantal gebeurtenis-ID's toe te voegen. U kunt ook de export/import-functie gebruiken om een back-up te maken van de gebeurtenisfilters, of om de lijst naar een andere server te migreren.

> Het gebruik van te veel regels kan de belasting van de telemetrieverzamelingsserver verhogen en de prestaties van de computer verminderen. We raden u aan om alleen noodzakelijke regels toe te voegen.

Gebeurtenisfilters exporteren en importeren in de Beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.

2. Selecteer in de beheerconsole **Policies**.

3. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

4. Selecteer **Algemene instellingen → Uitzonderingen en objecttypen** in het beleidsvenster.

5. In het blok **Telemetrie-instellingen → EDR Expert (on-premises)-telemetrie**, klikt u op de knop **Instellingen**.

6. Om de gebeurtenisfilters te exporteren:

   a. Klik op **Exporteren**.

   Geef in het geopende venster de naam van het JSON-bestand op waarnaar u de gebeurtenisfilters wilt exporteren. Selecteer vervolgens de map waarin u dit bestand wilt opslaan.

   b. Sla het bestand op.

   Kaspersky Endpoint Security exporteert de gebeurtenisfilters naar het JSON-bestand.

7. Om de gebeurtenisfilters te importeren:

   a. Klik op **Importeren**.

   b. Selecteer in het venster dat opent het JSON-bestand waaruit u de gebeurtenisfilters wilt importeren.

   c. Open het bestand.

   Als er al regels voor het filteren van gebeurtenissen op de computer bestaan, vervangt Kaspersky Endpoint Security deze tijdens het importeren.

8. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Gebeurtenisfilters in de webconsole exporteren en importeren

1. Selecteer in het hoofdvenster van de Webconsole het tabblad **Asset management → Policies**.

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 → Telemetry Settings**.

5. Selecteer het tabblad **EDR Expert (on-premises) telemetry**.

6. Om de gebeurtenisfilters te exporteren:

   a. Klik op **Export**.

   b. Geef in het geopende venster de naam van het JSON-bestand op waarnaar u de gebeurtenisfilters wilt exporteren. Selecteer vervolgens de map waarin u dit bestand wilt opslaan.

   c. Sla het bestand op.

   Kaspersky Endpoint Security exporteert de gebeurtenisfilters naar het JSON-bestand.

7. Om de gebeurtenisfilters te importeren:

    a. Klik op **Import**.

    b. Selecteer in het venster dat opent het JSON-bestand waaruit u de gebeurtenisfilters wilt importeren.

    c. Selecteer hoe u regels voor het filteren van gebeurtenissen wilt importeren: door deze toe te voegen aan bestaande regels of door bestaande regels te verwijderen en te vervangen door nieuwe.

    d. Open het bestand.

8. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

U kunt gebeurtenisfilters ook exporteren of importeren in de opdrachtregel.

Speciale overwegingen bij het gebruik van beleidsprofielen voor de configuratie van de integratie met EDR Expert (on-premises) en EDR (KATA)

Om integratie met EDR (KATA) voor bepaalde beheergroepen en met EDR Expert (on-premises) voor anderen als onderdeel van één beleid te configureren, moet u beleidsprofielen gebruiken. U moet de instellingen voor EDR (KATA)-integratie configureren in de beleidseigenschappen en de EDR Expert (on-premises)-integratie voor geselecteerde beheergroepen moet worden geconfigureerd in de eigenschappen van het beleidsprofiel.

Het gebruik van beleidsprofielen voor de configuratie van de integratie met EDR Expert (on-premises) heeft de volgende beperkingen:

- Als u de integratie met EDR Expert (on-premises) configureert in de beleidseigenschappen, zijn deze instellingen van toepassing op alle beheergroepen. integratie-instellingen uit beleidsprofielen worden niet toegepast.

- Wanneer u beleidsprofielen gebruikt om de integratie met EDR Expert (on-premises) te configureren, kunt u de Beheerconsole (MMC) niet gebruiken om het beleid te beheren. Wanneer u de beleidseigenschappen in de Beheerdersconsole opent, worden de EDR Expert (on-premises)-integratieinstellingen in de beleidsprofielen overschreven door de instellingen van het beleid, waardoor het onderdeel niet correct werkt. U moet de onderdeelinstellingen van Endpoint Detection and Response Expert (on-premises) volgens de onderstaande instructie resetten.

- Wanneer u beleidsprofielen gebruikt om de integratie met EDR Expert (on-premises) te configureren, kunt u geen onderliggend beleid gebruiken.

Als u al een beleid hebt geconfigureerd in een oudere versie van de webplug-in, moet u de instellingen voor het onderdeel Endpoint Detection and Response Expert (on-premises) resetten om de EDR Expert (on-premises) integratie-instellingen toe te passen op beheerde apparaten vanuit de beleidsprofielen.

Om de onderdeelinstellingen te resetten:

1. Selecteer in het hoofdvenster van de Webconsole het tabblad **Asset management** → **Policies**.

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 **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (on-premises)**.
5. Wijzig de uitvoermodus van **Endpoint Detection and Response Expert (version 7.1 or earlier)** naar **Endpoint Detection and Response Expert (versie 8.0 of nieuwer)-modus**.
6. Terugschakelen naar **Endpoint Detection and Response Expert (version 7.1 or earlier)**.
7. Sla uw wijzigingen op.

Endpoint Detection and Response Expert (cloud)

De integratie van Kaspersky Endpoint Security voor Windows met Kaspersky Endpoint Detection and Response Expert (cloud) is tijdelijk niet beschikbaar. Deze functionaliteit wordt volgens de plannign eind 2026 ondersteund. Houd onze Release-mededelingen bij om op de hoogte te blijven van programma-upgrades en nieuwe functies.



Kaspersky Endpoint Security voor Windows ondersteunt integratie met de Kaspersky Endpoint Detection and Response Expert (cloud)-oplossingen. *Kaspersky Endpoint Detection and Response Expert (cloud)* is een cloudgebaseerde-cyberbeveiligingsoplossing die Kaspersky-programma's bevat waarmee een organisatie zich kan verdedigen tegen de meeste soorten cyberrisico's en die de belangrijkste scenario's voor de verspreiding van dreigingen dekt. Onderdelen van EDR Expert (cloud) worden geïmplementeerd op het Open Single Management Platform (OSMP). Dit platform voert cross-platformscenario's uit in één enkele interface en maakt het mogelijk om Kaspersky-programma's te integreren met programma's van derden in een uitgebreid beveiligingssysteem.

Integratie met Kaspersky Endpoint Detection and Response Expert (cloud) wordt niet ondersteund op Arm-computers.

Een van de centrale elementen van de oplossing is: *SIEM*. SIEM houdt gebeurtenissen bij die afkomstig zijn van alle onderdelen en correleert deze gebeurtenissen met elkaar met behulp van door de leverancier en door de gebruiker gedefinieerde regels. EDR Expert (cloud) bekijkt logboeken en telemetriegegevens die worden ontvangen van de bedrijfsinfrastructuur om aanvallen automatisch te detecteren en maakt het onderzoek van incidenten mogelijk met behulp van een uniforme onderzoeksgrafiek die alle gebeurtenissen combineert die in EDR Expert (cloud) zijn verzameld, inclusief gebeurtenissen van Kaspersky-programma's en informatiebeveiligingsproducten van derden.

Voor de reactie op geavanceerde incidenten gebruikt EDR Expert (cloud) vooraf ingestelde en door de gebruiker gedefinieerde scenario's. U kunt ook responsacties van programma's van derden en responsscenario's waarbij meerdere programma's zijn betrokken, gebruiken.

Tools voor dreigingsinformatie

Kaspersky Endpoint Detection and Response gebruikt de volgende Threat Intelligence-tools:

- De integratie met Kaspersky Threat Intelligence Portal dat informatie over de reputatie van bestanden en webadressen bevat en toont.
- Kaspersky Threats-database.
- 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.

Werkingsprincipe van de oplossing

Het programma Kaspersky Endpoint Security 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 (telemetrie) wordt verzonden naar de EDR Expert (cloud) server. In dit geval verzendt Kaspersky Endpoint Security ook informatie over dreigingen gevonden door het programma, evenals informatie over verwerkingsresultaten voor deze dreigingen naar de servers voor het verzamelen van telemetriegegevens.

De EDR Expert (cloud) integratie wordt geconfigureerd op de Kaspersky Security Center-console. De ingebouwde agent wordt vervolgens beheerd met behulp van de Open Single Management Platform (OSMP), inclusief het uitvoeren van taken, het beheren van in quarantaine geplaatste objecten, het bekijken van rapporten en andere acties.

Integratie van de ingebouwde agent met EDR Expert (cloud)

Om integratie met de Kaspersky Endpoint Detection and Response (cloud)-oplossing in te stellen, moet u de onderdelen Endpoint Detection and Response Expert (cloud) installeren en Kaspersky Endpoint Security configureren.

De Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud), en Endpoint Detection and Response Expert (on-premises) onderdelen zijn niet compatibel met elkaar.

Toepassingsomstandigheden van EDR Expert (cloud)

EDR-expert (cloud) werkt alleen als u aan de volgende voorwaarden voldoet:

- De infrastructuur van Kaspersky Endpoint Detection and Response Expert (cloud) is beschikbaar in uw regio. Voor informatie over de beschikbaarheid van de EDR-expert (cloud) infrastructuur in uw regio kunt u contact opnemen met de Technische Support.
- OSMP (Open Single Management Platform) is geïnstalleerd.
- Kaspersky Endpoint Security geïnstalleerd in standaardmodus.
- Het Kaspersky Endpoint Security-programma is geactiveerd en de functionaliteit valt onder de licentie.
- U hebt de voorwaarden van de Kaspersky Endpoint Detection and Response Expert (cloud) Overeenkomst voor gegevensverwerking geaccepteerd.
- Endpoint Detection and Response Expert (cloud) – het component is ingeschakeld.

- Programmaonderdelen die zorgen voor de werking van EDR Expert (cloud) zijn ingeschakeld en operationeel.
  - File Threat Protection.
  - Web Threat Protection.
  - Mail Threat Protection.
  - Exploit-preventie.
  - Gedragsdetectie.
  - Host Intrusion Prevention.
  - Remediation Engine.
  - Adaptieve controle op afwijkingen.

Stappen voor integratie met EDR Expert (cloud)

Het opzetten van de EDR Expert (cloud) integratie omvat de volgende stappen:

1. **Het onderdeel installeren Endpoint Detection and Response Expert (cloud)**

   U kunt het onderdeel Endpoint Detection and Response Expert (cloud) selecteren tijdens: installatie of upgrade, alsook tijdens het gebruik van de taak *Programmaonderdelen wijzigen*.

   > U moet uw computer opnieuw opstarten om de upgrade van het programma met het nieuwe onderdeel te voltooien.

2. **Kaspersky Endpoint Detection and Response Expert (cloud) activeren**

   Voor Kaspersky Endpoint Detection and Response Expert (cloud) moet u een aparte licentie aanschaffen.

   De functie wordt beschikbaar na toevoeging van een afzonderlijke sleutel voor Kaspersky Endpoint Detection and Response Expert (cloud). Als resultaat worden er twee sleutels op de computer toegevoegd: een sleutel voor Kaspersky Endpoint Security en een sleutel voor Kaspersky Endpoint Detection and Response Expert (cloud).

   Licenties voor de zelfstandige Endpoint Detection and Response Expert (cloud) functionaliteit is hetzelfde als de licentie van Kaspersky Endpoint Security.

   Zorg ervoor dat de EDR Export (cloud)-functionaliteit is inbegrepen in de licentie en wordt uitgevoerd in de lokale interface van het programma.

3. **Verbinding maken met de server voor het verzamelen van telemetriegegevens en de responsserver**

   Kaspersky Endpoint Detection and Response Expert (cloud) vereist een vertrouwde verbinding tussen Kaspersky Endpoint Security en twee servers:

   - Een *telemetrieverzamelingsserver* is een server die deel uitmaakt van een SIEM oplossing die informatie over gebeurtenissen op de computer verzamelt, normaliseert, correleert, analyseert en opslaat.
   - Een *responsservers* is een server voor het ontvangen en scannen van gegevens, het bestuderen van het gedrag van objecten en het publiceren van de resultaten van dergelijke onderzoeken.

Een Kaspersky Endpoint Security-computer verbinden met EDR Expert (cloud) via de webconsole

1. Selecteer in het hoofdvenster van de Webconsole het tabblad **Asset management** → **Policies**.
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 **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (cloud)**.
5. Schakel het onderdeel in met de **Endpoint Detection and Response Expert (cloud) DISABLED** schakelaar.
6. Als het huidige beleid een onderliggend beleid is en het bovenliggende beleid verbiedt wijzigingen in de instellingen van de EDR-expert (cloud)-integratie (gesloten "hangslot"), kunt u de overname van instellingen configureren in de sectie **Inheritance**:

   - **Inherit connection settings from the policy** (standaardwaarde). De verbindingsinstellingen worden overgenomen van het bovenliggende beleid. U kunt de instellingen niet bewerken.
   - **Use custom connection settings**. U kunt de verbindingsinstellingen handmatig configureren.
7. Het tabblad **Response server** toont de volledig gekwalificeerde domeinnaam en poort van de responsserver, die automatisch worden opgehaald. Als het beveiligingsbeleid in uw infrastructuur niet toestaat dat u rechtstreeks verbinding maakt met servers van de EDR-expert (cloud), kunt u een verbinding via een TCP-tunnel tot stand brengen:

   a. Selecteer het selectievakje **Use a TCP tunnel for response**.

   b. Geef het serveradres (IPv4, IPv6) en de poort op om verbinding te maken met de tunnel.
8. Stel indien nodig de frequentie van de verzending van synchronisatieverzoeken naar de server in het veld **Send sync request to server every (min)**. Tijdens de synchronisatie ontvangt Kaspersky Endpoint Security responstaken op dreigingen en verstuurt het de resultaten van de taken.
9. Ga naar het tabblad **Telemetry collection server**.
10. Configureer de verbindingsinstellingen van de telemetrieverzamelingsserver:

    a. Klik op de koppeling **Edit**.

    b. Selecteer in het geopende venster de server voor het verzamelen van telemetriegegevens in de lijst. De KUMA-collector fungeert als de server voor het verzamelen van telemetriegegevens in EDR-expert (cloud). Raadpleeg voor meer informatie de Help van Kaspersky Unified Monitoring and Analysis Platform.

    Als er een fout optreedt tijdens het verbinden met de telemetrieverzamelingsserver, selecteer dan een andere server. Als u geen verbinding kunt maken met de telemetrieserver, neem dan contact op met de Technical Support.

    c. Indien nodig kunt u een verbinding met de telemetrieverzamelingsserver configureren via een TCP-tunnel, net zoals u zou doen voor de responsserver.
11. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Als gevolg hiervan wordt de computer toegevoegd aan de lijst met beheerde apparaten op het Open Single Management Platform (OSMP). Controleer de werkingsstatus van het onderdeel door het *Report on status of application components* 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 Expert (cloud)** wordt toegevoegd aan de lijst met Kaspersky Endpoint Security-onderdelen.

Instellingen voor EDR Expert (cloud) telemetrie configureren

Telemetrie is een lijst met gebeurtenissen die hebben plaatsgevonden op de beveiligde computer. Kaspersky Endpoint Security analyseert telemetriegegevens en verzendt deze tijdens synchronisatie naar telemetrieverzamelservers. Telemetriegebeurtenissen komen bijna continu op de server aan. Kaspersky Endpoint Security start de synchronisatie met de server wanneer aan een van de volgende voorwaarden is voldaan:

- Het synchronisatie-interval is vervallen.
- Het aantal gebeurtenissen in de buffer overschrijdt de bovengrens.

Daarom synchroniseert het programma standaard elke 30 seconden of wanneer de buffer 1024 gebeurtenissen bevat. U kunt het synchronisatiegedrag configureren in het Kaspersky Endpoint Security-beleid en optimale waarden selecteren die overeenkomen met uw netwerkbelasting (zie onderstaande instructies).

Als er geen verbinding is tussen Kaspersky Endpoint Security en de server, plaatst het programma nieuwe gebeurtenissen in de wachtrij. Wanneer de verbinding hersteld is, stuurt Kaspersky Endpoint Security gebeurtenissen in de wachtrij in de juiste volgorde naar de server. Om overbelasting van de server te voorkomen, kan Kaspersky Endpoint Security bepaalde gebeurtenissen overslaan. Hiervoor kunt u de instellingen voor gebeurtenisoverdracht optimaliseren zoals een maximale waarde voor gebeurtenissen per uur (zie onderstaande instructies).

Voer de volgende stappen uit om telemetrie-instellingen te configureren.

1. Selecteer in het hoofdvenster van de Webconsole het tabblad **Asset management** → **Policies**.
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 **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (cloud)**.
5. Selecteer in het geopende venster het tabblad **Data transmission settings**.
6. Zorg ervoor dat het selectievakje **Sending telemetry ENABLED** ingeschakeld is.
7. Schakel indien nodig het selectievakje **Send telemetry with IOA only** in. *Indicator van aanval (IOA)* is een regel die een beschrijving bevat van verdacht gedrag in het systeem dat kan wijzen op een gerichte aanval. Het programma vergelijkt het gedrag in het systeem met deze regels en registreert gebeurtenissen die wijzen op een gerichte aanval. Het programma gebruikt de *streaming scan*technologie die het mogelijk maakt om dergelijke gebeurtenissen in realtime bij te houden.

8. Configureer indien nodig de instellingen voor serversynchronisatie:

   - **Maximum event transmission delay (sec)**. Het programma synchroniseert met de server om gebeurtenissen te verzenden nadat het synchronisatie-interval is verlopen. De standaardinstelling is 30 seconden.

   - **Maximum number of event packages**. Het programma synchroniseert met de server wanneer de buffer gevuld is met gebeurtenissen. De standaardinstelling is 1024 gebeurtenissen.

9. Ga naar het tabblad **Request throttling**.

10. Schakel indien nodig de beperking van aanvragen uit met de **Request throttling ENABLED**-schakelaar.

    Dit helpt de belasting op de server te optimaliseren. Als deze functionaliteit is ingeschakeld, beperkt het programma de verzending van gebeurtenissen. Als het aantal gebeurtenissen de ingestelde limieten overschrijdt, stopt Kaspersky Endpoint Security met het verzenden van gebeurtenissen. Deze optie is standaard ingeschakeld.

11. Configureer optimalisatie-instellingen voor het verzenden van gebeurtenissen naar de server:

    - **Maximum number of events per hour**. Het programma analyseert de telemetriegegevensstroom en beperkt het verzenden van gebeurtenissen als de gebeurtenisstroom de geconfigureerde limiet voor gebeurtenissen per uur overschrijdt. Kaspersky Endpoint Security hervat het verzenden van gebeurtenissen na een uur. De standaardinstelling is 3000 gebeurtenissen per uur. Als het programma op een server is geïnstalleerd, is de telemetrie gegevensstroom hoger. Voor servers wordt aanbevolen om de waarde te verhogen tot 60 000 gebeurtenissen per uur.

    - **Percentage of event limit excess (%)**. Het programma sorteert gebeurtenissen op type (bijvoorbeeld 'wijzigingen in het register'-gebeurtenissen) en beperkt de overdracht van gebeurtenissen als de verhouding tussen gebeurtenissen van hetzelfde type en het totale aantal gebeurtenissen de geconfigureerde limiet overschrijdt. Kaspersky Endpoint Security hervat het verzenden van gebeurtenissen wanneer de verhouding tussen andere gebeurtenissen en het totale aantal gebeurtenissen opnieuw groot genoeg is. De standaardinstelling is 15 %.

12. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Uitzonderingen voor telemetrie van EDR Expert (cloud)

Om de prestaties te verbeteren en de gegevensoverdracht naar de telemetrieverzamelingsservers te optimaliseren, kunt u uitzonderingen voor telemetrie toevoegen. U kunt er bijvoorbeeld voor kiezen om geen gegevens voor netwerkcommunicaties voor individuele programma's te verzenden.

Het gebruik van te veel regels kan de belasting van de telemetrieverzamelingsserver verhogen en de prestaties van de computer verminderen. We raden u aan om alleen noodzakelijke regels toe te voegen.

Een telemetrie-uitzondering maken in de Webconsole en de Cloudconsole:

1. Selecteer in het hoofdvenster van de Webconsole het tabblad **Asset management** → **Policies**.

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** → **Telemetry Settings**.

5. Selecteer het tabblad **EDR Expert (cloud) telemetry**.

6. In het blok **General exclusions**, klikt u op de knop **Add**.

   Het venster **Add exclusion rule** wordt geopend.

7. Wijzig indien nodig de status van de regel. De regel is standaard ingeschakeld.

8. Voer een naam voor de regel in.

9. Selecteer de actie die moet worden uitgevoerd wanneer de regel wordt geactiveerd:

   - **Do not collect**. De gefilterde gebeurtenis wordt uitgesloten van de verzonden telemetrie.
   - **Exclude IOA**. De gebeurtenis die de IOA-regel activeert, wordt uitgezonderd van de verzonden telemetrie.

10. Als de **Exclude IOA** optie is geselecteerd, geeft u de IOA-regels op die aan uitzonderingen moeten worden toegevoegd:

    - **Exclude all**. Wanneer aan de opgegeven voorwaarde is voldaan, sluit het programma gebeurtenissen uit die zijn gegenereerd op basis van alle IOA-regels van de telemetrie.
    - **Exclude by GUID**. Geef de GUID van de IOA-regel op. U kunt meerdere GUID's opgeven met `,`. Voor meer informatie over de IOA-regels raadpleeg de: Help van EDR-expert (cloud).

11. Geef de filtervoorwaarde op:

    a. Selecteer de veldnaam die moet worden gebruikt voor het filteren.

    b. Selecteer een operator (zie de tabel hieronder) en geef de waarde op waarmee de veldwaarde van de gebeurtenis wordt vergeleken.

Lijst met voorwaardelijke operators

Operator	Beschrijving
<	Als de veldwaarde kleiner is dan de waarde die is opgegeven in de voorwaarde, wordt de gebeurtenis uitgefilterd.
≤	Als de veldwaarde kleiner is dan of gelijk is aan de waarde die is opgegeven in de voorwaarde, wordt de gebeurtenis uitgefilterd.
=	Als de waarde van het veld gelijk is aan de waarde die is opgegeven in de voorwaarde, wordt de gebeurtenis uitgefilterd.
≥	Als de waarde van het veld groter is dan of gelijk is aan de waarde die is opgegeven in de voorwaarde, wordt de gebeurtenis uitgefilterd.
>	Als de veldwaarde groter is dan de waarde die is opgegeven in de voorwaarde, wordt de gebeurtenis uitgefilterd.
≠	Als de waarde van het veld niet gelijk is aan de waarde die is opgegeven in de voorwaarde, wordt de gebeurtenis uitgefilterd.
is like	Als de veldwaarde overeenkomt met het masker dat is opgegeven in de voorwaarde, wordt de gebeurtenis uitgefilterd. Het programma ondersteunt de `*` en `?` tekens bij het invoeren van een masker:
is not like	Als de veldwaarde niet overeenkomt met het masker dat is opgegeven in de voorwaarde, wordt de gebeurtenis uitgefilterd. Het programma ondersteunt de `*` en `?` tekens bij het invoeren van een masker:
one of	Als de veldwaarde overeenkomt met een van de waarden in de lijst die is opgegeven in de voorwaarde, wordt de gebeurtenis uitgefilterd.
none of	Als de veldwaarde niet overeenkomt met een van de waarden in de lijst die in de voorwaarde is opgegeven, wordt de gebeurtenis uitgefilterd.
is like one of	Als de veldwaarde overeenkomt met een van de opgegeven maskers in de voorwaarde, wordt de gebeurtenis uitgefilterd. Het programma ondersteunt de * en ? tekens wanneer u een masker invoert.

Operator	Beschrijving
is not like one of	Als de veldwaarde niet overeenkomt met een van de opgegeven maskers in de voorwaarde, wordt de gebeurtenis uitgefilterd. Het programma ondersteunt de * en ? tekens wanneer u een masker invoert.
exists	Als het opgegeven veld in de voorwaarde aanwezig is in de gebeurtenis, wordt de gebeurtenis uitgefilterd.
not exists	Als het opgegeven veld in de voorwaarde niet aanwezig is in de gebeurtenis, wordt de gebeurtenis uitgefilterd.
contains	Als de opgegeven waarde in de voorwaarde aanwezig is in de veldwaarde, wordt de gebeurtenis uitgefilterd.
is equal to	Als de waarde van het veld gelijk is aan de waarde die is opgegeven in de voorwaarde, wordt de gebeurtenis uitgefilterd. De scan is niet hoofdlettergevoelig.
bitwise AND	Als het resultaat van de Bitwise AND (&)-bewerking tussen de veldwaarde en de opgegeven waarde in de voorwaarde 1 is, wordt de gebeurtenis uitgefilterd.

12. Indien nodig kunt u complexe filtercriteria maken door meerdere filtervoorwaarden en groepen voorwaarden toe te voegen. U kunt ook geneste voorwaarden en voorwaardegroepen toevoegen aan een voorwaardegroep. U kunt de volgende operators gebruiken:

    - **AND** betekent dat het filter gebeurtenissen selecteert die aan alle opgegeven voorwaarden voldoen.
    - **OR** betekent dat het filter gebeurtenissen selecteert die aan een van de opgegeven voorwaarden voldoen.
    - **NOT** (om deze operator te gebruiken, selecteer de optie **Add NOT before**) betekent dat de filter gebeurtenissen selecteert die niet aan een van de opgegeven voorwaarden voldoen.

    Voorwaarden en voorwaardegroepen op het eerste niveau worden gecombineerd met de **AND** operator.

13. Als u de gemaakte filterregel wilt scannen, klik op de knop **Check rule**.

    In het geopende venster wordt een tabel met gebeurtenissen weergegeven die zijn gefilterd op de gemaakte regel. Voor meer details, raadpleeg de Help van EDR-expert (cloud).

14. Indien nodig, onder **All event types**, voeg telemetrie-uitzonderingen toe op de type gebeurtenis.

    a. Klik op de naam van het gebeurtenistype.

    b. Klik in het venster op de knop **Set up manually**.

    c. Configureer indien nodig de verzending van telemetrie voor het geselecteerde type gebeurtenis met de **Send event** schakelaar. Standaard is verzending van telemetrie ingeschakeld voor alle gebeurtenistypen.

    d. In het blok **Exclusion rules**, klikt u op de knop **Add**.

    Het venster **Add exclusion rule** wordt geopend.

    e. Voer de acties uit die worden beschreven in stap 7–13 voor elke regel die u toevoegt.

15. Voor sommige gebeurtenistypen kunt u ook opnameregels toevoegen om de verzamelde telemetrie uit te breiden:

    a. In het blok **Inclusion rules**, klikt u op de knop **Add**.

    Het venster **Add inclusion rules** wordt geopend.

    b. Voer een naam voor de regel in.

    c. Onder **Condition**, voert u waarden voor de weergegeven velden in. Het type beschikbare velden hangt af van de geselecteerde gebeurtenis.

Uitzonderingsregels krijgen voorrang op opnameregels.

16. Als u het beleid wilt toepassen op computers, zorg er dan voor dat dat de hangsloten dicht zijn (🔒) en u uw wijzigingen opslaat.

EDR Expert (cloud) gebeurtenisfilters exporteren en importeren

U kunt de lijst met uitzonderingen exporteren naar een JSON-bestand. Vervolgens kunt u het bestand aanpassen om bijvoorbeeld een groot aantal gebeurtenis-ID's toe te voegen. U kunt ook de export/import-functie gebruiken om een back-up te maken van de gebeurtenisfilters, of om de lijst naar een andere server te migreren.

Het gebruik van te veel regels kan de belasting van de telemetrieverzamelingsserver verhogen en de prestaties van de computer verminderen. We raden u aan om alleen noodzakelijke regels toe te voegen.

Gebeurtenisfilters in de Webconsole exporteren of importeren

1. Selecteer in het hoofdvenster van de Webconsole het tabblad **Asset management** → **Policies**.
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** → **Telemetry Settings**.
5. Selecteer het tabblad **EDR Expert (cloud) telemetry**.
6. Om de gebeurtenisfilters te exporteren:
   a. Klik op **Export**.
   b. Geef in het geopende venster de naam van het JSON-bestand op waarnaar u de gebeurtenisfilters wilt exporteren. Selecteer vervolgens de map waarin u dit bestand wilt opslaan.
   c. Sla het bestand op.

      Kaspersky Endpoint Security exporteert de gebeurtenisfilters naar het JSON-bestand.
7. Om de gebeurtenisfilters te importeren:
   a. Klik op **Import**.
   b. Selecteer in het venster dat opent het JSON-bestand waaruit u de gebeurtenisfilters wilt importeren.
   c. Selecteer hoe u regels voor het filteren van gebeurtenissen wilt importeren: door deze toe te voegen aan bestaande regels of door bestaande regels te verwijderen en te vervangen door nieuwe.
   d. Open het bestand.

8. Als u het beleid wilt toepassen op computers, zorg er dan voor dat de hangsloten dicht zijn (🔒) en u uw wijzigingen opslaat.

    1. Selecteer in het hoofdvenster van de Webconsole het tabblad **Asset management** → **Policies**.
    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** → **Telemetry Settings**.
    5. Selecteer het tabblad **EDR Expert (cloud) telemetry**.
    6. Om de gebeurtenisfilters te exporteren:

        a. Klik op **Export**.

        b. Geef in het geopende venster de naam van het JSON-bestand op waarnaar u de gebeurtenisfilters wilt exporteren. Selecteer vervolgens de map waarin u dit bestand wilt opslaan.

        c. Sla het bestand op.

           Kaspersky Endpoint Security exporteert de gebeurtenisfilters naar het JSON-bestand.
    7. Om de gebeurtenisfilters te importeren:

        a. Klik op **Import**.

        b. Selecteer in het venster dat opent het JSON-bestand waaruit u de gebeurtenisfilters wilt importeren.

        c. Selecteer hoe u regels voor het filteren van gebeurtenissen wilt importeren: door deze toe te voegen aan bestaande regels of door bestaande regels te verwijderen en te vervangen door nieuwe.

        d. Open het bestand.
    8. Als u het beleid wilt toepassen op computers, zorg er dan voor dat de hangsloten dicht zijn (🔒) en u uw wijzigingen opslaat.

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 wanneer het is geïntegreerd met Kaspersky Detection and Response-oplossingen. 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, Kaspersky Endpoint Detection and Response Expert Help, Kaspersky Anti Targeted Attack Platform Help, en Kaspersky Endpoint Detection and Response Expert (on-premises) Help.

Kaspersky Endpoint Security gebruikt het systeemaccount (SYSTEEM) om bestanden in quarantaine te plaatsen.

U kunt quarataine-instellingen alleen beheren in de Kaspersky Security Center-console. U kunt ook Kaspersky Security Center-console 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 1024 MB. Wanneer Quarantaine de maximale grootte bereikt, stopt Kaspersky Endpoint Security met het verzenden van de bestanden en maakt het de *Onvoldoende ruimte in Quarantaine*-gebeurtenis aan. Om te voorkomen dat de schijfruimte voor quarantaine opraakt, kunt u een drempel instellen waarop Kaspersky Endpoint Security een *Quarantaine heeft bijna geen vrije ruimte meer*-gebeurtenis aanmaakt. U kunt geen bewaarperiode voor bestanden in quarantaine configureren om ze automatisch te laten verwijderen.

Als de Kaspersky Anti Targeted Attack Platform (EDR)-oplossing in uw organisatie geïmplementeerd is, raden we aan om de quarantaine te vergroten. Bij het uitvoeren van een YARA-scan kan het programma een grote geheugendump ondervinden. Als de geheugendump groter is dan de quarantaine, eindigt de YARA-scan met een fout en wordt de geheugendump niet in quarantaine geplaatst. We raden aan om de grootte van de Quarantaine gelijk te stellen aan de totale grootte van het RAM-geheugen op de computer (bijvoorbeeld 8 GB), of om de groottebeperking van Quarantaine uit te schakelen.

Maximale quarantainegrootte configureren in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Algemene instellingen** → **Rapporten en Opslag** in het beleidsvenster.
4. Configureer de **Quarantaine** grootte in het quarantaineblok:
   - **Beperk grootte van quarantaine tot N MB**. Als het selectievakje is ingeschakeld, is de maximale Quarantainegrootte beperkt tot de opgegeven waarde. De maximale grootte is standaard 1024 MB. Wanneer Quarantaine de maximale grootte bereikt, stuurt Kaspersky Endpoint Security de gebeurtenis *Onvoldoende ruimte in Quarantaine* 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.

     Als het selectievakje is uitgeschakeld, wordt de grootte van de Quarantaine beperkt door de beschikbare vrije schijfruimte.

   - **Meld wanneer de quarantaineopslag bereikt is N procent**. 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.

     Als dit selectievakje is uitgeschakeld, maakt het programma geen gebeurtenissen aan wanneer de drempel voor quarantaine is bereikt.

5. Sla uw wijzigingen op.

Maximale Quarantainegrootte configureren in de Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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** → **Reports and Storage**.
5. Configureer de **Quarantine** grootte in het quarantaineblok:

   - **Limit the size of Quarantine**. Als het selectievakje is ingeschakeld, wordt de Quarantainegrootte beperkt tot de opgegeven waarde. Als het selectievakje is uitgeschakeld, wordt de grootte van de Quarantaine beperkt door de beschikbare vrije schijfruimte. Dit kan nodig zijn voor: YARA-scans omdat het programma een groot geheugendumpbestand kan opslaan.
   - **Maximum size of Quarantine (MB)**. Als het selectievakje is ingeschakeld, is de maximale Quarantainegrootte beperkt tot de opgegeven waarde. De maximale grootte is standaard 1024 MB. Wanneer Quarantaine de maximale grootte bereikt, stuurt Kaspersky Endpoint Security de gebeurtenis *Onvoldoende ruimte in Quarantaine* 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.

     Als het selectievakje is uitgeschakeld, wordt de grootte van de Quarantaine beperkt door de beschikbare vrije schijfruimte.
   - **Notify when the Quarantine storage reaches (%)**. 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.
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 gegevens over bestanden in quarantaine inschakelen in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Algemene instellingen** → **Rapporten en Opslag** in het beleidsvenster.
4. In het blok **Gegevensoverdracht naar Administration Server**, klikt u op de knop **Instellingen**.

5. Selecteer in het venster dat opent het selectievakje **Quarantainebestanden**.
6. Sla uw wijzigingen op.

De overdracht van gegevens over bestanden in quarantaine inschakelen in de Webconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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** → **KSC Integration**.
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 een lijst met bestanden bekijken die op uw computer in quarantaine zijn geplaatst in de Kaspersky Security Center Console. U kunt ook de Kaspersky Security Center-console gebruiken om objecten in quarantaine te beheren (terugzetten, verwijderen, toevoegen, etc.). Voor meer informatie over het werken met Quarantaine raadpleegt u de Help van Kaspersky Security Center.

Bestanden terugzetten vanuit quarantaine

Kaspersky Endpoint Security zet bestanden terug naar hun oorspronkelijke map. Als de doelmap is verwijderd of als de gebruiker geen toegangsrechten tot die map heeft, plaatst het programma het bestand in de map `%DataRoot%\QB\Restored`. Daarna moet u het bestand handmatig naar de bestemmingsmap verplaatsen.

Bestanden terugzetten vanuit quarantaine:

1. Selecteer in het hoofdvenster van de webconsole **Operations** → **Repositories** → **Quarantine**.
2. Hiermee opent u de lijst met bestanden in quarantaine. Selecteer in die lijst de bestanden die u wilt terugzetten en klik op **Restore**.

   Kaspersky Endpoint Security zet dit bestand terug. Als de doelmap al een bestand met dezelfde naam heeft, annuleert het programma het terugzetten van het bestand. Voor EDR Optimum- en EDR Expert-oplossingen verwijdert het programma het bestand na herstel. Voor andere oplossingen bewaart het programma een kopie van het bestand in Quarantaine.

EDR-acties bewaken

Kaspersky Endpoint Security for Windows 12.9 introduceert het EDR action monitoring center. de *EDR action monitoring center* is een console waarin u de geschiedenis van Threat Response voor alle Kaspersky Detection and Response-oplossingen kunt bekijken. Als uw organisatie meerdere Detection and Response heeft geïmplementeerd (bijvoorbeeld EDR Optimum en MDR), toont Kaspersky Endpoint Security de geschiedenis van Threat Response voor alle oplossingen. Zo kunt u de prestaties van Detection and Response-oplossingen op een aparte computer analyseren en de instellingen van deze oplossingen optimaliseren.

Het monitoring center geeft de volgende informatie:

- Informatie over taken voor Threat Response (bijvoorbeeld de taak *Proces beëindigen*)
- Wijzigingen in de regels voor netwerkisolatie en uitvoeringspreventie

Als de dreigingsreactie een fout ondervindt met betrekking tot de toegang tot een netwerkshare, wordt een dergelijke fout weggelaten uit de weergegeven geschiedenis van Threat Response.

Zo navigeert u naar het EDR Action Monitoring Center:

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Assets (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** → **Response history**.

   Hiermee opent u de console van het EDR Action Monitoring Center. U kunt de console gebruiken om de taakstatussen voor Threat Response, de duur van de taak, wijzigingen in regels en details van de initiator te bekijken.

Kaspersky Unified Monitoring and Analysis Platform (KUMA)



Kaspersky Endpoint Security voor Windows ondersteunt de Kaspersky Unified Monitoring and Analysis Platform-oplossing. *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* is een security information and event management (SIEM) oplossing voor de IT-infrastructuur van organisaties. Met KUMA kunnen beveiligingsbedreigingen worden gedetecteerd, geanalyseerd en beperkt voordat ze schade kunnen veroorzaken.

Het programma Kaspersky Endpoint Security 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 (telemetriegegevens) wordt verzonden naar de Kaspersky Unified Monitoring and Analysis Platform (KUMA)-server. In de console geeft KUMA gebeurtenissen weer als een lijst zonder opmaak, vergelijkbaar met het Windows-gebeurtenislogboek.

Kaspersky Endpoint Security biedt niet alle functionaliteit van een agent voor KUMA. Het programma stuurt alleen gebeurtenissen naar KUMA zonder opmaak. Om toegang te krijgen tot alle KUMA-functionaliteit, moet u een licentie kopen en de oplossing implementeren in overeenstemming met de KUMA Beheerdersgids.

Integratie van Kaspersky Endpoint Security met KUMA

Voor het gebruik van KUMA moet aan de volgende voorwaarden worden voldaan:

- Kaspersky Security Center versie 14.2 of hoger. In eerdere versies van Kaspersky Security Center is het onmogelijk om de KUMA-functionaliteit te activeren.
- Het programma is geactiveerd en de functionaliteit valt onder de licentie.
- Het onderdeel KUMA-integratie wordt ingeschakeld.

Het opzetten van KUMA-integratie omvat de volgende stappen:

1. **Het onderdeel KUMA-integratie installeren**

   U kunt het onderdeel KUMA-inegratie selecteren tijdens: installeren of upgraden van het programma, alsook tijdens het gebruik van de taak *Programmaonderdelen wijzigen*.

   U moet uw computer opnieuw opstarten om de upgrade van het programma met het nieuwe onderdeel te voltooien.

2. **KUMA-activering**

   Naast een Kaspersky Endpoint Security programmalicentie (bijvoorbeeld Kaspersky Endpoint Security for Business Standard), heeft u een aparte licentie nodig voor de integratie van Kaspersky Endpoint Security met KUMA (Kaspersky Endpoint Security for Windows KUMA Integration Add-on).

Als u het programma in de EDR Agent-modus installeert, hebt u een licentie nodig voor de integratie van Kaspersky Endpoint Security met KUMA en een Kaspersky Anti Targeted Attack Platform (KATA)-licentie of een Kaspersky Managed Detection and Response (MDR)-licentie. U kunt EDR Agent niet alleen voor KUMA implementeren.

De functionaliteit komt beschikbaar na het toevoegen van de afzonderlijke KUMA-sleutel. Als gevolg hiervan zal er nog een actieve licentie op de computer aanwezig zijn voor de integratie van Kaspersky Endpoint Security met KUMA.

Licenties voor de zelfstandige KUMA-functionaliteit zijn hetzelfde als de licenties van Kaspersky Endpoint Security.

Zorg ervoor dat de KUMA-functionaliteit is inbegrepen in de licentie en werkt in de lokale interface van het programma.

3 **Verbinding maken met KUMA**

Om de computer met de Kaspersky Endpoint Security-programma te verbinden met de KUMA-oplossing:

1. Voeg in het Kaspersky Endpoint Security-beleid KUMA-serveradressen toe en geef de netwerkinstellingen van de verbinding op.

2. Voeg in de KUMA-console een collector toe met connectoren van het type tcp of udp en geef de basisnetwerkinstellingen van de verbinding op. Raadpleeg de Help van Kaspersky Unified Monitoring and Analysis Platform voor meer informatie over het beheren van verzamelprogramma's.

U kunt een vertrouwde verbinding tot stand brengen tussen Kaspersky Endpoint Security en KUMA-servers. Gebruik een TLS-certificaat om een vertrouwde verbinding te configureren. U kunt een TLS-certificaat krijgen op de KUMA Core-server (zie de instellingen voor de tcp-type connector in de Hulp bij Kaspersky Unified Monitoring and Analysis Platform). Vervolgens moet u het TLS-certificaat toevoegen aan Kaspersky Endpoint Security (zie onderstaande instructies).

Om de verbinding veiliger te maken, kunt u bovendien de verificatie van de computer op KUMA (twee-weg verificatie) inschakelen. Als u deze verificatie wilt inschakelen, moet u twee-weg verificatie inschakelen in de instellingen KUMA en Kaspersky Endpoint Security. Om twee-weg verificatie te gebruiken hebt u ook een crypto-container nodig. Een *crypto-container* is een PFX-archief met een certificaat en een privésleutel. U moet een certificaat genereren met de persoonlijke sleutel in de containerformaat PKCS#12 bij een externe certificeringsinstantie. Vervolgens moet u het PFX-archief toevoegen in de KUMA-console en in Kaspersky Endpoint Security (zie de instellingen voor de tcp-type connector in de Hulp bij Kaspersky Unified Monitoring and Analysis Platform).

Een Kaspersky Endpoint Security-computer verbinden met KUMA via de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.

2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

3. Selecteer in het beleidsvenster **KUMA-integratie**.

4. Selecteer het selectievakje **KUMA-integratie**.

5. Schakel in het blok **Integratie instellingen** het selectievakje **$IsKUMATelemetry ? "Overdracht van Windows-evenementen naar een KUMA-server inschakelen": "Overdracht van Windows-evenementen naar een SIEM-server inschakelen** in.

6. Schakel indien nodig het selectievakje in naast **Gebruik TLS-encryptie** in het blok **Instellingen om met KUMA-servers te verbinden**.

7. Configureer de vertrouwde verbinding:

   a. Klik op **Instellingen om met KUMA-servers te verbinden**.

   b. Configureer de serververbinding:

   - **Time-out (sec.)**. Maximale time-out voor de serverrespons van KUMA. Wanneer de time-out is verstreken, probeert Kaspersky Endpoint Security verbinding te maken met een andere KUMA-server.

   - **Server TLS certificaat**. TLS-certificaat voor het tot stand brengen van een vertrouwde verbinding met de KUMA-server. U kunt een TLS-certificaat verkrijgen in de console van Kaspersky Unified Monitoring and Analysis Platform (zie de instructies in Kaspersky Unified Monitoring and Analysis Platform).

     Om een vertrouwde verbinding tot stand te brengen, moet u in de KUMA-console, in de instellingen van de tcp-connector, de **With verification** TLS-modus (zie de instellingen voor de tcp-type connector in de Hulp bij Kaspersky Unified Monitoring and Analysis Platform).

   - **Gebruik twee-weg verificatie**. Tweerichtingsverificatie bij het tot stand brengen van een beveiligde verbinding tussen Kaspersky Endpoint Security en KUMA. Om tweerichtingsverificatie te gebruiken, moet u in de KUMA-console, in de instellingen van de tcp-connector, de **Custom PFX** TLS-modus (zie de instellingen voor de tcp-type connector in de Hulp bij Kaspersky Unified Monitoring and Analysis Platform). Dan moet u een cryptocontainer aanschaffen en een wachtwoord instellen om de cryptocontainer te beschermen. Een *crypto-container* is een PFX-archief met een certificaat en een privésleutel. Na het configureren van de KUMA-instellingen, moet u ook tweerichtingsverificatie inschakelen in de instellingen van Kaspersky Endpoint Security en een met een wachtwoord beveiligde crypto-container laden.

     > De crypto-container moet met een wachtwoord worden beveiligd. Het is niet mogelijk om een crypto-container toe te voegen met een leeg wachtwoord.

   c. Klik op **OK**.

8. Voeg KUMA-servers toe:

   a. Klik op **Toevoegen**.

   Hiermee opent u het formulier waarin u een KUMA-server kunt toevoegen.

   b. Selecteer het protocol om verbinding te maken met KUMA-servers: **HTTP / HTTPS**, **TCP**, **UDP**.

   Als u de **HTTP / HTTPS** protocol selecteert gebruikt het programma standaard HTTPS voor de verbinding met KUMA-servers. Als u HTTP wilt gebruiken, moet u dit protocol handmatig opgeven in het serveradres (bijvoorbeeld `http://server.com`).

   c. Voer het serveradres (IPv4, IPv6) en de poort in om verbinding te maken met de server.

   d. Klik op **OK**.

Kaspersky Endpoint Security maakt verbinding met de eerste KUMA-server in de lijst. Als de verbinding mislukt, maakt Kaspersky Endpoint Security verbinding met de tweede KUMA-server in de lijst, enzovoort.

9. Configureer indien nodig de instelling **Maximale vertraging gebeurtenisoverdracht (sec)** in het blok **Data-overdrachtsinstellingen**. Wanneer de opgegeven tijd om is, probeert Kaspersky Endpoint Security verbinding te maken met dezelfde server of maakt verbinding met de volgende server in de lijst als er meerdere servers zijn. De standaardinstelling is 30 seconden.

10. Sla uw wijzigingen op.

Een Kaspersky Endpoint Security-computer verbinden met KUMA via de webconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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 **Built-in Agents Configuration** → **KUMA Integration**.

5. Zet de schakelaar **KUMA Integration ENABLED** aan.

6. Schakel indien nodig de optie **Use TLS encryption** in bij de instellingen voor de **Server connection settings**.

7. Configureer de vertrouwde verbinding:

   a. Klik op **Connection settings**.

   b. Configureer de serververbinding:

   - **Timeout (sec)**. Maximale time-out voor de serverrespons van KUMA. Wanneer de time-out is verstreken, probeert Kaspersky Endpoint Security verbinding te maken met een andere KUMA-server.

   - **Server TLS certificate**. TLS-certificaat voor het tot stand brengen van een vertrouwde verbinding met de KUMA-server. U kunt een TLS-certificaat verkrijgen in de console van Kaspersky Unified Monitoring and Analysis Platform (zie de instructies in Kaspersky Unified Monitoring and Analysis Platform).

     Om een vertrouwde verbinding tot stand te brengen, moet u in de KUMA-console, in de instellingen van de tcp-connector, de **With verification** TLS-modus (zie de instellingen voor de tcp-type connector in de Hulp bij Kaspersky Unified Monitoring and Analysis Platform).

   - **Use two-way authentication**. Tweerichtingsverificatie bij het tot stand brengen van een beveiligde verbinding tussen Kaspersky Endpoint Security en KUMA. Om tweerichtingsverificatie te gebruiken, moet u in de KUMA-console, in de instellingen van de tcp-connector, de **Custom PFX** TLS-modus (zie de instellingen voor de tcp-type connector in de Hulp bij Kaspersky Unified Monitoring and Analysis Platform). Dan moet u een cryptocontainer aanschaffen en een wachtwoord instellen om de cryptocontainer te beschermen. Een *crypto-container* is een PFX-archief met een certificaat en een privésleutel. Na het configureren van de KUMA-instellingen, moet u ook tweerichtingsverificatie inschakelen in de instellingen van Kaspersky Endpoint Security en een met een wachtwoord beveiligde crypto-container laden.

     > De crypto-container moet met een wachtwoord worden beveiligd. Het is niet mogelijk om een crypto-container toe te voegen met een leeg wachtwoord.

   c. Klik op **OK**.

8. Voeg KUMA-servers toe:

   a. Klik op **Add**.

      Hiermee opent u het formulier waarin u een KUMA-server kunt toevoegen.

   b. Selecteer het protocol om verbinding te maken met KUMA-servers: **HTTP/HTTPS**, **TCP**, **UDP**.

      Als u de **HTTP/HTTPS** protocol selecteert gebruikt het programma standaard HTTPS voor de verbinding met KUMA-servers. Als u HTTP wilt gebruiken, moet u dit protocol handmatig opgeven in het serveradres (bijvoorbeeld `http://server.com`).

   c. Voer het serveradres (IPv4, IPv6) en de poort in om verbinding te maken met de server.

   d. Klik op **OK**.

   Kaspersky Endpoint Security maakt verbinding met de eerste KUMA-server in de lijst. Als de verbinding mislukt, maakt Kaspersky Endpoint Security verbinding met de tweede KUMA-server in de lijst, enzovoort.

9. Configureer indien nodig de instelling **Maximum delay when sending events (sec)** in het blok **Server connection settings**. Wanneer de opgegeven tijd om is, probeert Kaspersky Endpoint Security verbinding te maken met dezelfde server of maakt verbinding met de volgende server in de lijst als er meerdere servers zijn. De standaardinstelling is 30 seconden.

10. Sla uw wijzigingen op.

U kunt controleren of de KUMA-integratie correct is geconfigureerd in de KUMA-console (voor meer informatie zie Kaspersky Unified Monitoring and Analysis Platform Help). Controleer de werkingsstatus van het onderdeel door het *Report on status of application components* in de Kaspersky Security Center-console te bekijken. U kunt de werkingsstatus van een onderdeel ook in rapporten bekijken in de lokale interface van Kaspersky Endpoint Security. Het onderdeel **KUMA-integratie** wordt toegevoegd aan de lijst met Kaspersky Endpoint Security-onderdelen.

4 Het telemetrieverzending naar de KUMA-server inschakelen

Standaard is het verzenden van gebeurtenissen naar de KUMA-server uitgeschakeld. Om ervoor te zorgen dat KUMA correct werkt, moet u de verzending van telemetrie inschakelen. U kunt een gebeurtenisbron selecteren uit de standaardlogboeken: *Application*, *Security* or *System*.

Telemetrieverzending naar de KUMA-server inschakelen in de Beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de beheerconsole **Policies**.
3. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
4. Selecteer **Algemene instellingen** → **Uitzonderingen en objecttypen** in het beleidsvenster.
5. In het blok **Telemetrie-instellingen** → **KUMA-telemetrie**, klikt u op de knop **Instellingen**.
6. Selecteer gebeurtenislogboeken die u als gebeurtenisbronnen wilt gebruiken: *Application*, *Security* of *System*.

   Naast standaardlogboeken kunt u een log van een programma van derden.

7. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Verzenden van telemetriegegevens naar de KUMA-server in de Webconsole inschakelen

1. Selecteer in het hoofdvenster van de Webconsole het tabblad **Asset management** → **Policies**.
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** → **Telemetry Settings**.
5. Selecteer het tabblad **KUMA telemetry**.
6. Selecteer gebeurtenislogboeken die u als gebeurtenisbronnen wilt gebruiken: *Application*, *Security* of *System*.

   Naast standaardlogboeken kunt u een log van een programma van derden.
7. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Gebeurtenissen filteren die naar KUMA moeten worden verzonden

Standaard is het verzenden van gebeurtenissen naar de KUMA-server uitgeschakeld. Om ervoor te zorgen dat KUMA correct werkt, moet u de verzending van telemetrie inschakelen. U kunt een gebeurtenisbron selecteren uit de standaardlogboeken: *Application*, *Security* or *System*. Om de prestaties te verbeteren en de gegevensoverdracht naar de KUMA-server te optimaliseren, kunt u handmatig afzonderlijke gebeurtenissen toevoegen aan of uitsluiten van telemetrie. U kunt bijvoorbeeld Sysmon-gebeurtenissen uitsluiten.

In de Beheerdersconsole (MMC) een lijst met gebeurtenissen maken die naar KUMA moet worden verstuurt

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de beheerconsole **Policies**.
3. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
4. Selecteer **Algemene instellingen** → **Uitzonderingen en objecttypen** in het beleidsvenster.
5. In het blok **Telemetrie-instellingen** → **KUMA-telemetrie**, klikt u op de knop **Instellingen**.
6. Configureer in het weergegeven venster de gebeurtenisfilters die naar KUMA moeten worden verstuurt.

U kunt gebeurtenisfiltering configureren voor de standaard *Application*, *Security*, *System* logboeken of handmatig een ander logboek toevoegen:

a. Open de eigenschappen van het logboek of klik op de **Toevoegen** en voer de naam van het logboek in.

b. Selecteer een modus voor versturen van gebeurtenissen:

- **Alle evenementen versturen**. In deze modus verstuurt het programma alle gebeurtenissen uit het Windows-logboek, behalve gebeurtenissen die zijn toegevoegd aan uitzonderingsregels.
- **Alleen geselecteerde evenementen versturen**. In deze modus verstuurt het programma alleen gebeurtenissen die zijn toegevoegd aan inclusieregels.

c. Maak lijsten met uitzonderingsregels of opnameregels voor de relevante modus voor versturen van gebeurtenissen.

Om regels toe te voegen, moet u de ID van de gebeurtenis opgeven in het Windows-gebeurtenislogboeken. U kunt meerdere gebeurtenis-ID's in een regel opgeven. Als u meerdere gebeurtenis-ID's wilt opgeven, gebruik dan de komma (`,`).

d. Schakel indien nodig de logboekregistratie van gebeurtenissen in met behulp van het selectievakje naast de naam van het logboek.

7. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Een lijst met gebeurtenissen maken die naar KUMA moeten worden verstuurd in Webconsole

1. Selecteer in het hoofdvenster van de Webconsole het tabblad **Asset management** → **Policies**.
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** → **Telemetry Settings**.
5. Selecteer het tabblad **KUMA telemetry**.
6. Configureer in het weergegeven venster de gebeurtenisfilters die naar KUMA moeten worden verstuurt.

   U kunt gebeurtenisfiltering configureren voor de standaard *Application*, *Security*, *System* logboeken of handmatig een ander logboek toevoegen:

   a. Open de eigenschappen van het logboek of klik op de **Add** en voer de naam van het logboek in.

   b. Selecteer een modus voor versturen van gebeurtenissen:

   - **Send all events**. In deze modus verstuurt het programma alle gebeurtenissen uit het Windows-logboek, behalve gebeurtenissen die zijn toegevoegd aan uitzonderingsregels.
   - **Send only selected events**. In deze modus verstuurt het programma alleen gebeurtenissen die zijn toegevoegd aan inclusieregels.

c. Maak lijsten met uitzonderingsregels of opnameregels voor de relevante modus voor versturen van gebeurtenissen.

Om regels toe te voegen, moet u de ID van de gebeurtenis opgeven in het Windows-gebeurtenislogboeken. U kunt meerdere gebeurtenis-ID's in een regel opgeven. Als u meerdere gebeurtenis-ID's wilt opgeven, gebruik dan de komma (`,`).

d. Schakel indien nodig de logboekregistratie van gebeurtenissen in met de schakelaar naast de naam van het logboek.

7. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

KUMA gebeurtenisfilters exporteren en importeren

U kunt de lijst met uitzonderingen exporteren naar een JSON-bestand. Vervolgens kunt u het bestand aanpassen om bijvoorbeeld een groot aantal gebeurtenis-ID's toe te voegen. U kunt ook de export/import-functie gebruiken om een back-up te maken van de gebeurtenisfilters, of om de lijst naar een andere server te migreren.

Het gebruik van te veel regels kan de belasting van de KUMA-server verhogen en de prestaties van de computer verminderen. We raden u aan om alleen noodzakelijke regels toe te voegen.

Gebeurtenisfilters exporteren en importeren in de Beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de beheerconsole **Policies**.
3. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
4. Selecteer **Algemene instellingen** → **Uitzonderingen en objecttypen** in het beleidsvenster.
5. In het blok **Telemetrie-instellingen** → **KUMA-telemetrie**, klikt u op de knop **Instellingen**.
6. Om de gebeurtenisfilters te exporteren:
   a. Selecteer gebeurtenislogboeken met filters die u wilt exporteren.
   b. Klik op de knop → **Exporteren**.
   c. Geef in het geopende venster de naam van het JSON-bestand op waarnaar u de gebeurtenisfilters wilt exporteren. Selecteer vervolgens de map waarin u dit bestand wilt opslaan.
   d. Sla het bestand op.

   Kaspersky Endpoint Security exporteert de gebeurtenisfilters naar het JSON-bestand.
7. Om de gebeurtenisfilters te importeren:
   a. Klik op de knop → **Importeren**.
   b. Selecteer in het venster dat opent het JSON-bestand waaruit u de gebeurtenisfilters wilt importeren.

c. Open het bestand.

Als er al regels voor het filteren van gebeurtenissen op de computer bestaan, vervangt Kaspersky Endpoint Security deze tijdens het importeren.

8. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Gebeurtenisfilters in de webconsole exporteren en importeren

1. Selecteer in het hoofdvenster van de Webconsole het tabblad **Asset management** → **Policies**.
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** → **Telemetry Settings**.
5. Selecteer het tabblad **KUMA telemetry**.
6. Om de gebeurtenisfilters te exporteren:

   a. Selecteer gebeurtenislogboeken met filters die u wilt exporteren.

   b. Klik op de knop → **Export**.

   c. Geef in het geopende venster de naam van het JSON-bestand op waarnaar u de gebeurtenisfilters wilt exporteren. Selecteer vervolgens de map waarin u dit bestand wilt opslaan.

   d. Sla het bestand op.

   Kaspersky Endpoint Security exporteert de gebeurtenisfilters naar het JSON-bestand.
7. Om de gebeurtenisfilters te importeren:

   a. Klik op de knop → **Import**.

   b. Selecteer in het venster dat opent het JSON-bestand waaruit u de gebeurtenisfilters wilt importeren.

   c. Open het bestand.

   Als er al regels voor het filteren van gebeurtenissen op de computer bestaan, vervangt Kaspersky Endpoint Security deze tijdens het importeren.
8. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

U kunt gebeurtenisfilters ook exporteren of importeren in de opdrachtregel.

Gids voor migratie van KSWS naar KES

Vanaf versie 11.8.0 ondersteunt Kaspersky Endpoint Security voor Windows de basisfunctionaliteit van de Kaspersky Security for Windows Server (KSWS)-oplossing. *Kaspersky Security for 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 de werking van de oplossing raadpleegt u de Help van Kaspersky Security for Windows Server. Vanaf Kaspersky Endpoint Security 11.8.0 kunt u migreren van Kaspersky Security for Windows Server naar Kaspersky Endpoint Security voor Windows en dezelfde oplossing gebruiken om werkstations en servers te beschermen.

Softwarevereisten

Voordat u begint met de migratie van KSWS naar KES, moet u ervoor zorgen dat uw server voldoet aan de hardware- en softwarevereisten van Kaspersky Endpoint Security for Windows. De lijsten met ondersteunde besturingssysteemversies verschillen voor KES en KSWS. KES ondersteunt bijvoorbeeld geen servers met Windows Server 2003.

Minimale softwarevereisten voor het migreren van KSWS naar KES:

- Kaspersky Endpoint Security voor Windows 12.0.
- Kaspersky Security 11.0.1 voor Windows Server.

  Als u een eerdere versie van Kaspersky Security for Windows Server geïnstalleerd hebt, raden we u aan het programma te upgraden naar de nieuwste versie. De wizard voor de conversie van beleid en taken ondersteunt geen eerdere versies van Kaspersky Security for Windows Server.
- Kaspersky Security Center 14.2

  Als u een eerdere versie van Kaspersky Security Center geïnstalleerd hebt, werk deze dan bij naar 14.2 of hoger. In deze versie van Kaspersky Security Center kunt u met de wizard Batchconversie van beleid en taken een migratie uitvoeren van beleid naar een profiel in plaats van naar een beleid. In deze versie van Kaspersky Security Center kunt u met de wizard Batchconversie van beleid en taken ook een breder scala aan beleidsinstellingen migreren.
- Kaspersky Endpoint Agent 3.10.

  Als u een eerdere versie van Kaspersky Endpoint Agent hebt geïnstalleerd, raden we u aan het programma te upgraden naar de nieuwste versie. Kaspersky Endpoint Security ondersteunt de migratie van een [KSWS+KEA]-configuratie naar [KES+built-in agent] vanaf Kaspersky Endpoint Agent 3.10.

Aanbevelingen voor migratie

Volg de volgende aanbevelingen bij het migreren van KSWS naar KES:

- Plan de migratietijd van KSWS naar KES van tevoren. Kies een tijdstip waarop servers het minst belast zijn, bijvoorbeeld in het weekend.
- Schakel na de migratie de programmaonderdelen geleidelijk in. Begin bijvoorbeeld door alleen het onderdeel File Threat Protection in te schakelen, vervolgens andere beveiligingscomponenten in te schakelen, vervolgens besturingscomponenten in te schakelen, enzovoort. Bij elke stap moet u ervoor zorgen dat het programma correct werkt en de prestaties van de server controleren. De architectuur van KES verschilt van KSWS, daarom kan het besturingssysteem zich ook anders gedragen.
- Voer de migratie geleidelijk uit. Migreer eerst een enkele server, daarna meerdere servers en voer vervolgens de migratie uit op alle servers van de organisatie.
- Migreer verschillende soorten servers afzonderlijk. Dat wil zeggen dat u bijvoorbeeld eerst de databaseservers moet migreren, daarna de mailservers, enzovoort.
- Bij migratie op zwaarbelaste servers moet rekening worden gehouden met enkele speciale overwegingen.

Migratiestappen

De migratie van KSWS naar KES wordt halfautomatisch uitgevoerd. Dit is nodig vanwege de verschillende architecturen van de programma's. Om beleidsinstellingen te migreren, moet u de wizard Batchconversie van beleid en taken (de migratiewizard) uitvoeren. Na het migreren van beleidsinstellingen, moet u de instellingen die de migratiewizard niet automatisch kan migreren handmatig migreren (bijvoorbeeld instellingen voor wachtwoordbeveiliging). Na de migratie is het ook raadzaam om te controleren of de migratiewizard alle instellingen correct heeft gemigreerd.

Migreer van KSWS naar KES in deze volgorde:

1. **KSWS-taken en beleid migreren**

   Nadat u het beleid en de taken hebt gemigreerd, moet u aanvullende configuratiestappen uitvoeren. We raden ook aan ervoor te zorgen dat Kaspersky Endpoint Security het vereiste beveiligingsniveau biedt na de migratie van KSWS.

   > De wizard Batchconversie van beleid en taken voor Kaspersky Security for Windows Server is alleen beschikbaar in de Beheerconsole (MMC). Beleids- en taakinstellingen kunnen niet worden gemigreerd in de webconsole en Kaspersky Security Center-cloudconsole.

2. **Installeer Kaspersky Endpoint Security**

U kunt Kaspersky Endpoint Security op de volgende manieren installeren:

- KES installeren na het verwijderen van KSWS (aanbevolen).

  Het hulpprogramma Kavremover biedt geen ondersteuning voor het beheer van KSWS.

- KES installeren bovenop KSWS.

3. KES activeren met een KSWS-sleutel

4. **Controleer of het programma na de migratie werkt**

   Controleer na de migratie van KSWS naar KES of het programma correct werkt. Controleer de status van de server in de console (moet *OK* zijn). Zorg ervoor dat er geen fouten worden gerapporteerd voor het programma, controleer ook het tijdstip van de laatste verbinding met de beheerserver, het tijdstip van de laatste database-update en de serverbeveiligingsstatus.

   Besteed speciale aandacht aan de migratie van lijsten met uitzonderingen, vertrouwde programma's, vertrouwde webadressen, regels van Programmacontrole.

Correspondentie van KSWS- en KES-onderdelen

Bij het migreren van KSWS naar KES wordt de set onderdelen alleen gemigreerd wanneer het programma lokaal wordt geïnstalleerd.

Correspondentie van Kaspersky Security for Windows Server en Kaspersky Endpoint Security voor Windows componenten

Onderdeel Kaspersky Security for Windows Server.	Onderdeel Kaspersky Endpoint Security voor Windows
Basic functionality	Programmakernel
Log Inspection	Log Inspectie
Device Control	Apparaatcontrole
Firewall Management	*(niet ondersteund)* KSWS Firewall-functies worden uitgevoerd door de firewall op systeemniveau. In KES is een afzonderlijk onderdeel verantwoordelijk voor de Firewall-functionaliteit. Na de migratie kunt u de Kaspersky Endpoint Security Firewall configureren.
File Integrity Monitor	Systeemintegriteitscontrole
Exploit Prevention	Exploit-preventie
System Tray Icon	*(niet ondersteund)* U kunt gebruikersinteractie configureren in de instellingen programma-interface.
Integration with Kaspersky Security Center	Netwerkagent-connector
Endpoint Agent	*(niet ondersteund)* 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.
Network Threat Protection	Network Threat Protection
Anti-Cryptor	Gedragsdetectie
Anti-Cryptor for NetApp	*(niet ondersteund)*

Onderdeel Kaspersky Security for Windows Server.	Onderdeel Kaspersky Endpoint Security voor Windows
Traffic Security	Web Threat Protection Mail Threat Protection Webcontrole
On-Demand Scan	Programmakernel
ICAP Network Storage Protection	*(niet ondersteund)* Kaspersky Endpoint Security ondersteunt geen componenten van netwerkopslagbeveiliging. Als u deze componenten nodig hebt, kunt u Kaspersky Security for Windows Server blijven gebruiken.
RPC Network Storage Protection	*(niet ondersteund)* Kaspersky Endpoint Security ondersteunt geen componenten van netwerkopslagbeveiliging. Als u deze componenten nodig hebt, kunt u Kaspersky Security for Windows Server blijven gebruiken.
Real-Time File Protection	File Threat Protection
Script Monitoring	*(niet ondersteund)* Script Monitoring wordt afgehandeld door andere onderdelen, bijvoorbeeld AMSI-bescherming.
KSN Usage	Kaspersky Security Network
Applications Launch Control	Programmacontrole
Performance counters	*(niet ondersteund)*

Correspondentie van KSWS- en KES-instellingen

Bij het migreren van beleid en taken wordt KES geconfigureerd in overeenstemming met KSWS-instellingen. Instellingen van programmaonderdelen die KSWS niet heeft, zijn ingesteld op standaardwaarden.

Application settings

Scalability, interface and scanning settings

Programma-instellingen worden niet ondersteund in Kaspersky Endpoint Security voor Windows.

Programma-instellingen

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
Scalability settings	*(migreert niet)* Kaspersky Endpoint Security beheert alle werkprocessen.
Show System Tray Icon	*(migreert niet)* Op een clientcomputer zijn het hoofdvenster van Kaspersky Endpoint Security en het pictogram in het Windows-systeemvak standaard 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. U kunt gebruikersinteractie configureren in de instellingen programma-interface.
Restore file attributes after scanning	*(migreert niet)* Kaspersky Endpoint Security herstelt automatisch bestandskenmerken na het scannen van een bestand.
Limit CPU usage for scanning threads	*(migreert niet)* Kaspersky Endpoint Security beperkt het CPU-gebruik niet tijdens het scannen. U kunt de taak configureren om te worden uitgevoerd wanneer de computer onder minimale belasting werkt.

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
Folder for temporary files created during scanning	*(migreert niet)* Kaspersky Endpoint Security plaatst de tijdelijke bestanden in de map `C:\Windows\Temp`.
HSM system settings	*(migreert niet)* Kaspersky Endpoint Security ondersteunt geen HSM-adressen.

Security and reliability

KSWS-beveiligingsinstellingen worden gemigreerd naar de sectie **Algemene instellingen**, **Programma-instellingen** en subsecties **Interface**.

Beschermingsinstellingen programma

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
Protect application processes from external threats	**Zelfbescherming inschakelen** (subsectie **Programma-instellingen**)
Apply password protection	*(migreert niet)* Kaspersky Endpoint Security heeft een ingebouwde wachtwoordbeveiligingsfunctie (zie de subsectie **Interface**).
Perform task recovery	*(migreert niet)* Kaspersky Endpoint Security herstelt alleen automatisch *Malware-scan* taken. Kaspersky Endpoint Security voert andere taken uit volgens een schema.
Do not start scheduled scan tasks	**Geplande taken uitstellen bij werking op accustroom** (subsectie **Programma-instellingen**)
Stop current scan tasks	*(migreert niet)* Wanneer de computer wordt gevoed door een UPS, stopt Kaspersky Endpoint Security de scantaken die al worden uitgevoerd niet.

Connection settings

De interactie-instellingen van de Administration Server worden gemigreerd naar de sectie **Algemene instellingen**, subsecties **Netwerkinstellingen** en **Programma-instellingen**.

Interactie-instellingen Administration Server

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
Proxy server settings	**Proxyserverinstellingen** (subsectie **Netwerkinstellingen**)
Do not use proxy server for local addresses	**Geen proxyserver gebruiken voor lokale adressen** (subsectie **Netwerkinstellingen**)
Proxy server authentication settings	**Proxyserververificatie gebruiken** (subsectie **Netwerkinstellingen**) Het authenticatiewachtwoord van de proxyserver is niet gemigreerd. Na het migreren van een beleid moet het wachtwoord handmatig worden ingevoerd.
Use Kaspersky Security Center as a proxy server when activating the application	**Kaspersky Security Center gebruiken als proxyserver voor activering** (subsectie **Programma-instellingen**)

Run local system tasks

Kaspersky Endpoint Security negeert de instellingen voor het uitvoeren van lokale systeemtaken van Kaspersky Security for Windows Server. U kunt het gebruik van lokale KES-taken configureren onder **Lokale Taken**, **Taakbeheer**. U kunt ook een schema configureren voor het uitvoeren van de taken *Malware-scan* en *Update van databases en programmamodules* in de eigenschappen van deze taken.

Supplementary

Trusted zone

KSWS vertrouwde zone-instellingen worden gemigreerd naar de sectie **Algemene instellingen**, subsectie **Uitzonderingen**.

Instellingen vertrouwde zone

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
Object to scan (Exclusions)	**Scanuitzonderingen** (Scanuitzonderingen) De methoden die KSWS en KES gebruiken voor het selecteren van objecten verschillen. Bij het migreren ondersteunt KES uitzonderingen die zijn gedefinieerd als individuele bestanden of paden naar bestand/map. Als KSWS uitzonderingen heeft geconfigureerd als een vooraf gedefinieerd gebied of een script-URL, worden dergelijke uitzonderingen niet gemigreerd. Na de migratie moet u dergelijke uitzonderingen handmatig toevoegen. Uitzonderingen als vooraf gedefinieerde gebieden moeten worden geconfigureerd in de *Malware-scan*-taakinstellingen. Uitzonderingen als scriptwebadressen moeten worden toegevoegd aan vertrouwde webadressen voor Web Threat Protection.
Apply also to subfolders (Exclusions)	**Inclusief submappen** (Scanuitzonderingen)
Objects to detect (Exclusions)	**Type gedetecteerd object** (Scanuitzonderingen)
Exclusion usage scope (Exclusions)	**Beschermingsonderdelen** (Scanuitzonderingen) Als in KSWS ten minste één onderdeel is geselecteerd, past KES de uitzonderingen toe op alle programmaonderdelen.
Comment (Exclusions)	**Opmerking** (Scanuitzonderingen)
Trusted process (Trusted process)	**Vertrouwde programma's** Betrouwbare selectiemethoden voor processen / programma's verschillen in KSWS en KES. Bij het migreren ondersteunt KES vertrouwde programma's die zijn geconfigureerd als een pad naar het uitvoerbare bestand of masker. Als KSWS vertrouwde processen heeft geconfigureerd zoals een bestandshash, worden dergelijke vertrouwde processen niet gemigreerd. Na de migratie moet u dergelijke vertrouwde processen handmatig toevoegen.
Do not check file backup operations (Trusted process)	**Bewaak geen programma-activiteit** (Vertrouwde programma's)

Removable drives scan

Instellingen van scan van verwisselbare schijven worden gemigreerd naar de sectie **Lokale Taken**, subsectie **Scan van Verwisselbare Schijven**.

Instellingen van de Scan van verwisselbare schijven

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
Scan removable drives on connection via USB	**Actie op een verwisselbare schijfverbinding**
Scan removable drives if its stored data volume does not exceed (MB)	**Maximale grootte van verwisselbare schijven**

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
Scan with security level • **Maximum protection** • **Recommended** • **Maximum performance**	**Actie op een verwisselbare schijfverbinding** • **Maximale bescherming** • **Aanbevolen** KSWS-beveiligingsniveaus komen als volgt overeen met KES-scanmodi: • Maximum protection – Maximale bescherming • Recommended – Aanbevolen • Maximum performance – Aanbevolen

User permissions for application management

Kaspersky Endpoint Security biedt geen ondersteuning voor het toewijzen van gebruikerstoegangsrechten voor programmabeheer en programma-servicebeheer. U kunt toegangsinstellingen configureren voor gebruikers en gebruikersgroepen voor het beheer van het programma in Kaspersky Security Center.

User access permissions for Kaspersky Security Service management

Kaspersky Endpoint Security biedt geen ondersteuning voor het toewijzen van gebruikerstoegangsrechten voor programmabeheer en programma-servicebeheer. U kunt toegangsinstellingen configureren voor gebruikers en gebruikersgroepen voor het beheer van het programma in Kaspersky Security Center.

Storages

KSWS-opslaginstellingen worden gemigreerd naar de sectie **Algemene instellingen**, subsectie Rapporten en Opslag en naar de sectie **Essential Threat Protection**, subsectie Network Threat Protection.

Instellingen voor opslag

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
Backup folder	*(migreert niet)* Kaspersky Endpoint Security slaat back-ups van bestanden op in de map `C:\ProgramData\Kaspersky Lab\KES.14.1\QB`.
Maximum Backup size (MB)	**Beperk grootte van Back-up tot N MB** (sectie **Algemene instellingen** → **Rapporten en Opslag**)
Threshold value for space available (MB)	*(migreert niet)* Kaspersky Endpoint Security registreert de gebeurtenis *Quarantaine heeft bijna geen vrije ruimte meer* wanneer de drempel van 50% is bereikt.
Target folder for restoring objects	*(migreert niet)* Kaspersky Endpoint Security herstelt bestanden naar hun oorspronkelijke map.
Quarantine folder	*(migreert niet)* Kaspersky Endpoint Security slaat back-ups van bestanden op in de map `C:\ProgramData\Kaspersky Lab\KES.14.1\QB`.
Maximum Quarantine size (MB)	*(migreert niet)* Kaspersky Endpoint Security gebruikt Back-up om waarschijnlijk geïnfecteerde objecten op te slaan. Tijdens de migratie negeert Kaspersky Endpoint Security de quarantaine-instellingen.
Threshold value for space available (MB)	*(migreert niet)* Kaspersky Endpoint Security gebruikt Back-up om waarschijnlijk geïnfecteerde objecten op te slaan. Tijdens de migratie negeert Kaspersky Endpoint Security de quarantaine-instellingen.
Target folder for restoring objects	*(migreert niet)* Kaspersky Endpoint Security herstelt bestanden naar hun oorspronkelijke map.
Unblock automatically in N	**Blokkeer aanvallende apparaten voor N min** (sectie **Essential Threat Protection** → **Network Threat Protection**)

Real-time server protection

Real-Time File Protection

KSWS Instellingen voor realtime bestandsbeveiliging worden gemigreerd naar de sectie **Essential Threat Protection**, subsectie **File Threat Protection**.

Instellingen voor realtime bestandsbeveiliging

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
Objects protection mode • **Smart mode** • **When run** • **On access** • **On access and modification**	**Scanmodus** • **Intelligente modus** • **Bij uitvoeren** • **Bij openen** • **Bij openen en wijzigen**
Deeper analysis of launching processes	*(migreert niet)* Kaspersky Endpoint Security ondersteunt slechts één analysemodus, de Optimal modus.
Heuristic analyzer • **Light** • **Medium** • **Deep**	**Heuristische analyse** • **Oppervlakkige scan** • **Gemiddelde scan** • **Gedetailleerde scan**
Apply Trusted Zone	*(migreert niet)* Kaspersky Endpoint Security past de vertrouwde zone toe op alle onderdelen. U kunt uitzonderingen configureren in instellingen voor vertrouwde zone.
Use KSN for protection	*(migreert niet)* Kaspersky Endpoint Security gebruikt KSN voor alle programmaonderdelen.
Block access to network shared resources for the hosts that show malicious activity	*(migreert niet)* Kaspersky Endpoint Security blokkeert standaard de toegang tot gedeelde netwerkbronnen voor hosts die schadelijke activiteiten vertonen.
Launch critical areas scan when active infection is detected	*(migreert niet)* Kaspersky Endpoint Security start de scantaak voor kritieke gebieden niet wanneer een actieve infectie wordt gedetecteerd.
Use Kaspersky Sandbox for protection	*(migreert niet)* Kaspersky Endpoint Security verzendt standaard objecten om te scannen naar Kaspersky Sandbox.
Protection scope	**Beschermd bereik**
Schedule settings	*(migreert niet)* Kaspersky Endpoint Security gebruikt zijn eigen planning voor het pauzeren van File Threat Protection.

KSN Usage

Instellingen KSWS voor Kaspersky Security Network worden gemigreerd naar de sectie **Advanced Threat Protection**, subsectie **Kaspersky Security Network**.

Instellingen van Kaspersky Security Network

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
I confirm that I have fully read, understood, and accept the terms of participation in Kaspersky Security Network	**Kaspersky Security Network-verklaring** Kaspersky Endpoint Security vraagt toestemming voor de Kaspersky Security Network-verklaring wanneer het programma wordt geïnstalleerd, een nieuw beleid wordt gemaakt of het gebruik van Kaspersky Security Network wordt ingeschakeld.
Send data about scanned files	*(migreert niet)* Kaspersky Endpoint Security verzendt automatisch gegevens over gescande bestanden als KSN is ingeschakeld.

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
Send data about requested URLs	*(migreert niet)* Kaspersky Endpoint Security verzendt automatisch gegevens over aangevraagde URL's als KSN is ingeschakeld.
Send Kaspersky Security Network statistics	**Uitgebreide KSN-modus inschakelen**
Accept the terms of the Kaspersky Managed Protection Statement	*(migreert niet)* Kaspersky Endpoint Security de KMP-service niet.
Action to perform on KSN untrusted objects	*(migreert niet)* U kunt de actie bij detectie van bedreigingen configureren in de instellingen van het beschermingsonderdeel en de instellingen voor scantaken.
Do not calculate checksum before sending to KSN if file size exceeds N MB	*(migreert niet)* U kunt beperkingen voor het scannen van grote bestanden configureren in Instellingen voor beschermingsonderdelen en Instellingen voor scantaken.
Use Kaspersky Security Center as KSN Proxy	**Gebruik Administration Server als een KSN-proxyserver**
Schedule settings	*(migreert niet)* Het is niet mogelijk om voor het onderdeel een aparte planning in te stellen. Het onderdeel staat altijd aan terwijl Kaspersky Endpoint Security operationeel is.

Traffic Security

Beveiligingsinstellingen KSWS Traffic worden gemigreerd naar de sectie **Essential Threat Protection**, subsectie **Web Threat Protection** en subsectie **Mail Threat Protection**, sectie **Security Controls**, subsectie **Webcontrole**, sectie **Algemene instellingen**, subsectie **Netwerkinstellingen**.

Beschermingsinstellingen verkeer

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
Apply URL-based rules	**Webcontrole** (subsectie **Webcontrole**) Op URL gebaseerde regels worden gemigreerd naar aparte regels in Kaspersky Endpoint Security.
Apply certificate-based rules	*(migreert niet)* Kaspersky Endpoint Security ondersteunt de volgende op certificatie gebaseerde regels niet:
Apply rules for web traffic category control	**Webcontrole** (subsectie **Webcontrole**) Blokeerregels voor categoriebeheer van webverkeer worden gemigreerd naar één enkele blokkeerregel in Kaspersky Endpoint Security. Kaspersky Endpoint Security negeert toegestane regels voor categoriebeheer. De correspondentie van de KSWS- en KES-categorieën wordt hieronder vermeld.
Allow access if the web page can not be categorized	*(migreert niet)* Kaspersky Endpoint Security geeft toegang als de webpagina niet kan worden gecategoriseerd.
Allow access to legitimate web resources that can be used to damage a protected device	*(migreert niet)* Kaspersky Endpoint Security geeft toegang tot legitieme webbronnen die kunnen worden gebruikt om het beschermde apparaat te beschadigen.
Allow access to legitimate advertisement	*(migreert niet)* U kunt de toegang tot legitieme advertenties beheren met behulp van de categorie *Banners*-webbronnen in de instellingen van webcontrole.
Operation mode • **Driver Interceptor** • **Redirector** • **External Proxy**	*(migreert niet)* Kaspersky Endpoint Security ondersteunt alleen de Driver Interceptor-modus.
ICAP-service connection settings	*(migreert niet)* Kaspersky Endpoint Security biedt geen ondersteuning voor ICAP Network Storage Protection.
Check safe connections through the HTTPS protocol	Modus **Geëncrypte verbindingen scannen** / **Geëncrypte verbindingen altijd scannen** (subsectie **Netwerkinstellingen**)

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
Use TLS protocol version	*(migreert niet)* 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. U kunt bovendien SSL 2.0-verbindingen blokkeren in scaninstellingen voor versleutelde verbindingen.
Do not trust web-servers with invalid certificate	**Adres** (subsectie **Netwerkinstellingen**)
Intercept ports (Interception area)	**Bewaakte poorten** (subsectie **Netwerkinstellingen**) Tijdens de migratie schakelt KES de selectievakjes uit voor **Bewaak alle poorten voor de programma's die voorkomen op de lijst aanbevolen door Kaspersky** en **Bewaak alle poorten voor de opgegeven programma's**.
Exclude ports (Interception area)	*(migreert niet)*
Exclude IP addresses (Interception area)	**Configureer vertrouwde adressen** (subsectie **Netwerkinstellingen**)
Exclude processes (Interception area)	**Configureer vertrouwde programma's** (subsectie **Netwerkinstellingen**) Tijdens de migratie configureert KES de volgende instellingen voor het vertrouwde programma: • Het selectievakje **Scan geen netwerkverkeer** is geselecteerd. KES scant het netwerkverkeer niet op externe IP-adressen en poorten. • De andere selectievakjes in de instellingen voor vertrouwde programma's worden uitgeschakeld.
Security port	*(migreert niet)*
Use malicious URL database to scan web links	**Controleer of het webadres voorkomt in de database met schadelijke webadressen** (subsectie **Web Threat Protection**)
Use anti-phishing database to scan web pages	**Controleer of het webadres voorkomt in de database met phishingadressen** (subsectie **Web Threat Protection**)
Use KSN for protection	*(migreert niet)* Kaspersky Endpoint Security gebruikt KSN voor alle programmaonderdelen.
Use Trusted Zone	*(migreert niet)* Kaspersky Endpoint Security past de vertrouwde zone toe op alle onderdelen. U kunt uitzonderingen configureren in instellingen voor vertrouwde zone.
Use heuristic analyzer	**Gebruik heuristische analyse** (subsecties **Web Threat Protection** en **Mail Threat Protection**)
Security level	*(migreert niet)* Kaspersky Endpoint Security heeft zijn eigen beveiligingsniveaus voor de componenten Web Threat Protection en Mail Threat Protection. Kaspersky Endpoint Security stelt standaard het aanbevolen beveiligingsniveau in.
Enable mail threat protection	**Mail Threat Protection** (subsectie **Mail Threat Protection**) **Verbind Microsoft Outlook-extensie** **Alleen inkomende berichten** (Beschermd bereik) **Scannen bij ontvangen** (E-mailbescherming)
Schedule settings	*(migreert niet)* Het is niet mogelijk om voor het onderdeel een aparte planning in te stellen. Het onderdeel staat altijd aan terwijl Kaspersky Endpoint Security operationeel is.

Exploit Prevention

Instellingen van KSWS Exploit-preventie zijn gemigreerd naar de sectie **Advanced Threat Protection**, subsectie **Exploit-preventie**.

Instellingen van Exploit-preventie

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
Prevent vulnerable processes exploit • **Terminate on exploit** • **Notify only**	**Bij detectie van exploit** • **Blokkeren** • **Melden**
Notify about abused processes via Terminal Service	*(migreert niet)* Kaspersky Endpoint Security ondersteunt terminal services niet.
Prevent vulnerable processes exploit even if Kaspersky Security Service is disabled	*(migreert niet)* Kaspersky Endpoint Security voorkomt voortdurend misbruik van kwetsbare processen.
Protected processes	**Bescherming voor systeemprocessen in geheugen inschakelen** Kaspersky Endpoint Security ondersteunt het selecteren van volgende beschermde processen niet: U kunt alleen bescherming voor systeemprocessen in geheugen inschakelen.
Exploit prevention techniques • **Apply all available exploit prevention techniques** • **Apply selected exploit prevention techniques**	*(migreert niet)* Kaspersky Endpoint Security past alle beschikbare technieken voor exploit-preventie toe:

Network Threat Protection

Instellingen van KSWS Network Threat Protection zijn gemigreerd naar de sectie **Essential Threat Protection**, subsectie **Network Threat Protection**.

Instellingen van Network Threat Protection

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
Operation mode • **Pass-through** • **Only inform about network attacks** • **Block connections when attack is detected**	**Network Threat Protection** Als de modus **Pass-through** is geselecteerd, dan is Network Threat Protection uitgeschakeld. Als de modus **Only inform about network attacks** of **Block connections when attack is detected** geselecteerd is, is Network Threat Protection ingeschakeld. Kaspersky Endpoint Security werkt altijd in de modus **Block connections when attack is detected**
Do not stop traffic analysis when the task is not running	*(migreert niet)* Kaspersky Endpoint Security analyseert het verkeer continu als het onderdeel is ingeschakeld.
Do not control excluded IP addresses	**Uitzonderingen**
Schedule settings	*(migreert niet)* Het is niet mogelijk om voor het onderdeel een aparte planning in te stellen. Het onderdeel staat altijd aan terwijl Kaspersky Endpoint Security operationeel is.

Script Monitoring

Kaspersky Endpoint Security ondersteunt het onderdeel Script Monitoring niet. Script Monitoring wordt afgehandeld door andere onderdelen, bijvoorbeeld AMSI-bescherming.

Website categories

Kaspersky Endpoint Security ondersteunt niet alle categorieën van Kaspersky Security for Windows Server. Categorieën die niet bestaan in Kaspersky Endpoint Security worden niet gemigreerd. Daarom worden classificatieregels voor webbronnen met niet-ondersteunde categorieën niet gemigreerd.

Websitecategorieën

Kaspersky Security for Windows Server-categorieën.	Kaspersky Endpoint Security voor Windows-categorieën
Wargaming	Videospellen
Abortion	*(migreert niet)*
Lotteries (extended)	Gokken, loterijen, sweepstakes

Kaspersky Security for Windows Server-categorieën.	Kaspersky Endpoint Security voor Windows-categorieën
Alcohol	Alcohol, tabak, drugs
Anonymous proxy servers	Anonymizers
Anorexia	*(migreert niet)*
Rentals for real estate	*(migreert niet)*
Audio, video and software	Software, audio, video
Banks	Banken
Blogs	Blogs
Military	Wapens, explosieven, leger inhoud
For children	*(migreert niet)*
Discrimination	Geweld, intolerantie
Home and family	*(migreert niet)*
Hosting and domain services	Online communicatie
Pets and animals	*(migreert niet)*
Law and politics	Verboden door regionale wetgeving
Restricted by Roskomnadzor (RF)	Verboden door wetgeving van de Russische Federatie
Restricted by Federal Law 436 (RF)	Verboden door wetgeving van de Russische Federatie
Restricted by RF legislation	Verboden door wetgeving van de Russische Federatie
Restricted by global legislation	Verboden door regionale wetgeving
Adult dating	Erotische inhoud
Internet services	*(migreert niet)*
Sex shops	Erotische inhoud
Information technologies	*(migreert niet)*
Casinos, card games	Gokken, loterijen, sweepstakes
Books and writing	*(migreert niet)*
Computer games	Videospellen
Health and beauty	*(migreert niet)*
Culture and society	*(migreert niet)*
LGBT	Erotische inhoud
Lotteries	Gokken, loterijen, sweepstakes
Medicine	*(migreert niet)*
Fashion	*(migreert niet)*
Music	*(migreert niet)*
Drugs	Alcohol, tabak, drugs
Violence	Geweld, intolerantie
Discontent	*(migreert niet)*
Illegal drugs	Alcohol, tabak, drugs
Hate and discrimination	Geweld, intolerantie
Obscene vocabulary	Grof taalgebruik, obsceniteit
Lingerie	Erotische inhoud
News	Nieuwsbronnen
Nudism	Erotische inhoud

Kaspersky Security for Windows Server-categorieën.	Kaspersky Endpoint Security voor Windows-categorieën
Education	*(migreert niet)*
Online shopping	Online winkels
All communication media	Online communicatie
Payment by credit cards	Betaalsystemen
Online shopping (own payment system)	Online winkels
Online encyclopedias	*(migreert niet)*
Online banking	Banken
Weapons	Wapens, explosieven, leger inhoud
Fishing and hunting	*(migreert niet)*
Payment systems	Betaalsystemen
Job search	Jobsites
Search engines	*(migreert niet)*
Police decision (JP)	Verboden door politie van Japan
Trusted by KPSN	*(migreert niet)*
Untrusted by KPSN	*(migreert niet)*
Porn	Erotische inhoud
Media hosting and streaming	Nieuwsbronnen
Web Mail	Webmail
Traveling	*(migreert niet)*
TV and radio	Nieuwsbronnen
Teasers and ads services	Banners
Religion	Godsdienst, religieuze groeperingen
Restaurants, cafe and food	*(migreert niet)*
Dating sites	Datingsites
Sex education	Erotische inhoud
Social networks	Sociale netwerken
Sport	*(migreert niet)*
Betting	Gokken, loterijen, sweepstakes
Suicide	Geweld, intolerantie
Tobacco	Alcohol, tabak, drugs
Torrents	Torrents
Mentioned in Federal list of extremists (RF)	Verboden door wetgeving van de Russische Federatie
File sharing	Bestandsdeling
Pharmacy	*(migreert niet)*
Hobby and entertainment	*(migreert niet)*
Chats and forums	Chats, forums, IM
Schools and universities pages	*(migreert niet)*
Astrology and esoterica	*(migreert niet)*
Extremism and racism	Geweld, intolerantie
E-commerce	Online winkels

Kaspersky Security for Windows Server-categorieën.	Kaspersky Endpoint Security voor Windows-categorieën
Erotic	Erotische inhoud
Humor	*(migreert niet)*

Local activity control

Applications Launch Control

KSWS Instellingen van Programmacontrole worden gemigreerd naar de sectie **Security Controls**, subsectie **Programmacontrole**.

Instellingen voor Programma's Launch Control

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
Operation mode • **Statistics only** • **Active**	**Actie** (Programmacontrole) • **Regels testen**. • **Regels toepassen**.
Repeat action taken for the first file launch on all the subsequent launches for this file	*(migreert niet)* Kaspersky Endpoint Security scant het programma elke keer dat het probeert te starten.
Deny the command interpreters launch with no command to execute	*(migreert niet)* Kaspersky Endpoint Security staat het uitvoeren van opdrachtinterpreters toe als ze niet worden verboden door Programmacontrole.
Rules	**Regels van Programmacontrole** *(ondersteund met beperkingen)* Kaspersky Endpoint Security 11.11.0 introduceert ondersteuning voor het migreren van regels van programmacontrole. De functie voor het migreren van regels van programmacontrole heeft enkele beperkingen. Standaard omvatten regels van programmacontrole van KSWS twee regels: • **Allow scripts and MSI by OS-trusted certificate** • **Allow executable by OS-trusted certificate** Als ten minste één bron-KSWS-regel het type **Allow** heeft, dan creëert KES tijdens de migratie een nieuwe regel voor toestaan, **Applications with trusted root certificates**. Dat wil zeggen, KES Programmacontrole gebruikt één enkele regel om het uitvoeren van vertrouwde scripts, MSI-pakketten en uitvoerbare bestanden toe te staan. Als beide bron-KSWS-regels het type **Deny** hebben, voegt KES geen regels toe voor het beheren van programma's met vertrouwde basicertificaten.
Apply rules to executable files	*(migreert niet)* Het bereik van de regeltoepassing kan niet worden geconfigureerd in de instellingen van Programmacontrole van KES. KES Programmacontrole past regels toe op alle soorten bestanden: uitvoerbare bestanden, scripts en MSI-pakketten. Als alle bestandstypen zijn opgenomen in het toepassingsbereik van de regel in KSWS, neemt KES tijdens de migratie de KSWS-regels over. Als een bepaald bestandstype is uitgesloten van het toepassingsbereik van de regel in KSWS, neemt KES tijdens de migratie ook de KSWS-regels over, maar wordt **Regels testen** geselecteerd als de actie voor Programmacontrole.
Monitor loading of DLL modules	**Het laden van DLL-modules controleren (verhoogt de systeembelasting aanzienlijk)**
Apply rules to scripts and MSI packages	*(migreert niet)* Het bereik van de regeltoepassing kan niet worden geconfigureerd in de instellingen van Programmacontrole van KES. KES Programmacontrole past regels toe op alle soorten bestanden: uitvoerbare bestanden, scripts en MSI-pakketten. Als alle bestandstypen zijn opgenomen in het toepassingsbereik van de regel in KSWS, neemt KES tijdens de migratie de KSWS-regels over. Als een bepaald bestandstype is uitgesloten van het toepassingsbereik van de regel in KSWS, neemt KES tijdens de migratie de KSWS-regels over, maar wordt **Regels testen** geselecteerd als de actie voor Programmacontrole.
Deny applications untrusted by KSN	*(migreert niet)* Kaspersky Endpoint Security houdt geen rekening met de reputatie van programma's en staat wel of niet toe dat programma's volgens de regels worden uitgevoerd.

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
Allow applications trusted by KSN	Tijdens de migratie voegt KES een nieuwe regel voor toestaan toe. De KL-categorie **Overige software\Programma's, vertrouwd op basis van hun reputatie in KSN** is gespecificeerd als de voorwaarde voor het activeren van de regel.
Users and / or user groups allowed to run applications trusted by KSN	**Gebruikers en hun rechten** in een regel voor Programmacontrole die de KL-categorie bevat **Overige software\Programma's, vertrouwd op basis van hun reputatie in KSN**
Automatically allow software distribution via applications and packages listed	Software Distribution Control in KSWS en KES werkt anders. Tijdens de migratie voegt KES nieuwe regels toe voor het toestaan van programma's waarvoor automatische softwaredistributie is toegestaan. De bestandshash wordt gespecificeerd als voorwaarde voor het activeren van de regel.
Always allow software distribution via Windows Installer	Software Distribution Control in KSWS en KES werkt anders. Tijdens de migratie voegt KES nieuwe regels toe voor het toestaan van programma's waarvoor automatische softwaredistributie is toegestaan (**Software distribution applications and packages allowed**). De bestandshash wordt gespecificeerd als voorwaarde voor het activeren van de regel. In de accounteigenschappen is het selectievakje **Vertrouwde updaters** ingeschakeld.
Always allow software distribution via SCCM using the Background Intelligent Transfer Service	*(migreert niet)*
Software distribution applications and packages allowed	Software Distribution Control in KSWS en KES werkt anders. Tijdens de migratie voegt KES nieuwe regels toe voor het toestaan van programma's waarvoor automatische softwaredistributie is toegestaan. De bestandshash wordt gespecificeerd als voorwaarde voor het activeren van de regel. In de accounteigenschappen is het selectievakje **Vertrouwde updaters** ingeschakeld.
Schedule settings	*(migreert niet)* Als er een planning is geconfigureerd voor het onderdeel in de KSWS-instellingen, wordt het onderdeel Programmacontrole ingeschakeld bij migratie. Als er geen planning is geconfigureerd voor het onderdeel in de KSWS-instellingen, wordt het onderdeel Programmacontrole uitgeschakeld bij migratie. Het is niet mogelijk om voor het onderdeel een aparte planning in te stellen. Het onderdeel staat altijd aan terwijl Kaspersky Endpoint Security operationeel is.

Device Control

KSWS Instellingen van apparaatcontrole worden gemigreerd naar de sectie **Security Controls**, subsectie Apparaatcontrole.

Instellingen van het Apparaatcontrole

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
Operation mode • **Active** • **Statistics only**	*(migreert niet)* Programmacontrole werkt in de *Active* modus. De apparaatverbindingstatistieken worden continu geleverd door Audit.
Allow using all external devices when the Device Control task is not running	*(migreert niet)* Apparaatcontrole is altijd ingeschakeld terwijl Kaspersky Endpoint Security actief is.
Device Control rules	**Vertrouwde apparaten** Tijdens de migratie negeert Kaspersky Endpoint Security uitgeschakelde KSWS-regels.
Schedule settings	*(migreert niet)* Kaspersky Endpoint Security gebruikt zijn eigen schema om toegang te krijgen tot bepaalde apparaattypen.

Network-Attached Storages Protection

RPC Network Storage Protection

Kaspersky Endpoint Security ondersteunt geen componenten van netwerkopslagbeveiliging. Als u deze componenten nodig hebt, kunt u Kaspersky Security for Windows Server blijven gebruiken.

ICAP Network Storage Protection

Kaspersky Endpoint Security ondersteunt geen componenten van netwerkopslagbeveiliging. Als u deze componenten nodig hebt, kunt u Kaspersky Security for Windows Server blijven gebruiken.

Anti-Cryptor for NetApp

Kaspersky Endpoint Security biedt geen ondersteuning voor Anti-Cryptor voor NetApp. Anti-Cryptor-functionaliteit wordt geleverd door andere programma-onderdelen, zoals: gedragsdetectie.

Network activity control

Firewall Management

Kaspersky Endpoint Security ondersteunt geen KSWS Firewallbeheer. KSWS Firewall-functies worden uitgevoerd door de firewall op systeemniveau. Na de migratie kunt u de Kaspersky Endpoint Security Firewall configureren.

Anti-Cryptor

Instellingen van Netwerk Anti-Cryptor zijn gemigreerd naar de sectie **Advanced Threat Protection**, subsectie **Gedragsdetectie**.

Anti-Cryptor-instellingen

KSWS-instellingen	KES-instellingen
Operation mode • **Statistics only** • **Active**	**Bij detectie van externe encryptie van gedeelde mappen** • **Melden** • **Blokkeren**
Heuristic analyzer	*(migreert niet)* Kaspersky Endpoint Security gebruikt geen heuristische analyse voor gedragsdetectie.
Configuration of protection scope • **All shared network folders on the protected device** • **Only specified shared folders**	*(migreert niet)* Kaspersky Endpoint Security voorkomt encryptie van alle gedeelde netwerkmappen van de beveiligde computer.
Exclusions	*(migreert niet)* Kaspersky Endpoint Security heeft zijn eigen uitzonderingen voor het onderdeel Gedragsdetectie. U kunt handmatig exclusies toevoegen na de migratie.
Schedule settings	*(migreert niet)* Het is niet mogelijk om voor het onderdeel een aparte planning in te stellen. Het onderdeel staat altijd aan terwijl Kaspersky Endpoint Security operationeel is.

System Inspection

File Integrity Monitor

Instellingen voor Bestandsintegriteitsmonitor van KSWS worden gemigreerd naar het gedeelte **Security Controls**, subsectie **Systeemintegriteitscontrole**.

Instellingen voor Bestandsintegriteitsmonitor

KSWS-instellingen	KES-instellingen
Log information about file operations that appear during the monitor interruption period	*(migreert niet)* Kaspersky Endpoint Security registreert geen gebeurtenissen voor bestandsbewerkingen die zijn uitgevoerd tijdens de onderbrekingsperiode van de monitor.
Block attempts to compromise the USN log	*(migreert niet)* Kaspersky Endpoint Security blokkeert geen pogingen om het USN-logboek te compromitteren.
Monitoring scope	**Bereik van bewaking → Bestand** *(ondersteund met beperkingen)* Uitgeschakelde bewakingsbereikrecords worden niet gemigreerd naar KES. Kaspersky Endpoint Security voegt alleen ingeschakelde records toe aan het bewakingsbereik.
Trusted users	**Vertrouwde gebruikers en/of gebruikersgroepen**
File operation markers	**Markeringen voor bestandsbewerkingen**
Calculate checksum for the file if possible	**Hashing**
Exclusions	**Uitzonderingen → Bestand**

Log Inspection

KSWS Log inspectie instellingen worden gemigreerd naar **Security Controls**, subsectie **Log Inspectie**.

Log inspectie instellingen

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
Apply custom rules for log inspection	*(migreert niet)* Kaspersky Endpoint Security past alle ingeschakelde aangepaste regels toe.
Custom rules	**Aangepaste regels** De voorgedefinieerde regel **A service was installed in the system (for Server 2003 OS)** wordt niet gemigreerd naar KES.
Apply predefined rules for log inspection	*(migreert niet)* Kaspersky Endpoint Security past alle ingeschakelde voorgedefinieerde regels toe.
Predefined rules	**Voorgedefinieerde regels**
Password brute-force detection	**Brute-force aanvalsdetectie**
Network logon detection	**Netwerk aanmeld detectie**
Exclusions (IP addresses)	**Uitzonderingen** (IP-adres)
Exclusions (users)	**Uitzonderingen** (Gebruikers)
Schedule settings	*(migreert niet)* Het is niet mogelijk om voor het onderdeel een aparte planning in te stellen. Het onderdeel staat altijd aan terwijl Kaspersky Endpoint Security operationeel is.

Logs and notifications

Task logs

Instellingen van KSWS Logs worden gemigreerd naar de sectie **Algemene instellingen**, subsectie **Interface** en subsecties **Rapporten en Opslag**.

Logboekinstellingen

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
Event logging	**Meldingen** (subsectie **Interface**)
Logs folder	*(migreert niet)* Kaspersky Endpoint Security slaat rapporten op in de map `C:\ProgramData\Kaspersky Lab\KES.14.1\Report`.
Remove task logs older than N day(s)	*(migreert niet)* U kunt de opslagperiode voor KES-rapporten configureren onder **Algemene instellingen**, **Rapporten en Opslag**.
Remove from the audit log events N day(s)	*(migreert niet)* Kaspersky Endpoint Security past rapportopslagbeperkingen toe op alle rapporten, inclusief systeemauditrapporten.
Integration with SIEM	*(migreert niet)* U kunt de integratie met SIEM configureren in Kaspersky Security Center.

Event notifications

Instellingen voor KSWS-meldingen worden gemigreerd naar de sectie **Algemene instellingen**, subsectie **Interface**.

Instellingen voor meldingen

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
Notifications	**Meldingen**
Notify users • **By using terminal service** • **By using Windows Messenger Service command**	*(migreert niet)* Kaspersky Endpoint Security ondersteunt het wijzigen van meldingstekst niet: Kaspersky Endpoint Security geeft standaardmeldingen weer.
Notify administrators • **By using Windows Messenger Service command** • **By running executable file** • **By sending email**	Alleen instellingen voor e-mailmeldingen worden gemigreerd naar Kaspersky Endpoint Security – **Instellingen voor e-mailmeldingen** (blok **Meldingen**). Andere methoden om beheerders te informeren worden niet ondersteund.
Application database is out of date	**Verstuur de melding "Databases verouderd" als de databases niet zijn geüpdatet**
Application database is extremely out of date	**Verstuur de melding "Databases erg verouderd" als de databases niet zijn geüpdatet**
Critical areas scan has not been performed for a long time	*(migreert niet)* Kaspersky Endpoint Security genereert na drie dagen een gemiste Kritieke Gebiedenscan-gebeurtenis.

Interaction with Administration Server

Interactie-instellingen van KSWS Administration Server zijn gemigreerd naar de sectie **Algemene instellingen**, subsectie **Rapporten en Opslag**.

Interactie-instellingen Administration Server

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
Quarantined files	**Quarantainebestanden**
Backed up files	**Back-upbestanden**
Blocked hosts	*(migreert niet)* Kaspersky Endpoint Security verzendt automatisch gegevens over geblokkeerde hosts.

Tasks

Activating the application

Kaspersky Endpoint Security ondersteunt de taak *Application activation* (KES) niet. U kunt een *Licentie toevoegen*-taak maken, een licentiecode toevoegen aan het Installatiepakket, of de automatische distributie van licentiecodes inschakelen.

Copying Updates

De taakinstellingen voor *Copying Updates* (KSWS) worden gemigreerd naar de taak *Update van databases en programmamodules* (KES).

Instellingen van updatetaak kopiëren

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
Update source • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Updatebron** • **Kaspersky Security Center** • **Kaspersky-updateservers** • **Opgegeven door gebruiker**
Use Kaspersky update servers if specified servers are not available	*(migreert niet)* Kaspersky Endpoint Security staat toe meerdere updatebronnen te selecteren, inclusief Kaspersky-updateservers. Als de eerste updatebron niet beschikbaar is, kunt u met Kaspersky Endpoint Security-updates verkrijgen van een andere bron in de lijst.
Use proxy server settings to connect to Kaspersky update servers	*(migreert niet)* Kaspersky Endpoint Security gebruikt de proxyserver voor alle onderdelen. U kunt de proxyserververbinding configureren in netwerkopties van het programma.
Use proxy server settings to connect to other servers	*(migreert niet)* Kaspersky Endpoint Security gebruikt de proxyserver voor alle onderdelen. U kunt de proxyserververbinding configureren in netwerkopties van het programma.
Copying updates settings • **Copy database updates** • **Copy critical software modules updates** • **Copy database updates and critical updates of application modules**	*(migreert niet)* Kaspersky Endpoint Security kopieert database-updates en kritieke updates van programmamodules als één pakket.
Folder for local storage of copied updates	**Updates naar map kopiëren**

Baseline File Integrity Monitor

De *Baseline File Integrity Monitor* taakinstellingen (KSWS) worden gemigreerd naar de *Systeemintegriteitscheck* taak en naar de beleidssectie **Security Controls**, subsectie **Systeemintegriteitscontrole**.

Baseline File Integrity Monitor taakinstellingen

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
Hash calculation algorithm • **MD5** • **SHA256**	*(migreert niet)* Kaspersky Endpoint Security gebruikt het SHA256-algoritme voor de berekening van de controlesom.
Scan scope	**Bereik van bewaking** (subsectie **Systeemintegriteitscontrole**)

Database Update

De taakinstellingen voor *Database Update* (KSWS) worden gemigreerd naar de taak *Update van databases en programmamodules* (KES).

Instellingen van de database-updatetaak

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
Update source • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Updatebron** • **Kaspersky Security Center** • **Kaspersky-updateservers** • **Opgegeven door gebruiker**
Use Kaspersky update servers if specified servers are not available	*(migreert niet)* Kaspersky Endpoint Security staat toe meerdere updatebronnen te selecteren, inclusief Kaspersky-updateservers. Als de eerste updatebron niet beschikbaar is, kunt u met Kaspersky Endpoint Security-updates verkrijgen van een andere bron in de lijst.
Use proxy server settings to connect to Kaspersky update servers	*(migreert niet)* Kaspersky Endpoint Security gebruikt de proxyserver voor alle onderdelen. U kunt de proxyserververbinding configureren in netwerkopties van het programma.
Use proxy server settings to connect to other servers	*(migreert niet)* Kaspersky Endpoint Security gebruikt de proxyserver voor alle onderdelen. U kunt de proxyserververbinding configureren in netwerkopties van het programma.
Lower the load on the disk I/O	*(migreert niet)*

Software modules updates

De taakinstellingen voor *Software Modules Update* (KSWS) worden gemigreerd naar de taak *Update van databases en programmamodules* (KES).

Taakinstellingen voor softwaremodules bijwerken

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
Update source • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Updatebron** • **Kaspersky Security Center** • **Kaspersky-updateservers** • **Opgegeven door gebruiker**
Use Kaspersky update servers if specified servers are not available	*(migreert niet)* Kaspersky Endpoint Security staat toe meerdere updatebronnen te selecteren, inclusief Kaspersky-updateservers. Als de eerste updatebron niet beschikbaar is, kunt u met Kaspersky Endpoint Security-updates verkrijgen van een andere bron in de lijst.
Use proxy server settings to connect to Kaspersky update servers	*(migreert niet)* Kaspersky Endpoint Security gebruikt de proxyserver voor alle onderdelen. U kunt de proxyserververbinding configureren in netwerkopties van het programma.
Use proxy server settings to connect to other servers	*(migreert niet)* Kaspersky Endpoint Security gebruikt de proxyserver voor alle onderdelen. U kunt de proxyserververbinding configureren in netwerkopties van het programma.
Copy and install critical software modules updates	**Essentiële en goedgekeurde updates installeren**
Only check for critical software updates available	*(migreert niet)* Kaspersky Endpoint Security controleert voortdurend de beschikbaarheid van essentiële updates voor programmamodules.
Allow operating system restart	*(migreert niet)* Kaspersky Endpoint Security vraagt de gebruiker om toestemming om de computer opnieuw op te starten.
Receive information about available scheduled software modules updates	*(migreert niet)* Kaspersky Endpoint Security geeft meldingen weer over updates van softwaremodules.

Rollback of Application Database Update

De taakinstellingen voor *Rollback of Application Database Update* (KSWS) worden gemigreerd naar de taak *Update terugdraaien* (KES). De nieuwe *Update terugdraaien*-taak (KES) heeft een taakstartschema – *Manually*.

On-Demand Scan

De taakinstellingen voor *On-Demand Scan* (KSWS) worden gemigreerd naar de taak *Malware-scan* (KES).

Taakinstellingen voor virusscan

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
Scan scope	Scanbereik
Protection level • Maximum protection • Recommended • Maximum performance	Beveiligingsniveau • Hoog • Aanbevolen • Laag De instellingen voor het beveiligingsniveau zijn verschillend in KSWS en KES.
Objects to scan • All objects • Objects scanned by format • Objects scanned according to list of extensions specified in anti-virus database • Objects scanned by specified list of extensions	Bestandstypen • Alle bestanden • Bestanden gescand op indeling • Bestanden gescand op extensie Kaspersky Endpoint Security staat het maken van aangepaste extensielijsten niet toe. Kaspersky Endpoint Security vervangt de waarde **Objects scanned by specified list of extensions** door de waarde **Bestanden gescand op extensie**.
Subfolders	Inclusief submappen
Subfiles	*(migreert niet)*
Scan disk boot sectors and MBR	*(migreert niet)*
Scan alternate NTFS streams	*(migreert niet)*
Scan only new and modified files	Scan alleen nieuwe en gewijzigde bestanden
Scan of compound objects • All archives • All SFX archives • All email databases • All packed objects • All plain email • All embedded OLE objects	Scan van samengestelde bestanden • Scan archieven. • Scan archieven met wachtwoordbeveiliging. • Scan distributiepakketten. • Bestanden in e-mailindeling scannen. • Scan Microsoft Office-bestanden.
Action to perform on infected and other objects • Disinfect • Disinfect. Remove if disinfection fails • Remove • Perform recommended action • Notify only	Actie bij detectie van een dreiging • Desinfecteren of verwijderen als desinfectie mislukt. • Desinfecteren of melden als desinfectie mislukt. • Melden.
Action to perform on probably infected objects • Quarantine • Remove • Perform recommended action • Notify only	*(migreert niet)* Kaspersky Endpoint Security past de actie toe als er een bedreiging wordt gedetecteerd.
Perform actions depending on the type of object detected	*(migreert niet)*
Entirely remove compound file that cannot be modified by the application in case of embedded object detection	*(migreert niet)*
Exclude files	*(migreert niet)* Kaspersky Endpoint Security past de vertrouwde zone toe op alle onderdelen. U kunt uitzonderingen configureren in instellingen voor vertrouwde zone.
Do not detect	*(migreert niet)*
Stop scanning if it takes longer than N sec	Sla bestanden over waarvan scan langer duurt dan N s

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
Do not scan compound objects larger than N MB	**Grote samengestelde bestanden niet uitpakken**
Use iSwift technology	**iSwift-technologie**
Use iChecker technology	**iChecker-technologie**
Action on the offline files • **Do not scan** • **Scan resident part of file only** • **Scan entire file** • **Only if the file has been accessed within the specified period (days)** • **Do not copy file to a local hard drive, if possible**	*(migreert niet)* Kaspersky Endpoint Security scant offline bestanden in hun geheel.

Application Integrity Check

De taakinstellingen voor *Application Integrity Control* (KSWS) worden gemigreerd naar de taak *Programma Integriteitscontrole* (KES).

Rule Generator for Applications Launch Control

Kaspersky Endpoint Security ondersteunt de taak *Applications Launch Control Generator* niet. U kunt regels genereren in Instellingen voor Programmacontrole.

Rule Generator for Device Control

Kaspersky Endpoint Security ondersteunt de taak *Rule Generator for Device Control* niet. U kunt toegangsregels genereren in Instellingen van Apparaatcontrole.

KSWS-componenten migreren

Alvorens de lokale installatie begint, controleert Kaspersky Endpoint Security of er andere Kaspersky-programma's op de computer geïnstalleerd zijn. Als Kaspersky Security for Windows Server op de computer is geïnstalleerd, detecteert KES de set KSWS-componenten die is geïnstalleerd en selecteert dezelfde componenten voor installatie.

KES-componenten die KSWS niet heeft, worden als volgt geïnstalleerd:

- AMSI-bescherming, Host Intrusion Prevention, Remediation Engine worden geïnstalleerd met standaardinstellingen.
- De componenten BadUSB Attack Prevention, Adaptieve controle op afwijkingen, Gegevensencryptie, Detection and Response worden geweigerd.

Bij een externe installatie negeert het KES-programma de set geïnstalleerde KSWS-onderdelen. Het installatieprogramma installeert onderdelen die u selecteert in de eigenschappen van het installatiepakket. Na het installeren van Kaspersky Endpoint Security en het migreren van beleid en taken worden de KES-instellingen geconfigureerd in overeenstemming met KSWS-instellingen.

KSWS-taken en -beleid migreren

U kunt KSWS-beleids- en taakinstellingen op de volgende manieren migreren:

- Met behulp van de Wizard batchconversie beleid en taken (hierna ook "Migratiewizard").

  De migratiewizard voor KSWS is alleen beschikbaar in de beheerconsole (MMC). Beleids- en taakinstellingen kunnen niet worden gemigreerd in de webconsole en cloudconsole.

  De batchconversiewizard werkt anders voor verschillende versies van Kaspersky Security Center. We raden u aan de oplossing te upgraden naar versie 14.2 of hoger. In deze versie van Kaspersky Security Center kunt u met de wizard Batchconversie van beleid en taken een migratie uitvoeren van beleid naar een profiel in plaats van naar een beleid. In deze versie van Kaspersky Security Center kunt u met de wizard Batchconversie van beleid en taken ook een breder scala aan beleidsinstellingen migreren.

- De wizard Nieuw beleid voor Kaspersky Endpoint Security voor Windows gebruiken.

  Met de wizard voor nieuw beleid kunt u KES-beleid maken op basis van een KSWS-beleid.

KSWS-beleidsmigratieprocedures verschillen bij gebruik van de wizard Migratie en de wizard Nieuw beleid.

Batchconversiewizard voor beleid en taken

De migratiewizard draagt KSWS-beleidsinstellingen over naar het beleidsprofiel in plaats van KES-beleidsinstellingen. Het *beleidsprofiel* is een set beleidsinstellingen die op een computer worden geactiveerd als de computer voldoet aan de geconfigureerde activeringsregels. Het apparaattag `UpgradedFromKSWS` is geselecteerd als activeringscriterium van het beleidsprofiel. Kaspersky Security Center voegt automatisch de tag `UpgradedFromKSWS` toe aan alle computers waarop u KES bovenop KSWS installeert met behulp van de installatietaak op afstand. Als je een andere installatiemethode hebt gekozen, kun je de tag handmatig aan apparaten toewijzen.

Een tag aan een apparaat toevoegen:

1. Maak een nieuwe tag aan voor servers — `UpgradedFromKSWS`.

   Voor meer informatie over het aanmaken van tags raadpleegt u de Help van Kaspersky Security Center.

2. Maak een nieuwe beheergroep in de Kaspersky Security Center-console en voeg servers toe waaraan u de tag aan deze groep wilt toewijzen.

   U kunt servers groeperen met behulp van de selectietool. Voor meer informatie over het werken met selecties raadpleegt u de Help van Kaspersky Security Center.

3. Selecteer alle servers van de beheergroep in de Kaspersky Security Center-console, open de eigenschappen van de geselecteerde servers en wijs de tag toe.

Als u meerdere KSWS-beleidsregels migreert, wordt elk beleid geconverteerd naar een profiel binnen één overkoepelend beleid. Als het KSWS-beleid al profielen bevat, worden deze profielen ook als profielen gemigreerd. Het resultaat is dat u één beleid krijgt met profielen voor elk KSWS-beleid.

De wizard Batchconversie voor beleid en taken gebruiken om KSWS-taak- en -beleidsinstellingen te migreren

1. Selecteer Beheerserver in de Beheerconsole en klik met de rechtermuisknop om het contextmenu te openen.
2. Selecteer **All tasks** → **Policies and tasks batch conversion wizard**.

De wizard Batchconversie beleid en taken wordt gestart. Volg de instructies van de wizard.

Stap 1. Het programma selecteren waarvoor u beleid en taken moet converteren

Bij deze stap moet u Kaspersky Endpoint Security voor Windows selecteren. Ga naar de volgende stap.

Stap 2. Conversie van beleid

De migratiewizard maakt KSWS-beleidsprofielen aan binnen een KES-beleid. Selecteer het Kaspersky Security for Windows Server-beleid dat u wilt converteren in beleidsprofielen. Ga naar de volgende stap.

De migratiewizard begint dan met het converteren van het beleid. De namen van nieuwe beleidsprofielen komen overeen met het oorspronkelijke KSWS-beleid.

Stap 3. Rapport beleidsmigratie

De migratiewizard maakt een beleidsmigratierapport. Het beleidsmigratierapport bevat de datum en tijd waarop het beleid werd geconverteerd, de naam van het oorspronkelijke KSWS-beleid, de naam van het doel-KES-beleid en de naam van het nieuwe beleidsprofiel.

Stap 4. Conversie van taken

De migratiewizard maakt nieuwe taken voor Kaspersky Endpoint Security voor Windows. In de takenlijst selecteert u de KSWS-taken die u wilt maken voor Kaspersky Endpoint Security. Nieuwe taken krijgen een naam *<KSWS naam taak> (geconverteerd)*. Ga naar de volgende stap.

Stap 5. Voltooiing van wizard

Verlaat de wizard verlaten. Als gevolg hiervan doet de wizard het volgende:

- Nieuwe beleidsprofielen worden toegevoegd aan het Kaspersky Endpoint Security-beleid.

  Het beleid bevat profielen met de instellingen van Kaspersky Security for Windows Server. Het nieuwe beleid heeft de status *Active*. De Wizard laat het KSWS-beleid ongewijzigd.

- Maakt nieuwe Kaspersky Endpoint Security-taken.

  De nieuwe taken zijn kopieën van KSWS-taken. De Wizard laat de KSWS-taken ongewijzigd.

Het nieuwe beleidsprofiel met KSWS-instellingen krijgt een naam *UpgradedFromKSWS <Naam van het Kaspersky Security for Windows Server-beleid>*. In profieleigenschappen selecteert de migratiewizard automatisch de apparaattag `UpgradedFromKSWS` als het triggercriterium. De instellingen van het beleidsprofiel worden zo automatisch toegepast op servers.

Wizard voor het maken van een beleid op basis van een KSWS-beleid

Wanneer een KES-beleid wordt gemaakt op basis van een KSWS-beleid, draagt de wizard de instellingen dienovereenkomstig over naar het nieuwe beleid. Dat wil zeggen dat één KES-beleid overeenkomt met één KSWS-beleid. De wizard converteert het beleid niet naar een profiel.

De wizard Nieuw beleid gebruiken om KSWS-beleidsinstellingen te migreren

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 **Policies**.
4. Klik op **New policy**.

   De wizard Beleid wordt gestart.
5. Volg de instructies van de wizard Beleid.

Stap 1: Het programma selecteren om groepsbeleid te maken

Selecteer een programma **Kaspersky Endpoint Security for Windows (14.1)**.

Stap 2. Het groepsbeleid een naam geven

Voer een naam in voor het groepsbeleid, bijvoorbeeld *Beleid voor kantoor*.

Selecteer het selectievakje **Use policy settings for an earlier version of the application**. Klik op **Browse** en selecteer het KSWS-beleid.

Stap 3. Deelnemen aan Kaspersky Security Network

Lees en accepteer de voorwaarden van de Kaspersky Security Network-verklaring (KSN).

Stap 4. De programmagebruiksmodus op computers selecteren

Selecteer **Standaardmodus om hosts te beschermen**. Kaspersky Endpoint Security biedt een gemeenschappelijk beleid voor alle applicatiemodi en besturingssysteemtypen.

> We raden aan om verschillende beleidsregels te gebruiken voor verschillende modi en typen besturingssystemen.

Stap 5. Instellingen importeren

> Deze stap is beschikbaar als u handmatige beleidsconfiguratie selecteert bij stap 4.

U kunt een beleid maken op basis van de instellingen van Kaspersky Endpoint Security vanuit een CFG-configuratiebestand. Wanneer u een programma-configuratiebestand importeert, zijn niet alle beleidsinstellingen beschikbaar voor de wizard. Beleidsprofielen ontbreken bijvoorbeeld in programma-instellingen. Als u alle instellingen en profielen wilt overzetten naar het beleid, kunt u: ander beleid importeren vanuit een KLP-bestand.

> Bij het importeren van een configuratiebestand verstuurt Kaspersky Endpoint Security geen wachtwoorden voor crypto-containers. Als u tweerichtingsverificatie gebruikt wanneer u verbinding maakt met servers, moet u een geheel nieuw wachtwoord voor crypto-containers opgeven.

Stap 6 - 10. Beleidsinstellingen configureren

> Deze stap is beschikbaar als u handmatige beleidsconfiguratie selecteert bij stap 4.

Volg de stappen om de beleidsinstellingen te beheren.

Stap 11. De vertrouwde zone configureren

Configureer de vertrouwde zone. U kunt vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's toevoegen. Vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's helpen bij het snel configureren van Kaspersky Endpoint Security op SQL-servers, Microsoft Exchange-servers en System Center Configuration Manager. Dit betekent dat u niet handmatig een vertrouwde zone voor het programma op servers hoeft in te stellen. Vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's kunnen u ook helpen Kaspersky Endpoint Security snel te configureren in de Light Agent-modus in virtuele Citrix- en VMware-omgevingen.

Stap 12. Selecteer de status van het beleid

- **Active**. Na de volgende synchronisatie wordt het beleid gebruikt als het actieve beleid op de computer.

  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.

- **Inactive**. Back-upbeleid. Een inactief beleid kan indien nodig worden geactiveerd.

  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.

- **Out-of-office**. Het beleid wordt geactiveerd wanneer de computer niet meer verbonden is met het bedrijfsnetwerk.

Verlaat de wizard verlaten.

Aanvullende configuratie van beleid en taken na migratie

KSWS en KES hebben verschillende sets onderdelen en beleidsinstellingen. Daarom moet u na de migratie controleren of de beleidsinstellingen voldoen aan de beveiligingsvereisten van uw bedrijf.

Controleer de volgende basisbeleidsinstellingen:

- Wachtwoordbeveiliging. Instellingen voor KSWS-wachtwoordbeveiliging worden niet gemigreerd. Kaspersky Endpoint Security heeft een ingebouwde functie voor wachtwoordbeveiliging. Schakel indien nodig Wachtwoordbeveiliging in en stel een wachtwoord in.

- Vertrouwde zone. De methoden die KSWS en KES gebruiken voor het selecteren van objecten verschillen. Bij het migreren ondersteunt KES uitzonderingen die zijn gedefinieerd als individuele bestanden of paden naar bestand/map. Als KSWS uitzonderingen heeft geconfigureerd als een vooraf gedefinieerd gebied of een script-URL, worden dergelijke uitzonderingen niet gemigreerd. Na de migratie moet u dergelijke uitzonderingen handmatig toevoegen.

  > Om ervoor te zorgen dat Kaspersky Endpoint Security correct werkt op servers, wordt aanbevolen om bestanden die belangrijk zijn voor het functioneren van de server toe te voegen aan de vertrouwde zone. Voor SQL-servers moet u MDF- en LDF-databasebestanden toevoegen. Voor Microsoft Exchange-servers moet u CHK-, EDB-, JRS-, LOG- en JSL-bestanden toevoegen. U kunt bijvoorbeeld maskers gebruiken, bijvoorbeeld `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

  > Beginnend met Kaspersky Endpoint Security 12.6 voor Windows, uitzonderingen scannen en vertrouwde programma's worden toegevoegd aan de vertrouwde zone. Vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's helpen bij het snel configureren van Kaspersky Endpoint Security op SQL-servers, Microsoft Exchange-servers en System Center Configuration Manager. Dit betekent dat u niet handmatig een vertrouwde zone voor het programma op servers hoeft in te stellen.

- Firewall. KSWS Firewall-functies worden uitgevoerd door de firewall op systeemniveau. In KES is een afzonderlijk onderdeel verantwoordelijk voor de Firewall-functionaliteit. Na de migratie kunt u de Kaspersky Endpoint Security Firewall configureren.

- Kaspersky Security Network. Kaspersky Endpoint Security biedt geen ondersteuning voor het configureren van KSN voor individuele onderdelen. Kaspersky Endpoint Security gebruikt KSN voor alle programmaonderdelen. Om KSN te gebruiken, moet u de nieuwe voorwaarden van de Kaspersky Security Network-verklaring accepteren.

- Webcontrole. Blokeerregels voor categoriebeheer van webverkeer worden gemigreerd naar één enkele blokkeerregel in Kaspersky Endpoint Security. Kaspersky Endpoint Security negeert toegestane regels voor categoriebeheer. Kaspersky Endpoint Security ondersteunt niet alle categorieën van Kaspersky Security for Windows Server. Categorieën die niet bestaan in Kaspersky Endpoint Security worden niet gemigreerd. Daarom worden classificatieregels voor webbronnen met niet-ondersteunde categorieën niet gemigreerd. Voeg indien nodig regels toe voor webcontrole.

- Proxyserver. Het wachtwoord voor verbinding met de proxyserver wordt niet gemigreerd. Voer het wachtwoord in dat moet worden gebruikt om handmatig verbinding te maken met de proxyserver.

- Schema's van afzonderlijke onderdelen. Kaspersky Endpoint Security biedt geen ondersteuning voor het configureren van schema's voor afzonderlijke onderdelen. De onderdelen staan altijd aan terwijl Kaspersky Endpoint Security operationeel is.

- Set onderdelen. Welke functies van Kaspersky Endpoint Security beschikbaar zijn, hangt af van het type besturingssysteem: werkstation of server. Van de encryptietools is bijvoorbeeld alleen BitLocker Drive Encryption beschikbaar op servers.

- Attribuut . De status van het attribuut wordt niet gemigreerd. Het attribuut heeft de standaardwaarde. Standaard geldt voor bijna alle instellingen in het nieuwe beleid een verbod op het wijzigen van instellingen in onderliggende beleidsregels en in de lokale programma-interface. Het attribuut heeft de waarde voor beleidsinstellingen in de sectie **Managed Detection and Response (Industrial CyberSecurity)** en in de groep instellingen **Gebruikersondersteuning** (sectie **Interface**). Configureer indien nodig het overnemen van instellingen van het bovenliggende beleid.

- Werken met actieve dreigingen. De geavanceerde desinfectie werkt verschillend voor werkstations en servers. U kunt geavanceerde desinfectie configureren in *Malware-scan*-taakinstellingen en in programma-instellingen.

- Het programma upgraden. Om belangrijke updates en patches te installeren zonder opnieuw op te starten, moet u de upgrademodus van het programma veranderen. Standaard is de functie Programma-updates installeren zonder opnieuw op te starten uitgeschakeld.

- Kaspersky Endpoint Agent beheren. Kaspersky Endpoint Security heeft een ingebouwde agent voor het werken met Detection and Response-oplossingen. Zet indien nodig Kaspersky Endpoint Agent-beleidsinstellingen over naar het Kaspersky Endpoint Security-beleid.

- *Update van databases en programmamodules*-taken. Zorg ervoor dat de instellingen van de *Update van databases en programmamodules*-taak correct gemigreerd zijn. In plaats van de drie taken van KSWS, gebruikt KES een enkele KES-taak. U kunt de *Update van databases en programmamodules*-taken optimaliseren en overbodige taken verwijderen.

- Andere taken. De onderdelen Programmacontrole, Apparaatcontrole en Bestandsintegriteitsmonitor werken verschillend in KSWS en KES. KES gebruikt *Baseline File Integrity Monitor*, *Applications Launch Control Generator*, *Rule Generator for Device Control*-taken niet. Daarom worden deze taken niet gemigreerd. Na de migratie kunt u de onderdelen Bestandsintegriteitsmonitor, Programmacontrole en Apparaatcontrole configureren.

De vertrouwde KSWS-zone migreren

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. U kunt vertrouwde zoneobjecten migreren van KSWS naar KES met behulp van de *Batchconversiewizard voor beleid en taken* of de *wizard voor het maken van een nieuw KES-beleid op basis van het KSWS-beleid*. KSWS en KES hebben verschillende sets onderdelen en functies. Daarom moet u na de migratie controleren of de uitzonderingen voldoen aan de beveiligingsvereisten van uw bedrijf. De methoden voor het toevoegen van uitzonderingen aan de vertrouwde zone zijn ook verschillend voor KES en KSWS. De migratiewizard beschikt niet over hulpmiddelen om alle KSWS-uitzonderingen te migreren. Dit betekent dat u na de migratie handmatig enkele KSWS-uitzonderingen moet toevoegen.

Om ervoor te zorgen dat Kaspersky Endpoint Security correct werkt op servers, wordt aanbevolen om bestanden die belangrijk zijn voor het functioneren van de server toe te voegen aan de vertrouwde zone. Voor SQL-servers moet u MDF- en LDF-databasebestanden toevoegen. Voor Microsoft Exchange-servers moet u CHK-, EDB-, JRS-, LOG- en JSL-bestanden toevoegen. U kunt bijvoorbeeld maskers gebruiken, bijvoorbeeld `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

Beginnend met Kaspersky Endpoint Security 12.6 voor Windows, uitzonderingen scannen en vertrouwde programma's worden toegevoegd aan de vertrouwde zone. Vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's helpen bij het snel configureren van Kaspersky Endpoint Security op SQL-servers, Microsoft Exchange-servers en System Center Configuration Manager. Dit betekent dat u niet handmatig een vertrouwde zone voor het programma op servers hoeft in te stellen.

KES en KSWS vertrouwde methoden voor het maken van zones.

KSWS		KES
Object to scan		
• Predefined scope	*(migreert niet)*	
• Disk, folder or network location	→	**Bestand of map**
• File	→	**Bestand of map**
• Script file or web address	*(migreert niet)*	
Detected object	→	**Type gedetecteerd object**
Trusted processes	→	**Vertrouwde programma's**

Migratie van gescande objecten

KSWS-uitzonderingen waarvoor de **Object to scan**-methode is geselecteerd in hun eigenschappen, worden gemigreerd naar KES-uitzonderingen waarvoor de **Bestand of map**-methode is geselecteerd in hun eigenschappen, met enkele beperkingen. De migratie van een uitzonderingen is afhankelijk van de object-selectiemethode:

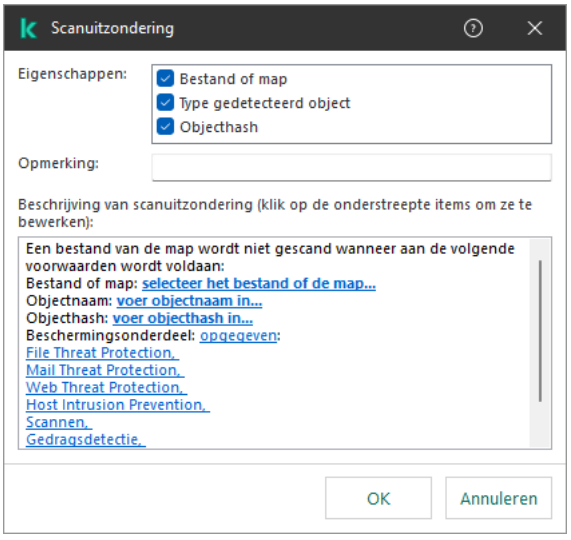
- Predefined scope – *migreert niet*.

  Na de migratie moet u dergelijke uitzonderingen handmatig toevoegen. Uitzonderingen als vooraf gedefinieerde gebieden moeten worden geconfigureerd in de *Malware-scan*-taakinstellingen.

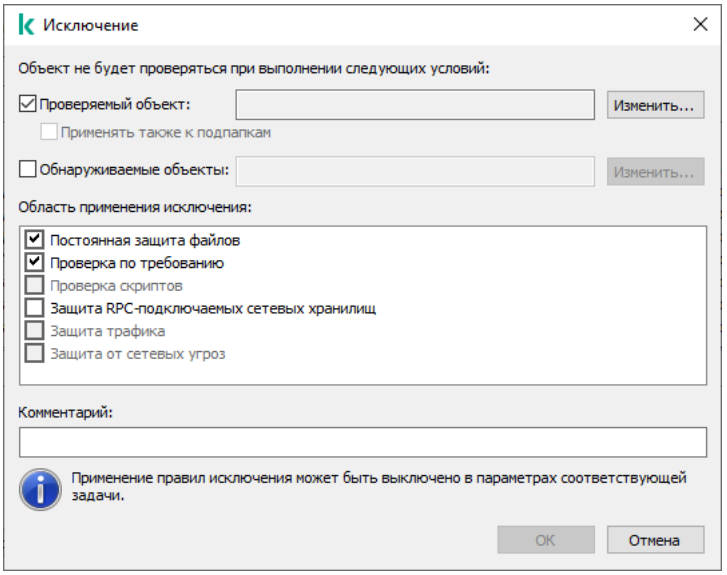
- Disk, folder or network location – migreer naar KES-uitzonderingen waarvoor de methode 'Bestand of map' is geselecteerd in eigenschappen.
- File – migreer naar KES-uitzonderingen waarvoor de methode 'Bestand of map' is geselecteerd in eigenschappen.
- Script file or web address – *migreert niet*.

  Na de migratie moet u dergelijke uitzonderingen handmatig toevoegen. Uitzonderingen als scriptwebadressen moeten worden toegevoegd aan vertrouwde webadressen voor Web Threat Protection.

Als het **Apply also to subfolders** selectievakje is geselecteerd voor het gescande object, wordt deze instelling gemigreerd naar KES-uitzonderingen (het **Inclusief submappen** selectievakje).



KES-uitsluitingsinstellingen



KSWS-uitsluitingsinstellingen

Migratie van gedetecteerde objecten

KSWS-uitzonderingen waarvoor de **Detected object**-methode is geselecteerd in hun eigenschappen, worden gemigreerd naar KES-uitzonderingen waarvoor de **Type gedetecteerd object**-methode is geselecteerd in hun eigenschappen. De naam van het gedetecteerde object komt overeen met de classificatie van de encyclopedie van Kaspersky (bijvoorbeeld `Email-Worm`, `Rootkit` of `RemoteAdmin`). Kaspersky Endpoint Security ondersteunt maskers met het vraagteken `?` (komt overeen met elk afzonderlijk teken) en de asterisk `*` (komt overeen met elke reeks tekens).

Migratie van het gebruiksbereik van uitzonderingen

Het gebruiksbereik van een uitzondering is een set onderdelen waarop de uitzondering van toepassing is. KES en KSWS hebben verschillende sets onderdelen, zodat de migratiewizard het gebruiksbereik van de uitzondering niet kan migreren. Als er ten minste één onderdeel in het KSWS-gebruiksbereik is geselecteerd, past KES de uitzonderingen toe op alle programmaonderdelen.

U kunt het KSWS-gebruiksbereik configureren in de vertrouwde zone-instellingen en ook in de instellingen van KSWS-beveiligingsonderdelen. Om dit te doen, kunt u het **Apply Trusted Zone** selectievakje in het overeenkomstige gedeelte van het beleid in- of uitschakelen. De instellingen van KES-beveiligingsonderdelen bevatten een dergelijk selectievakje niet. Dit betekent dat de status van de vertrouwde zone in de individuele instellingen van het onderdeel bij de migratie verloren gaat. Nadat de migratie is voltooid, selecteer onderdelen waarop de uitzondering van toepassing is in de vertrouwde zone-instellingen in het KES-beleid.

Opmerkingen migreren

Opmerkingen uit de vertrouwde KSWS-zone worden zonder wijzigingen gemigreerd naar de opmerkingen van KES-uitzonderingen.

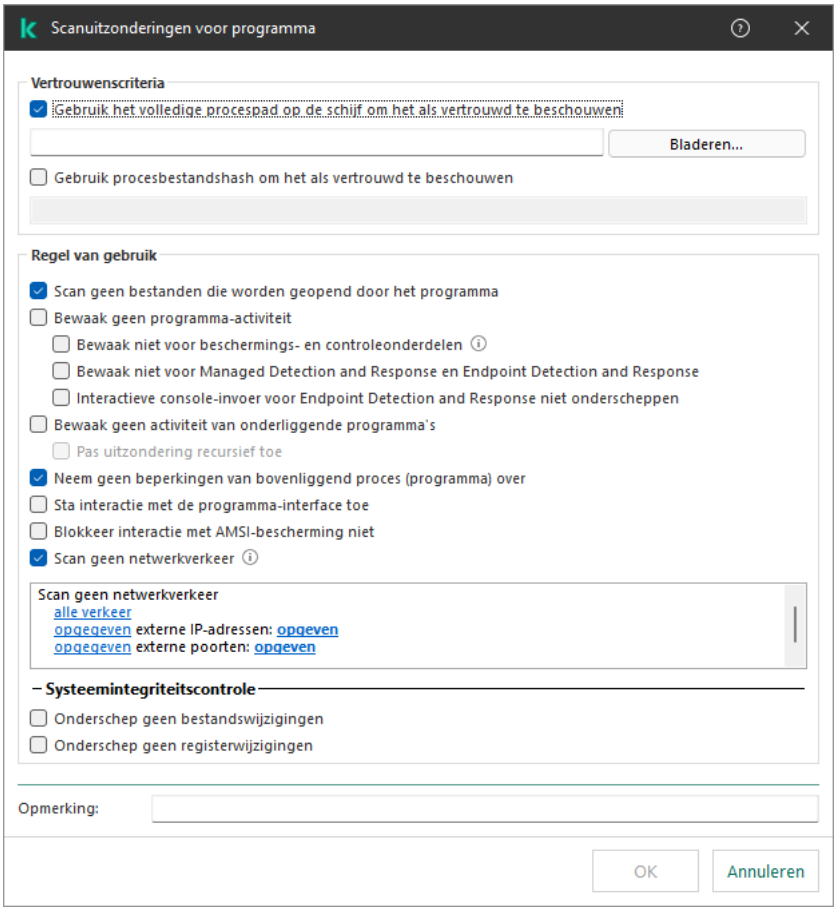
Vertrouwde processen migreren

Vertrouwde KSWS-processen worden met enkele beperkingen gemigreerd naar vertrouwde KES-processen. Het migreren van vertrouwde processen is afhankelijk van de object-selectiemethode:

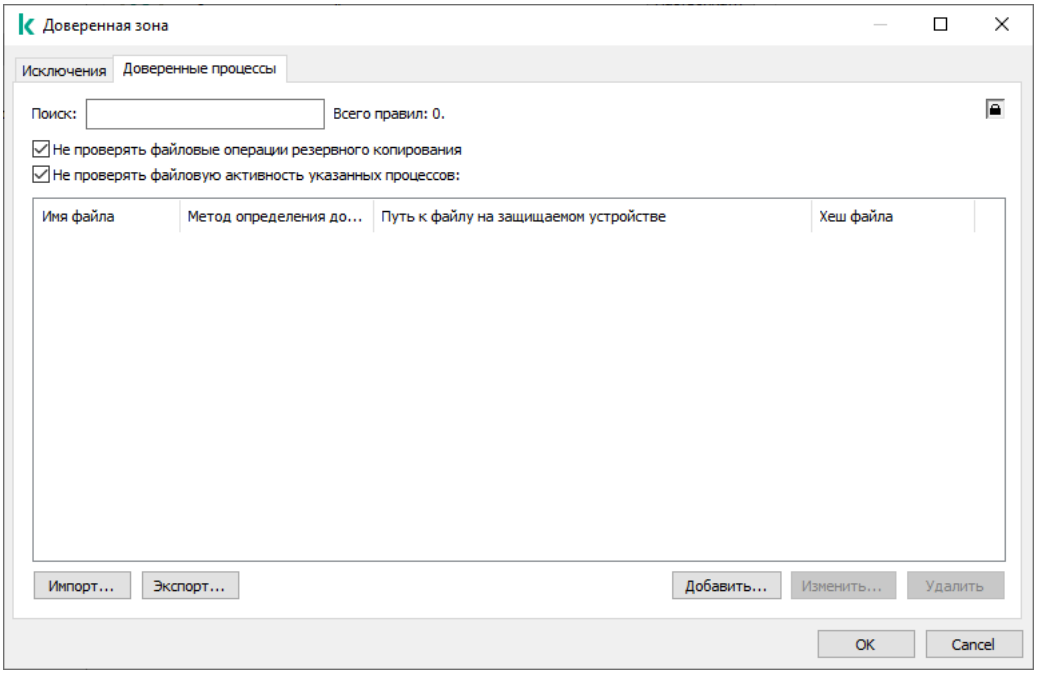
- Path to the file on the protected device – migreert naar vertrouwde KES-programma's.
- File hash – *migreert niet*.

Als KSWS vertrouwde processen heeft geconfigureerd zoals een bestandshash, worden dergelijke vertrouwde processen niet gemigreerd. Na de migratie moet u dergelijke vertrouwde processen handmatig toevoegen.

Als het **Do not check file backup operations** selectievakje is geselecteerd in de vertrouwde procesinstellingen, wordt deze instelling gemigreerd naar vertrouwde KES-programma's (het **Bewaak geen programma-activiteit** selectievakje).



KES vertrouwde programma-instellingen



KSWS vertrouwde procesinstellingen

Migreren van KSWS-programma's Launch Control-regels

Programma's Lanceercontrole van KSWS is standaard bloksgewijs. Dat wil zeggen dat Programma's Lanceercontrole automatisch alle programma's blokkeert die niet in de regels zijn gespecificeerd als toegestane programma's. Daarom stelt de migratiewizard voor KES Programmacontrole automatisch de **Allowlist**-besturingsmodus in, wat overeenkomt met het standaardblokkeringsprincipe.

U kunt regels van KSWS naar KES migreren met behulp van de *Batchconversiewizard voor beleid en taken* of de *wizard voor het maken van een nieuw KES-beleid op basis van het KSWS-beleid*.

De modus van Programma's Lanceercontrole migreren

De modus van KSWS Programma's Lanceercontrole migreert als volgt naar KES Programmacontrole:

- **Statistics only** → **Regels testen**;
- **Active** → **Regels toepassen**.

Migreren van KSWS Programma's Lanceercontrole vooraf gedefinieerde regels

Standaard omvatten regels van programmacontrole van KSWS twee regels:

- **Allow scripts and MSI by OS-trusted certificate**
- **Allow executable by OS-trusted certificate**

Met vooraf gedefinieerde regels kunt u *scripts*, *MSI-pakketten* en *uitvoerbare bestanden* uitvoeren die zijn ondertekend door een vertrouwd basiscertificaat. Als ten minste één vooraf gedefinieerd KSWS-regel het type **Allow** heeft, dan creëert de wizard de migratie een nieuwe regel voor toestaan, **Applications with trusted root certificates**. Dat wil zeggen, KES Programmacontrole gebruikt één enkele regel om het uitvoeren van vertrouwde scripts, MSI-pakketten en uitvoerbare bestanden toe te staan.

Als beide vooraf gedefinieerde KSWS-regels het type **Deny** hebben, negeert KES de vooraf gedefinieerde regels.

Migreren van aangepaste regels voor KSWS Programma's Lanceercontrole

De regels van Programma's Lanceercontrole reguleren de uitvoering van bestanden in overeenstemming met de volgende criteria:

- handtekening met een digitaal certificaat;
- SHA256 hash;
- bestandspad.

Regels worden in KSWS en KES op een andere manier gemaakt. Daarom maakt de migratiewizard *categorieën van programma's* aan, die voorwaarden en uitsluitingen van KSWS-regels bevatten, en voegt deze categorieën van programma's toe aan KES-regels. De wizard gebruikt de voorwaarden **Certificaat**, **Pad naar map**, en **Bestandshash** categorieën van programma's. Nieuwe categorieën van programma's zijn beschikbaar in de Kaspersky Security Center Administration Console in de **Application management** → **Application categories** sectie.

De migratiewizard groepeert KSWS-regels op type en op gebruiker. Vervolgens maakt de wizard categorieën van programma's aan die voorwaarden en uitzonderingen van KSWS-regels bevatten. Vervolgens worden de categorieën van programma's toegevoegd aan nieuwe KES-regels. De wizard specificeert de namen van KSWS-regels in het veld **Beschrijving** van KES-regels.

Geavanceerde instellingen voor KSWS Programma Lanceercontrole migreren

Het werkingsprincipe van KSWS Programma Lanceercontrole en KES Programmacontrole is verschillend, waardoor de migratiewizard slechts een subset van instellingen kan migreren.

Instellingen voor Programma's Launch Control

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
Repeat action taken for the first file launch on all the subsequent launches for this file	*(migreert niet)* Kaspersky Endpoint Security scant het programma elke keer dat het probeert te starten.
Deny the command interpreters launch with no command to execute	*(migreert niet)* Kaspersky Endpoint Security staat het uitvoeren van opdrachtinterpreters toe als ze niet worden verboden door Programmacontrole.
Apply rules to executable files	*(migreert niet)* Het bereik van de regeltoepassing kan niet worden geconfigureerd in de instellingen van Programmacontrole van KES. KES Programmacontrole past regels toe op alle soorten bestanden: uitvoerbare bestanden, scripts en MSI-pakketten. Als alle bestandstypen zijn opgenomen in het toepassingsbereik van de regel in KSWS, neemt KES tijdens de migratie de KSWS-regels over. Als een bepaald bestandstype is uitgesloten van het toepassingsbereik van de regel in KSWS, neemt KES tijdens de migratie ook de KSWS-regels over, maar wordt **Regels testen** geselecteerd als de actie voor Programmacontrole.
Monitor loading of DLL modules	**Het laden van DLL-modules controleren (verhoogt de systeembelasting aanzienlijk)**
Apply rules to scripts and MSI packages	*(migreert niet)* Het bereik van de regeltoepassing kan niet worden geconfigureerd in de instellingen van Programmacontrole van KES. KES Programmacontrole past regels toe op alle soorten bestanden: uitvoerbare bestanden, scripts en MSI-pakketten. Als alle bestandstypen zijn opgenomen in het toepassingsbereik van de regel in KSWS, neemt KES tijdens de migratie de KSWS-regels over. Als een bepaald bestandstype is uitgesloten van het toepassingsbereik van de regel in KSWS, neemt KES tijdens de migratie de KSWS-regels over, maar wordt **Regels testen** geselecteerd als de actie voor Programmacontrole.

Instellingen Kaspersky Security for Windows Server.	Instellingen Kaspersky Endpoint Security voor Windows
Deny applications untrusted by KSN	*(migreert niet)* Kaspersky Endpoint Security houdt geen rekening met de reputatie van programma's en staat wel of niet toe dat programma's volgens de regels worden uitgevoerd.
Allow applications trusted by KSN	Tijdens de migratie voegt KES een nieuwe regel voor toestaan toe. De KL-categorie **Overige software\Programma's, vertrouwd op basis van hun reputatie in KSN** is gespecificeerd als de voorwaarde voor het activeren van de regel.
Users and / or user groups allowed to run applications trusted by KSN	**Gebruikers en hun rechten** in een regel voor Programmacontrole die de KL-categorie bevat **Overige software\Programma's, vertrouwd op basis van hun reputatie in KSN**
Automatically allow software distribution via applications and packages listed	Software Distribution Control in KSWS en KES werkt anders. Tijdens de migratie voegt KES nieuwe regels toe voor het toestaan van programma's waarvoor automatische softwaredistributie is toegestaan. De bestandshash wordt gespecificeerd als voorwaarde voor het activeren van de regel.
Always allow software distribution via Windows Installer	Software Distribution Control in KSWS en KES werkt anders. Tijdens de migratie voegt KES nieuwe regels toe voor het toestaan van programma's waarvoor automatische softwaredistributie is toegestaan (**Software distribution applications and packages allowed**). De bestandshash wordt gespecificeerd als voorwaarde voor het activeren van de regel. In de accounteigenschappen is het selectievakje **Vertrouwde updaters** ingeschakeld.
Always allow software distribution via SCCM using the Background Intelligent Transfer Service	*(migreert niet)*
Software distribution applications and packages allowed	Software Distribution Control in KSWS en KES werkt anders. Tijdens de migratie voegt KES nieuwe regels toe voor het toestaan van programma's waarvoor automatische softwaredistributie is toegestaan. De bestandshash wordt gespecificeerd als voorwaarde voor het activeren van de regel. In de accounteigenschappen is het selectievakje **Vertrouwde updaters** ingeschakeld.
Schedule settings	*(migreert niet)* Als er een planning is geconfigureerd voor het onderdeel in de KSWS-instellingen, wordt het onderdeel Programmacontrole ingeschakeld bij migratie. Als er geen planning is geconfigureerd voor het onderdeel in de KSWS-instellingen, wordt het onderdeel Programmacontrole uitgeschakeld bij migratie. Het is niet mogelijk om voor het onderdeel een aparte planning in te stellen. Het onderdeel staat altijd aan terwijl Kaspersky Endpoint Security operationeel is.

KES installeren in plaats van de KSWS.

U kunt Kaspersky Endpoint Security op de volgende manieren installeren:

- KES installeren na het verwijderen van KSWS (aanbevolen).
- KES installeren bovenop KSWS.

Kaspersky Security for Windows Server verwijderen

U kunt het programma op afstand verwijderen met behulp van de taak *Uninstall application remotely* of lokaal op de server. Mogelijk moet u de server opnieuw opstarten na het verwijderen van KSWS. Als u Kaspersky Endpoint Security wilt installeren zonder opnieuw op te starten, zorg er dan voor dat Kaspersky Security for Windows Server volledig verwijderd is. Als het programma niet volledig verwijderd is kan het installeren van Kaspersky Endpoint Security leiden tot een foutieve werking van de server. Het wordt ook aanbevolen om het programma volledig te verwijderen als u het hulpprogramma Kavremover hebt gebruikt. Het hulpprogramma Kavremover biedt geen ondersteuning voor het beheer van KSWS.

> Als Wachtwoordbeveiliging is ingeschakeld om de toegang tot KSWS te beperken, voert u het verwijderingswachtwoord in de instellingen van het KES-installatiepakket in.

Na het verwijderen van KSWS, installeert u Kaspersky Endpoint Security voor Windows met een van de beschikbare methoden.

Kaspersky Endpoint Security installeren

Wanneer u KES op afstand installeert, worden de onderdelen die u hebt geselecteerd in de eigenschappen van het installatiepakket geïnstalleerd op de server. We raden aan de standaardonderdelen te selecteren in de eigenschappen van het installatiepakket. Een herstart is niet nodig bij het installeren van KES bovenop KSWS.

Alvorens de lokale installatie begint, controleert Kaspersky Endpoint Security of er andere Kaspersky-programma's op de computer geïnstalleerd zijn. Als Kaspersky Security for Windows Server op de computer is geïnstalleerd, detecteert KES de set KSWS-componenten die is geïnstalleerd en selecteert dezelfde componenten voor installatie. Een herstart is niet nodig bij het installeren van KES bovenop KSWS.

> Als het installeren van KES bovenop KSWS mislukt, kunt u de installatie ongedaan maken. Na het ongedaan maken van de installatie is het raadzaam om de server opnieuw op te starten en het opnieuw te proberen.

KSWS-instellingen en -taken worden niet gemigreerd wanneer Kaspersky Endpoint Security voor Windows is geïnstalleerd. Om instellingen en taken te migreren, voert u de wizard Batchconversie van beleid en taken uit.

U kunt de lijst van geïnstalleerde onderdelen controleren in het gedeelte **Beveiliging** van de programma-interface, met de opdracht `status` of in de Kaspersky Security Center-console in computereigenschappen. U kunt de set componenten na installatie wijzigen met behulp van *Programmaonderdelen wijzigen*.

De [KSWS+KEA]-configuratie migreren naar [KES+built-in agent]

Om ondersteuning te bieden voor het gebruik van Kaspersky Endpoint Security for Windows als onderdeel van EDR (KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox, KUMA en MDR werd een ingebouwde agent toegevoegd aan het programma. U hebt geen apart Kaspersky Endpoint Agent-programma meer nodig om met deze oplossingen te werken.

Bij het migreren van KSWS naar KES blijven de oplossingen EDR (KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox, KUMA, en MDR werken met Kaspersky Endpoint Security ingebouwde agents. Daarnaast wordt Kaspersky Endpoint Agent van de computer verwijderd.

Het migreren van de configuratie [KSWS+KEA] naar [KES+ingebouwde agent] omvat de volgende stappen:

1. **Migreren van KSWS naar KES**

   Migreren van KSWS naar KES omvat het installeren van Kaspersky Endpoint Security in plaats van Kaspersky Security for Windows Server.

   Beheerders schakelen doorgaans wachtwoordbeveiliging in om de toegang tot KSWS en KEA te beperken. Vanaf Kaspersky Security Center Linux 15.1, kun je het programma verwijderingswachtwoord invoeren in de *Install application remotely* taakinstellingen. De taak staat de invoer van slechts één verwijderingswachtwoord toe. Dat wil zeggen, als hetzelfde wachtwoord is ingesteld voor KSWS en KEA, worden de KSWS- en KEA-programma's met succes verwijderd. Als de wachtwoorden verschillend zijn, mislukt het verwijderen van een van de programma's met een toegangsfout. Om de migratie te voltooien, moet u Wachtwoordbeveiliging uitschakelen voor het programma waarvan u het wachtwoord niet kon invoeren in de instellingen van de *Install application remotely* taak.

   Om de migratie uit te voeren, moet u de onderdelen selecteren die nodig zijn om Detection and Response-oplossingen te ondersteunen als onderdeel van Kaspersky Endpoint Security. Na het installeren van het programma schakelt Kaspersky Endpoint Security over op het gebruik van de ingebouwde agent en wordt Kaspersky Endpoint Agent verwijderd.

2. **Het beleid en de taken migreren**

   Het migreren van [KSWS+KEA] beleid en taken naar [KES+ingebouwde agent] omvat de volgende stappen:

   1. Beleid en taken migreren van KSWS naar KES met behulp van de wizard Batchconversie van beleid en taken (alleen beschikbaar in de Beheerconsole (MMC)).

      Als resultaat wordt een beleidsprofiel met de naam *UpgradedFromKSWS <Naam van het beleid van Kaspersky Security for Windows Server>* toegevoegd aan het KES-beleid. Nieuwe KES-taken worden ook aangemaakt met de namen *<KSWS-taaknaam> (geconverteerd)*.

   2. Beleid en taken migreren van KEA naar KES met behulp van de wizard voor migratie van Kaspersky Endpoint Agent (alleen beschikbaar op de webconsole en cloudconsole).

      Als resultaat wordt een nieuw beleid gemaakt met de naam *<Naam van het Kaspersky Endpoint Security-beleid> & <Naam van het Kaspersky Endpoint Agent-beleid>*. Er worden ook nieuwe taken en KES-taken gemaakt.

3. **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 Add-on-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 *Add key*.

   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.

   Alleen de Kaspersky Anti Targeted Attack Platform-licentie kan worden gebruikt om Kaspersky Endpoint Security te activeren als onderdeel van de Kaspersky Anti Targeted Attack Platform-oplossing. Nadat u het programma hebt geüpgraded naar versie 12.1, wordt de EDR (KATA)-functionaliteit automatisch geactiveerd. U hoeft verder niets te doen.

4. **De status van Kaspersky Endpoint Detection and Response Optimum en Kaspersky Sandbox controleren**

   Als de computer na de upgrade de status *Critical* heeft in de Kaspersky Security Center-console:

   - Zorg ervoor dat op de computer Netwerkagent versie 13.2 of hoger is geïnstalleerd.
   - Controleer de werkingsstatus van het ingebouwde agent door het *Report on status of application components* te bekijken. Als een onderdeel de status *Not installed* heeft, installeer dan de onderdeel met de taak *Change application components*.
   - 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 *Report on status of application components* dat de EDR Optimum-functionaliteit is geactiveerd. Als een onderdeel de status *Geen onderdeel van licentie* heeft, zorg er dan voor dat de functie voor automatische distributie van licentiesleutels van EDR Optimum is ingeschakeld.

Ervoor zorgen dat Kaspersky Security for Windows Server met succes is verwijderd

Zorg ervoor dat Kaspersky Security for Windows Server volledig verwijderd is:

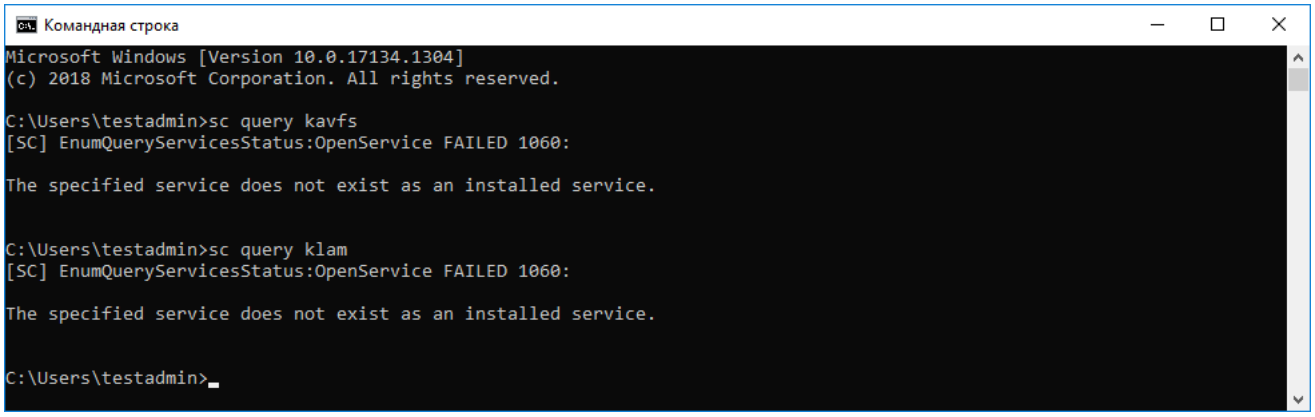
- De map `%ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\` bestaat niet.
- De volgende diensten zijn niet aanwezig:
  - Kaspersky Security Service (KAVFS)
  - Kaspersky Security Management service (KAVFSGT)

- Kaspersky Security Exploit Prevention service (KAVFSSLP)
- Kaspersky Security Script Checker service (KAVFSSCS)

U kunt actieve services controleren in Taakbeheer of met de opdracht `sc query` (zie onderstaande afbeelding).

- De volgende stuurprogramma's zijn niet aanwezig:
  - klam.sys
  - klflt.sys
  - klramdisk.sys
  - klelaml.sys
  - klfltdev.sys
  - klips.sys
  - klids.sys
  - klwtpee

  U kunt de geïnstalleerde stuurprogramma's controleren in de map `C:\Windows\System32\drivers` of door het verzenden van de opdracht `sc query`. Als er een service of stuurprogramma ontbreekt, krijgt u het volgende antwoord:



Ervoor zorgen dat Kaspersky Security for Windows Server-services en -stuurprogramma's met succes zijn verwijderd

Als er programma- of stuurprogrammabestanden op de server achterblijven, verwijdert u de relevante bestanden handmatig. Als Kaspersky Security for Windows Server-services nog steeds actief zijn op de server, stop de services dan (`sc stop`) en verwijder ze (`sc delete`) 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 for Windows Server (KSWS). Het activeringsproces na migratie is afhankelijk van de KSWS-activeringsmethode (zie onderstaande tabel).

Kaspersky Endpoint Security biedt geen ondersteuning voor de licentie van *Kaspersky Security for Storage*. Om met deze licentie te werken, moet u Kaspersky Security for Windows Server gebruiken.

Om KES te activeren met de KSWS-sleutel kunt u enkel de activatiecode gebruiken. Als u een licentiebestand gebruikt om het programma te activeren, dan moet u contact opnemen met de Technische Support voor een Kaspersky Endpoint Security-licentiebestand.

Kaspersky Endpoint Security voor Windows activeren met een Kaspersky Security for Windows Server-code

Kaspersky Security for 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 wordt toegevoegd door een taak	Als uw KSWS wordt geactiveerd met behulp van de taak, wordt de KSWS-licentiecode verwijderd tijdens de migratie van KSWS. U moet het programma opnieuw activeren. U kunt bijvoorbeeld een licentiecode toevoegen aan het Kaspersky Endpoint Security voor Windows-installatiepakket.
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 een licentiecode toevoegen aan het Kaspersky Endpoint Security voor Windows-installatiepakket.
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 een licentiecode toevoegen aan het Kaspersky Endpoint Security voor Windows-installatiepakket.
Betaalde virtuele machine-image (Amazon Machine Image – AMI) in Amazon Web Services (AWS).	Als u Kaspersky Security Center hebt gekocht als een betaalde image van een virtuele machine (Amazon Machine Image – AMI) in Amazon Web Services (AWS), hoeft u KES niet te activeren. In dit geval gebruikt Kaspersky Security Center het AWS-abonnement dat al aan het programma is toegevoegd.
Kant-en-klare gratis Kaspersky Security Center-image met uw eigen licentie (Bring Your Own License – BYOL-model).	Als u een out-of-the-box gratis Kaspersky Security Center-image gebruikt met uw eigen licentie in een cloudomgeving (het Bring Your Own License – BYOL-model), moet u het programma activeren met behulp van een beschikbare methode. U hebt een Kaspersky Hybrid Cloud Security-licentie nodig.

Speciale overwegingen voor het migreren van zwaarbelaste servers

Op zwaarbelaste servers is het belangrijk om de prestaties te bewaken en fouten te voorkomen. Na de migratie naar Kaspersky Endpoint Security voor Windows raden we aan om programmacomponenten die veel serverbronnen gebruiken in vergelijking met andere componenten tijdelijk uit te schakelen. Nadat u ervoor hebt gezorgd dat de server normaal presteert, kunt u de programmacomponenten weer inschakelen.

We raden aan om servers met een hoge belasting als volgt te migreren:

1. Maak een Kaspersky Endpoint Security-beleid met standaardinstellingen.

   Standaardinstellingen worden als optimaal beschouwd. Deze instellingen worden aanbevolen door Kaspersky-experts. Standaardinstellingen bieden aanbevolen beschermingsniveau en optimaal gebruik van bronnen.

2. Schakel in de beleidsinstellingen de volgende onderdelen uit: Network Threat Protection, Gedragsdetectie, Exploit-preventie, Remediation Engine, Programmacontrole.

   Als uw organisatie de Kaspersky Managed Detection and Response (MDR)-oplossing heeft geïmplementeerd, upload het BLOB-configuratiebestand dan naar het Kaspersky Endpoint Security-beleid.

3. Verwijder Kaspersky Security for Windows Server van de server.

4. Installeer Kaspersky Endpoint Security voor Windows met de standaardset onderdelen.

   Als uw organisatie Detection and Response-oplossingen heeft geïmplementeerd, selecteert u de relevante onderdelen in de eigenschappen van het installatiepakket.

5. Controleer de instellingen van het programma:

   - Het programma wordt geactiveerd met de KSWS-licentiecode.
   - Het nieuwe beleid wordt toegepast. Eerder geselecteerde onderdelen worden uitgeschakeld.

6. Controleer of de server werkt. Zorg ervoor dat Kaspersky Endpoint Security voor Windows niet meer dan 1% van de serverbronnen gebruikt.

7. Maak indien nodig scanuitzonderingen, voeg vertrouwde programma's toe en maak een lijst met vertrouwde webadressen.

8. Schakel de onderdelen Gedragsdetectie, Exploit-preventie en Remediation Engine in. Zorg ervoor dat Kaspersky Endpoint Security voor Windows niet meer dan 1% van de serverbronnen gebruikt.

9. Schakel het onderdeel Network Threat Protection in. Zorg ervoor dat Kaspersky Endpoint Security voor Windows niet meer dan 2% van de serverbronnen gebruikt.

10. Schakel het onderdeel Programmacontrole in regeltestmodus.

11. Zorg ervoor dat programmacontrole werkt. Voeg indien nodig nieuwe regels voor programmacontrole toe en schakel de regeltestmodus uit nadat u hebt bevestigd dat programmacontrole werkt.

Controleer na de migratie van KSWS naar KES of het programma correct werkt. Controleer de status van de server in de console (moet *OK* zijn). Zorg ervoor dat er geen fouten worden gerapporteerd voor het programma, controleer ook het tijdstip van de laatste verbinding met de beheerserver, het tijdstip van de laatste database-update en de serverbeveiligingsstatus.

Het programma beheren op een server in Server Core-modus

Een server in de Server Core-modus 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 server in Server Core-mode 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 een server in Server Core-modus 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 een server in Server Core-modus omvat de volgende speciale overwegingen:

- De server in Server Core-modus 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 *Malware-scan*. Vervolgens moet u de *Malware-scan* 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 server in Server Core-modus te installeren:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /s
```

Voer de volgende opdracht uit om het programma te activeren:

```
avp.com license /add <activation code or key file>
```

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
```

Migreren van [KSWS+KEA] naar [KES+built-in agent]

Bij het migreren van Kaspersky Security for Windows Server (KSWS) naar Kaspersky Endpoint Security (KES), kunt u de volgende aanbevelingen gebruiken om de serverbeveiliging te configureren en de prestaties te optimaliseren. Hier kijken we naar een migratievoorbeeld voor een enkele organisatie.

Infrastructuur van de organisatie

Het bedrijf heeft de volgende apparatuur geïnstalleerd:

- Kaspersky Security Center 14.2

  De beheerder beheert Kaspersky-oplossingen met behulp van de Beheerconsole (MMC). Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) is ook ingezet

  In Kaspersky Security Center worden drie beheergroepen gemaakt, die de servers van de organisatie bevatten: twee beheergroepen voor SQL-servers en een beheergroep voor Microsoft Exchange-servers. Elke beheergroep heeft een eigen beleid. De taken *Database Update* en *On-demand scan* worden gemaakt voor alle servers in de organisatie.

  De KSWS-activeringssleutel wordt toegevoegd aan Kaspersky Security Center. Automatische codedistributie is ingeschakeld.

- SQL-servers waarop Kaspersky Security for Windows Server 11.0.1 en Kaspersky Endpoint Agent 3.11 geïnstalleerd zijn. De SQL-servers worden in twee clusters gecombineerd.

  KSWS wordt beheerd door het *SQL_Policy(1)*-beleid en het *SQL_Policy(2)*-beleid. De taken *Database Update* en *On-demand scan* worden ook gemaakt.

- Een Microsoft Exchange-server met Kaspersky Security for Windows Server 11.0.1 en Kaspersky Endpoint Agent 3.11 geïnstalleerd.

  KSWS wordt beheerd door het *Exchange_Policy*-beleid. De taken *Database Update* en *On-demand scan* worden ook gemaakt.

Plannen van de migratie

De migratie omvat de volgende stappen:

1. KSWS-taken en beleid migreren met behulp van de wizard Batchconversie van beleid en taken.
2. Het beleid van Kaspersky Endpoint Agent migreren met behulp van de wizard Batchconversie van beleid en taken.
3. Tags gebruiken om beleidsprofielen te activeren in de eigenschappen van het nieuwe beleid.
4. KES installeren in plaats van de KSWS.
5. EDR Optimum activeren.
6. Bevestigen dat KES werkt.

Het migratiescenario wordt eerst uitgevoerd op een van de clusters van de SQL-servers. Vervolgens wordt het migratiescenario uitgevoerd op de andere cluster SQL-servers. Vervolgens wordt het migratiescenario uitgevoerd op de Microsoft Exchange.

KSWS-taken en beleid migreren met behulp van de wizard Batchconversie van beleid en taken

Om KSWS-taken te migreren, kunt u de wizard Batchconversie van beleid en taken gebruiken (de migratiewizard). Als gevolg hiervan krijgt u in de plaats van het *SQL_Policy(1)*-, *SQL_Policy(2)*- en *Exchange_Policy*-beleid één beleid met drie profielen voor respectievelijk SQL- en Microsoft Exchange-servers. Het nieuwe beleidsprofiel met KSWS-instellingen krijgt een naam *UpgradedFromKSWS <Naam van het Kaspersky Security for Windows Server-beleid>*. In profieleigenschappen selecteert de migratiewizard automatisch de apparaattag `UpgradedFromKSWS` als het triggercriterium. De instellingen van het beleidsprofiel worden zo automatisch toegepast op servers.

Het beleid van Kaspersky Endpoint Agent migreren met behulp van de wizard Batchconversie van beleid en taken

Om een Kaspersky Endpoint Agent-beleid te migreren, kunt u de wizard batchconversie beleid en taken gebruiken. De wizard Migratie van beleid en taken voor Kaspersky Endpoint Agent is alleen beschikbaar in de webconsole.

Tags gebruiken om beleidsprofielen te activeren in de eigenschappen van het nieuwe beleid

Selecteer de apparaattag die u eerder hebt toegewezen als voorwaarde voor profielactivering. Open de beleidseigenschappen en selecteer *General rules for policy profile activation* als voorwaarde voor profielactivering.

KES installeren in plaats van de KSWS.

Voordat u KES installeert, moet u wachtwoordbeveiliging uitschakelen in de KSWS-beleidseigenschappen.

Het installeren van KES omvat de volgende stappen:

1. Bereid het installatiepakket voor. Selecteer in de eigenschappen van het installatiepakket de Kaspersky Endpoint Security voor Windows 12.0-distributiekit en selecteer de standaardset onderdelen.

2. Maak een *Install application remotely*-taak aan voor een van de beheergroepen van de SQL-server.

3. Selecteer in taakeigenschappen het installatiepakket en het licentiebestand.

4. Wacht tot de taak voltooid is.

5. Herhaal de KES-installatie voor de overige beheergroepen.

Kaspersky Security Center voegt automatisch de tag `UpgradedFromKSWS` toe aan namen van computers op de console nadat de KES-installatie voltooid is.

Om de KES-installatie te controleren, kunt u *Report on protection deployment* gebruiken. U kunt ook de apparaatstatus controleren. Om de activering van het programma te bevestigen, kunt u *Report on usage of license keys* gebruiken.

EDR Optimum activeren

U kunt de EDR Optimum-functie activeren met een alleenstaande licentie voor de invoegtoepassing Kaspersky Endpoint Detection and Response Optimum. U moet bevestigen dat de EDR Optimum-sleutel is toegevoegd aan de Kaspersky Security Center-opslagplaats en dat de automatische distributie van licentiecodes is ingeschakeld.

Om de activering van EDR Optimum te controleren, kunt u *Report on status of application components* gebruiken.

Bevestigen dat KES werkt

Om te bevestigen dat KES werkt, kunt u controleren of er geen fouten worden gerapporteerd. De apparaatstatus moet *OK* zijn. Update- en malwarescantaken succesvol voltooid.

Light Agent-modus om virtuele machines te beschermen

Vanaf versie 12.8 kunt u Kaspersky Endpoint Security voor Windows gebruiken als onderdeel van Kaspersky Security for Virtualization Light Agent. *Kaspersky Security for Virtualization Light Agent* iis een geïntegreerde oplossing die uitgebreide bescherming biedt voor virtuele machines tegen verschillende soorten bedreigingen voor de informatiebeveiliging, netwerkaanvallen en phishing-aanvallen. Om deze oplossing te gebruiken, moet u het programma installeren in de Light Agent-modus.

De installatie van Kaspersky Endpoint Security in de Light Agent-modus op virtuele machines met Arm wordt niet ondersteund.

Vanaf versie 6.2 kunt u Kaspersky Endpoint Security in de Light Agent-modus gebruiken als onderdeel van Kaspersky Security for Virtualization Light Agent.

Wanneer u Light Agent start, wordt er een verbinding met de virtuele machine SVM tot stand gebracht en onderhouden (Secure Virtual Machine). Er is een Protection Server geïmplementeerd op de SVM. De *Protection Server* is het onderdeel van de Kaspersky Security for Virtualization Light Agent-oplossing dat bestanden scant op virussen en andere malware, antivirusdatabases bijwerkt en licentiesleutels beheert. Light Agent stuurt bestanden of fragmenten ervan die gescand moeten worden naar de SVM. De scanresultaten zijn beschikbaar voor alle virtuele machines waarop Light Agent is geïnstalleerd (de SharedCache-technologie). Deze technologie verhoogt de efficiëntie van de oplossing en zorgt voor een snellere reactie op bedreigingen.

De infrastructuur van de organisatie kan veel virtuele machines met Light Agent geïnstalleerd en veel SVM's bevatten. De integratieserver zorgt voor de interactie tussen virtuele machines en SVM's. De *integratieserver* is een onderdeel van de Kaspersky Security for Virtualization Light Agent dat een lijst met beschikbare SVM's genereert en deze gegevens doorstuurt naar Light Agents, ontdekking van SVM's door Light Agents, de verbinding tussen Light Agents en SVM's beveiligt en andere functies vervult .

Speciale overwegingen voor de Light Agent-modus

U kunt Kaspersky Endpoint Security beheren in de Standaardmodus en de Light Agent-modus met behulp van Kaspersky Endpoint Security-beleid en -taken. In de Light Agent-modus zijn sommige onderdelen en functies van het programma niet beschikbaar.

Databases en softwaremodules van het programma bijwerken

Kaspersky Endpoint Security in de Light Agent-modus maakt gebruik van speciale malwaredatabases die het programma nodig heeft om te werken als onderdeel van de Kaspersky Security for Virtualization Light Agent-oplossing. Kaspersky Endpoint Security ontvangt databases en programmamodule-updates van de Protection Server.

Databases en modules op beveiligde virtuele machines worden bijgewerkt met behulp van een speciale taak *Update van databases en programmamodules*, waarin een map op de SVM wordt opgegeven als de updatebron. Light Agent voert de *Update van databases en programmamodules* taak automatisch uit. U kunt geen andere updatebron selecteren, de taakplanning configureren of de taak verwijderen.

Het terugdraaien van de laatste update van de malware-database wordt ook door de Protection Server afgehandeld. Na het terugdraaien van een update van de databases en applicatiemodules op de SVM, wordt een speciale lokale *Update van databases en programmamodules* taak gestart op de beveiligde virtuele machine. Door deze taak gaat de Light Agent terug naar de vorige set malware-databases.

Kaspersky Endpoint Security in de Light Agent-modus ondersteunt de taak *Update terugdraaien* niet.

Light Agent activeren

Om het programma te activeren, moet u een licentiesleutel toevoegen aan de SVM waarmee de Light Agent is verbonden. U hoeft het programma niet apart te activeren.

Andere speciale overwegingen voor de Light Agent-modus

- Wanneer u een beleid voor het programma maakt, raden wij u aan de Light Agent-modus te selecteren. In deze modus vraagt de Nieuwe beleidswizard u om de SVM-verbinding te configureren. Deze instellingen zijn vereist om het programma in de Light Agent-modus te laten werken.
- U kunt geen Onderdelen voor gegevensencryptie en Adaptieve controle op afwijkingen installeren in de Light Agent-modus. De set onderdelen is ook afhankelijk van het type gastbesturingssysteem: werkstation of server.
- Light Agent ondersteunt geen integratie met de oplossingen Kaspersky Endpoint Detection and Response Expert en Kaspersky Endpoint Detection and Response Expert (cloud).
- U kunt Light Agent beheren via de Beheerder (MMC) en de Kaspersky Security Center Webconsole. Het is niet mogelijk om Light Agent te beheren in de Kaspersky Security Center Cloudconsole.
- Het wijzigen van de set programma-onderdelen op VDI-virtuele machines wordt niet ondersteund.
- Kaspersky Endpoint Security communiceert met KSN-servers via een KSN proxyserver. Directe communicatie met KSN wordt niet ondersteund.
- De Cloudmodus van Kaspersky Security Network wordt niet ondersteund.
- Het gebruik van de proxyserver van het programma bij verbinding met de Integrationserver (VIIS), de Protection Server (SVM) en KSN-servers wordt niet ondersteund.

Voorlopige configuratie van de virtuele machine

U kunt Kaspersky Endpoint Security installeren op een virtuele machine die gebruikmaakt van virtuele platformtechnologie. Kaspersky Endpoint Security ondersteunt VMware, Microsoft Hyper-V, virtuele Citrix-platforms. Vóór de installatie moet u de voorlopige configuratie van de virtuele machines uitvoeren.

Compatibiliteit met Citrix App Layering-technologie

Als u van plan bent de Full User Layer om de status van de tijdelijke virtuele machines op te slaan, moet u het volgende doen voordat u virtuele machines op de sjabloon installeert:

1. Maak de C:\Program Files\Unidesk\Uniservice\UserExclusions\KESLA.txt bestand en voeg de volgende uitzonderingen toe:

   - `C:\ProgramData\KasperskyLab\`
   - `C:\ProgramData\Kaspersky Lab\`
   - `C:\Program Files (x86)\Kaspersky Lab\`

2. In het register van het besturingssysteem, in de HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Unifltr sleutel, maak een nieuwe DWORD-waarde met de naam MiniFilterBypass en stel deze in op 1.

3. In het register van het besturingssysteem in de HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Unirsd sleutel, maak een nieuwe MULTI_SZ-waarde met de naam ExcludeKey en stel deze in op \Registry\Machine\SOFTWARE\WOW6432Node\KasperskyLab.

4. Start de virtuele machine opnieuw op.

Voor installatie op virtuele machines in een infrastructuur die gebruikmaakt van Citrix App Layering, moet u het volgende doen:

1. Installeer de Kaspersky Security Center Administration Agent en Kaspersky Endpoint Security for Windows op de virtuele-machinesjabloon in de programmalaag.

2. Maak een image van een virtuele machine die uit meerdere lagen bestaat.

3. Implementeer de gemaakte afbeelding op hypervisors die de Citrix App Layering-oplossing ondersteunen.

4. Configureer het maken van tijdelijke virtuele machines op basis van de gemaakte afbeelding.

Voor meer informatie over de installatie van antivirussoftware naast Citrix App Layering, raadpleeg de Citrix App Layering-documentatie.

Compatibiliteit met Citrix Provisioning (Citrix Provisioning Services) technologie

Om ervoor te zorgen dat het programma compatibel is met de Citrix Provisioning-technologie (Citrix Provisioning Services):

- Als de Citrix Provisioning Target Device-software op de virtuele machine is geïnstalleerd, moet u deze verwijderen voordat u het Kaspersky Endpoint Security-programma installeert (voor meer informatie kunt u de website van de technische ondersteuning van Citrix raadplegen). Na het installeren van het programma moet u Citrix Provisioning Target Device opnieuw installeren.

- Bij het installeren van het programma met behulp van de installatiewizard of op afstand met Kaspersky Security Center, moet u de **Zorg voor compatibiliteit met Citrix PVS** selectievakje selecteren.

Compatibiliteit met Omnissa App Volumes-technologie

Voordat u op de sjabloon voor virtuele machines installeert, moet u het %SVAgent%\Config\Custom\snapvol.cfg bestand en voeg de volgende uitzonderingen toe:

- `exclude_path=\ProgramData\Kaspersky Lab`
- `exclude_path=\ProgramData\KasperskyLab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files\Common Files\Kaspersky Lab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files\Kaspersky Lab`
- `exclude_process_name=avp.exe`
- `exclude_process_name=klnagent.exe`
- `exclude_registry=\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\KasperskyLab`
- `exclude_registry=\REGISTRY\MACHINE\SOFTWARE\KasperskyLab`

- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_arkmon`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klark`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klbg`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_mark`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_swmon`

Raadpleeg de Omnissa-documentatie voor meer informatie.

Light Agent installeren

De installatie van Kaspersky Endpoint Security in de Light Agent-modus op virtuele machines met Arm wordt niet ondersteund.

Het installeren van het programma in de Light Agent-modus verloopt op dezelfde manier als in de Standaardmodus. Voordat u Light Agent op een virtuele machine installeert, moet u ervoor zorgen dat Kaspersky Security Center Network Agent is geïnstalleerd. *Netwerkagent* vereenvoudigt de interactie tussen Administration Server en een virtuele machine.

Light agent kan op een van de volgende manieren op een virtuele machine worden geïnstalleerd:

- Op afstand via Kaspersky Security Center.
- Lokaal met behulp van de Installatiewizard.
- Lokaal via de opdrachtregel.

Om Light agent te installeren, moet u de juiste configuratie selecteren in de Instellingen van het installatiepakket of in de Installatiewizard.

Wanneer u Light Agent op een server installeert, worden geavanceerde beschermingsonderdelen (Gedragsdetectie, Exploitpreventie, Remediation Engine) uitgesloten van de standaardconfiguratie van het programma. De standaard programma-instellingen bieden het aanbevolen beschermingsniveau en optimaal gebruik van serverbronnen. Bij installatie van Light Agent op een werkstation worden geavanceerde beschermingsonderdelen opgenomen in de standaardconfiguratie van het programma.

Bij de installatie van Light Agent adviseren wij u om vooraf gedefinieerde uitzonderingen en vertrouwde programma's voor de relevante virtuele omgeving te selecteren. Met vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's kunt u het programma snel instellen en compatibiliteitsproblemen met virtuele omgevingen voorkomen. U kunt ook na de installatie in het beleid vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's configureren.

Wanneer u Light Agent op permanente virtuele machines installeert, moet u mogelijk het algoritme voor het genereren van de Sensor ID wijzigen. (Sensor ID) wordt in de oplossing Kaspersky Anti Targeted Attack Platform gebruikt om computers te identificeren die telemetrie naar de server sturen. Om een unieke Sensor ID te maken, stel `EnableUniqueSensorID=1` in wanneer u het programma op de opdrachtregel installeert.

Hoe Light agent installeren met behulp van de Installatiewizard

1. Kopieer de distributiekit map naar de virtuele machine.
2. Voer setup_kes.exe uit.

   De Installatiewizard wordt gestart.

Configuratie van Kaspersky Endpoint Security



De configuratie van het programma kiezen

Selecteer de **Light Agent om virtuele omgevingen te beschermen** configuratie. Deze configuratie is bedoeld voor het programma die wordt gebruikt als onderdeel van de Kaspersky Security for Virtualization Light Agent-oplossing. Light Agent moet worden geïnstalleerd op elke virtuele machine die met de oplossing moet worden beschermd. In deze configuratie kunt u geen Onderdelen voor gegevensencryptie of Adaptieve controle op afwijkingen gebruiken. Als u Light Agent installeert op een virtuele machinesjabloon die zal worden gebruikt om *niet-permanente virtuele machines* te maken, schakel dan het selectievakje **Bescherm de VDI-infrastructuur** (VDI staat voor Virtual Desktop Infrastructure). De VDI-beschermingsmodus helpt de prestaties van Kaspersky Endpoint Security op niet-permanente virtuele machines te optimaliseren. In deze modus weigert Light Agent programma-updates waarvoor de virtuele machine opnieuw moet worden opgestart. Bij het ontvangen van programma-updates die een herstart vereisen, genereert Light Agent een event over de noodzaak om de template van de beschermde virtuele machines bij te werken.

Kaspersky Endpoint Security-onderdelen

Selecteer de onderdelen die u wilt installeren (zie onderstaande afbeelding). 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.

Geavanceerde instellingen



Geavanceerde instellingen van programma-installatie

Bescherm het installatieproces van het programma. 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 Remote Desktop), wordt u aanbevolen de bescherming van het installatieproces uit te schakelen.

Zorg voor compatibiliteit met Citrix PVS. U kunt de ondersteuning voor Citrix Provisioning Services inschakelen om Kaspersky Endpoint Security op een virtuele machine te installeren.

Voeg het pad naar het bestand avp.com toe aan de systeemvariabele %PATH%. U kunt het pad voor de installatie toevoegen aan de variabele %PATH% om de opdrachtregel-interface eenvoudig te gebruiken.

Light Agent installeren met behulp van de opdrachtregel

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 /pLIGHTAGENTMODE=1 [/pVDI=1] [/s]
   ```

   of

   ```
   msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 LIGHTAGENTMODE=1 [VDI=1] [/qn]
   ```

   De `VDI` optie schakelt de VDI (Virtual Desktop Infrastructure) beschermingsmodus in. De VDI-beschermingsmodus helpt de prestaties van Kaspersky Endpoint Security op niet-permanente virtuele machines te optimaliseren. In deze modus weigert Light Agent programma-updates waarvoor de virtuele machine opnieuw moet worden opgestart. Bij het ontvangen van programma-updates die een herstart vereisen, genereert Light Agent een event over de noodzaak om de template van de beschermde virtuele machines bij te werken. Standaard is de VDI-beschermingsmodus uitgeschakeld.

Hierdoor wordt Light Agent op de virtuele machine geïnstalleerd met de standaardset onderdelen. U kunt de set onderdelen bewerken en geavanceerde instellingen opgeven met behulp van het bestand setup.ini. U kunt de installatie-instellingen ook op de opdrachtregel opgeven.

Light Agent installeren met behulp van de Beheerconsole (MMC)

1. Open de Beheerconsole van Kaspersky Security Center.
2. Selecteer in de consolestructuur de map **Advanced** → **Remote installation** → **Installation packages**.

   Er wordt een lijst geopend met installatiepakketten die zijn gedownload naar Kaspersky Security Center.
3. Open de eigenschappen van het installatiepakket van Kaspersky Endpoint Security voor Windows.

   Indien nodig, maak een nieuw installatiepakket.
4. Ga naar het gedeelte **Settings**.
5. Selecteer de **Light Agent om virtuele omgevingen te beschermen** configuratie. Deze configuratie is bedoeld voor het programma die wordt gebruikt als onderdeel van de Kaspersky Security for Virtualization Light Agent-oplossing. Light Agent moet worden geïnstalleerd op elke virtuele machine die met de oplossing moet worden beschermd. In deze configuratie kunt u geen Onderdelen voor gegevensencryptie of Adaptieve controle op afwijkingen gebruiken. Als u Light Agent installeert op een virtuele machinesjabloon die zal worden gebruikt om *niet-permanente virtuele machines* te maken, schakel dan het selectievakje **Bescherm VDI-infrastructuur** (VDI staat voor Virtual Desktop Infrastructure). De VDI-beschermingsmodus helpt de prestaties van Kaspersky Endpoint Security op niet-permanente virtuele machines te optimaliseren. In deze modus weigert Light Agent programma-updates waarvoor de virtuele machine opnieuw moet worden opgestart. Bij het ontvangen van programma-updates die een herstart vereisen, genereert Light Agent een event over de noodzaak om de template van de beschermde virtuele machines bij te werken.
6. Selecteer de onderdelen die u wilt installeren.

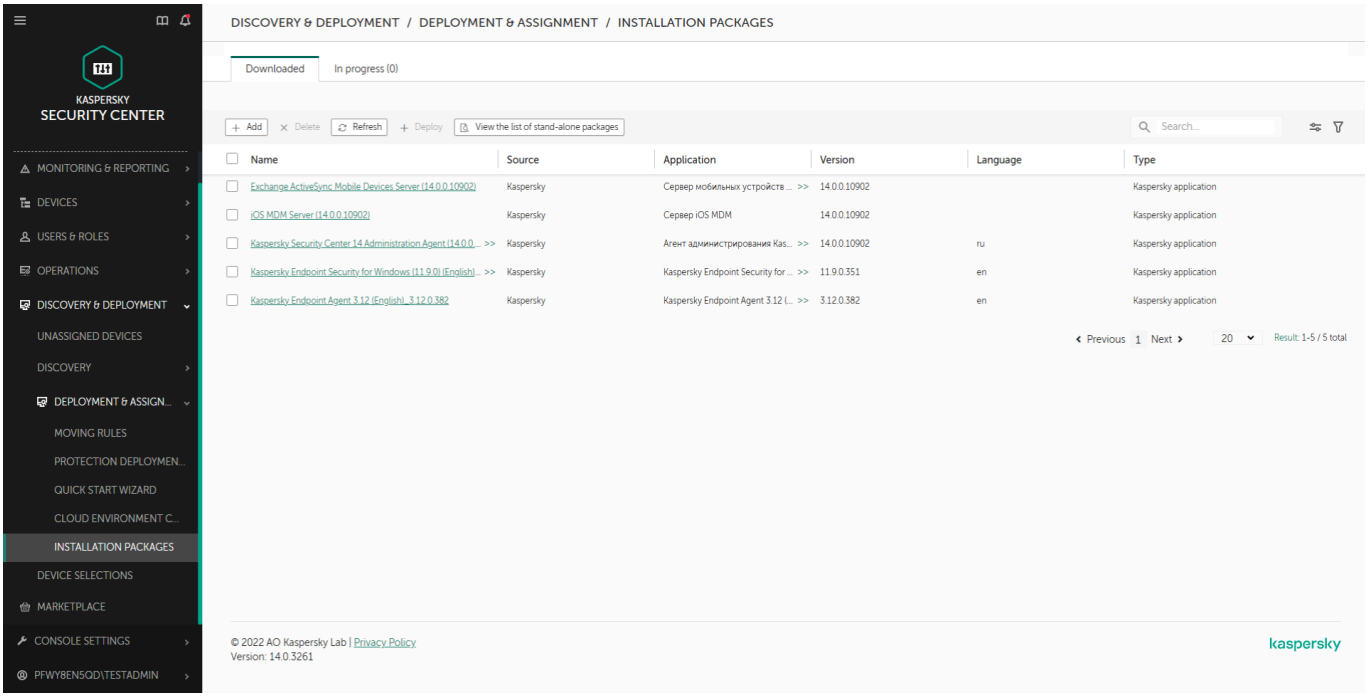
   U kunt de beschikbare programmaonderdelen wijzigen nadat het programma geïnstalleerd is.
7. Configureer de vertrouwde zone. Selecteer vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's voor de virtuele omgeving waarin u het programma installeert.

   Met vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's kunt u het programma snel instellen en compatibiliteitsproblemen met virtuele omgevingen voorkomen.
8. Sla uw wijzigingen op.
9. Een taak voor een externe installatie maken. Selecteer in taakeigenschappen het installatiepakket dat u hebt gemaakt.

Hoe Light-agent installeren met behulp van de Webconsole

1. Selecteer 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.



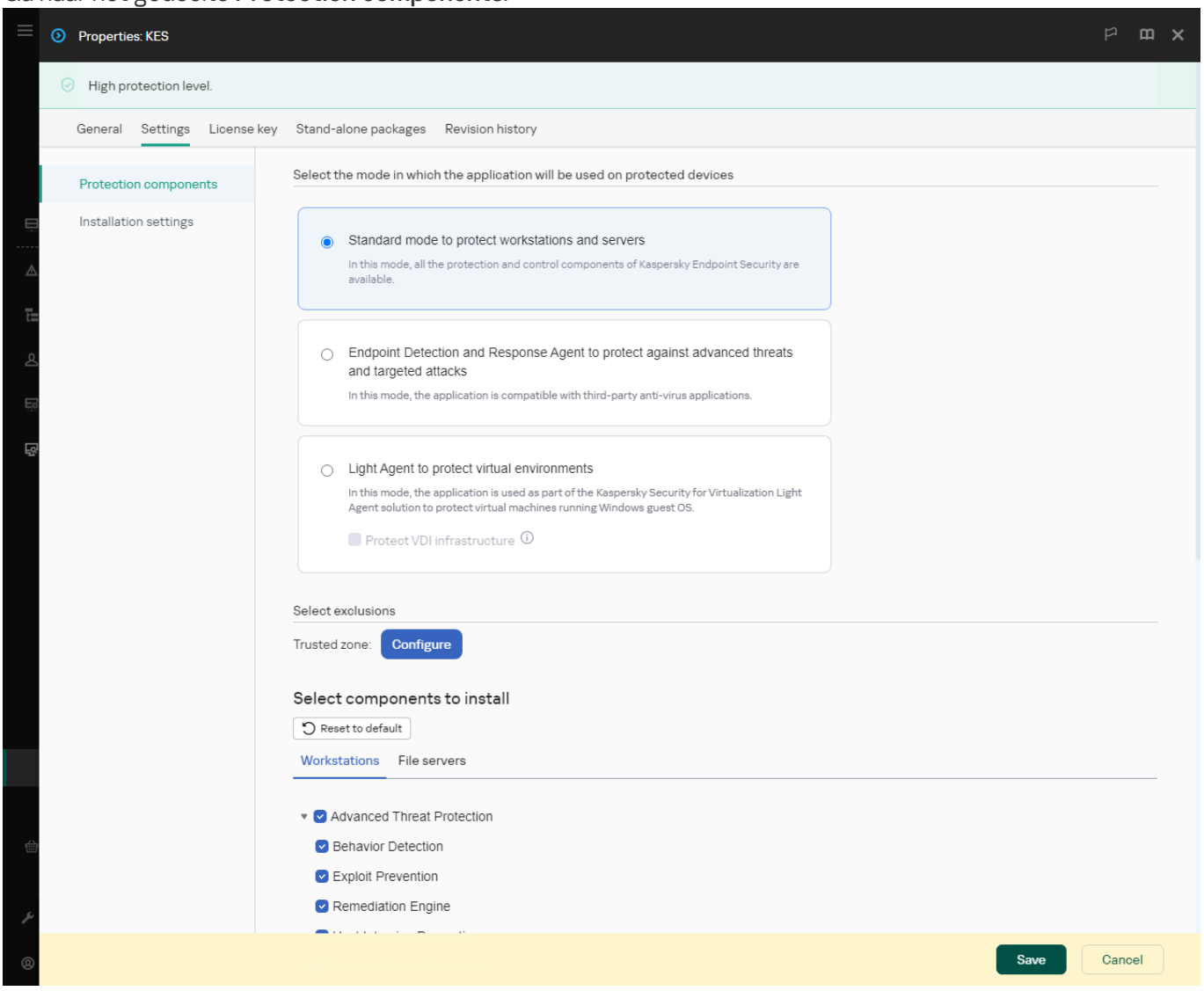
Lijst van installatiepakketten

2. Open de eigenschappen van het installatiepakket van Kaspersky Endpoint Security voor Windows.

   Indien nodig, maak een nieuw installatiepakket.

3. Selecteer het tabblad **Settings**.

4. Ga naar het gedeelte **Protection components**.



Onderdelen opgenomen in het installatiepakket

5. Selecteer de **Light Agent to protect virtual environments** configuratie. Deze configuratie is bedoeld voor het programma die wordt gebruikt als onderdeel van de Kaspersky Security for Virtualization Light Agent-oplossing. Light Agent moet worden geïnstalleerd op elke virtuele machine die met de oplossing moet worden beschermd. In deze configuratie kunt u geen Onderdelen voor gegevensencryptie of Adaptieve controle op afwijkingen gebruiken. Als u Light Agent installeert op een virtuele machinesjabloon die zal worden gebruikt om *niet-permanente virtuele machines* te maken, schakel dan het selectievakje **Protect VDI infrastructure** (VDI staat voor Virtual Desktop Infrastructure). De VDI-beschermingsmodus helpt de prestaties van Kaspersky Endpoint Security op niet-permanente virtuele machines te optimaliseren. In deze modus weigert Light Agent programma-updates waarvoor de virtuele machine opnieuw moet worden opgestart. Bij het ontvangen van programma-updates die een herstart vereisen, genereert Light Agent een event over de noodzaak om de template van de beschermde virtuele machines bij te werken.

6. Selecteer de onderdelen die u wilt installeren.

   U kunt de beschikbare programmaonderdelen wijzigen nadat het programma geïnstalleerd is.

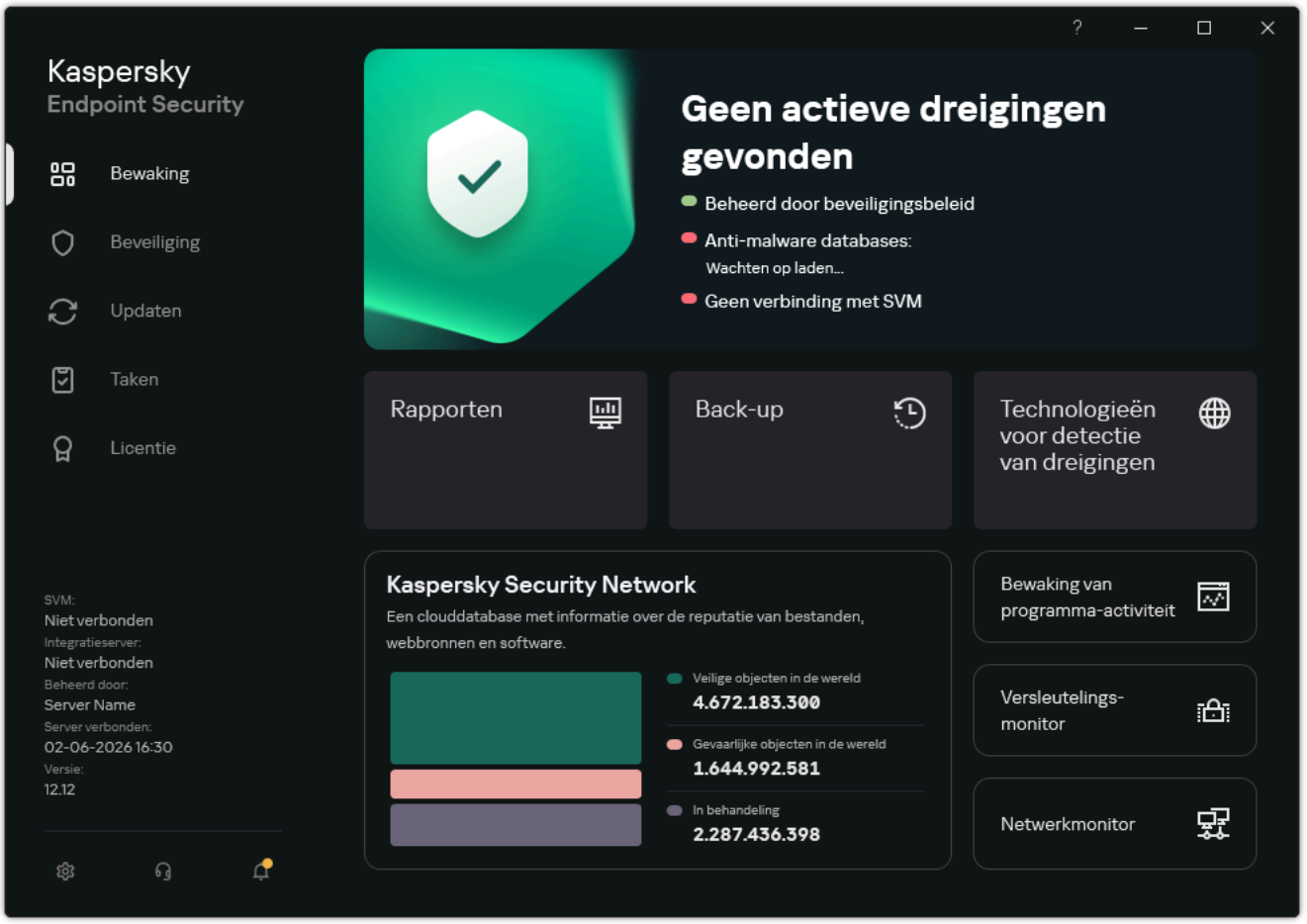
7. Configureer de vertrouwde zone. Selecteer vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's voor de virtuele omgeving waarin u het programma installeert.

   Met vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's kunt u het programma snel instellen en compatibiliteitsproblemen met virtuele omgevingen voorkomen.

8. Sla uw wijzigingen op.

9. Een taak voor een externe installatie maken. Selecteer in taakeigenschappen het installatiepakket dat u hebt gemaakt.

Hierdoor wordt Light Agent op de virtuele machine geïnstalleerd. U kunt de interface van het programma gebruiken en er wordt een pictogram van het programma weergegeven in het systeemvak . Nu moet u de verbinding van de Light Agent met SVM configureren.



Hoofdvenster van Light Agent.

Light Agent verbinden met SVM

De Kaspersky Security for Virtualization Light Agent-oplossing vereist continue communicatie tussen de Light Agent en SVM. Dit is nodig om bestanden die door de Light Agent worden verzonden, te scannen op virussen en andere malware. Zonder SVM-verbinding kan de Light Agent geen bestanden ter scan verzenden. Als de verbinding langer dan vijf minuten niet tot stand kan worden gebracht, wordt de scan met een foutmelding beëindigd.

Het verbinden van een Light Agent met een SVM omvat de volgende stappen:

1. Light Agent ontvangt de lijst met beschikbare SVM's.

2. Light Agent bepaalt een beschikbare Protection Server (SVM) die optimaal is voor verbinding volgens het SVM-selectiealgoritme.

3. Light Agent controleert aanvullende SVM-verbindingsinstellingen: tags, status voor verbindingsinstellingen, programmafunctionaliteit die onder de licentie valt.

4. Light Agent verbinden met SVM.

U kunt informatie over de status van de verbinding van de Light Agent met de SVM opvragen in Kaspersky Endpoint Security of via de programmaopdracht. Het programma genereert een gebeurtenis wanneer de SVM-verbinding van de Light Agent wordt verbroken of tot stand wordt gebracht en stuurt deze gebeurtenissen naar Kaspersky Security Center. Als u een Integratieserver voor SVM-detectie gebruikt, kunt u informatie over de status van de SVM en het aantal verbonden Light Agents opvragen in de Integration Server Console. Raadpleeg de Help van Kaspersky Security for Virtualization Light Agent voor meer informatie over SVM-statusbewaking.

SVM-detectie

U kunt een van de SVM-detectiemethoden voor de Light Agent selecteren:

- Gebruik van de Integratieserver (VIIS).

  Integratieserver is het oplossingsonderdeel dat de interactie van Kaspersky Security for Virtualization Light Agent met de virtuele infrastructuur mogelijk maakt en een lijst van SVM's dat beschikbaar is voor verbinding aanmaakt. Light Agent maakt verbinding met de Integratieserver en haalt de lijst met SVM-adressen op.

  De integratieserver is het nuttigst in grote virtuele infrastructuren omdat hij automatisch de belasting tussen SVM's verdeelt, informatie over beschikbare SVM's ophaalt, deze informatie analyseert en Light Agents van een lijst voorziet met Protection Servers (SVM's) die optimaal zijn voor de verbinding.

  Om ervoor te zorgen dat Light Agent een lijst met SVM's kan ophalen, hoeft u alleen het adres van de Integratieserver in te voeren.

- Gebruik de lijst met SVM-adressen.

  Als u afzonderlijke SVM's wilt opgeven waarmee Light Agent verbinding moet maken, kunt u handmatig een lijst voorbereiden.

  U moet de adressen van beschikbare SVM's opgeven waarmee de Light Agent verbinding kan maken.

Configureer SVM-detectie door Light Agent in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.

2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.

3. Selecteer **Light Agent-modus** → **SVM-ontdekkingsinstellingen** in het beleidsvenster.

4. Selecteer een SVM-detectiemethode.

   - **Gebruik Integratieserver**. Voer de verbindingsinstellingen voor de Integratieserver in. Voer het IP-adres in IPv4-indeling of de volledig gekwalificeerde domeinnaam (FQDN) in van het apparaat waarop de Integratieserver is geïnstalleerd.

   - **Gebruik een aangepaste lijst met SVM-adressen**. Maak een lijst met SVM's waarmee Light Agent verbinding kan maken. Geef het IP-adres op in IPv4-formaat of de volledig gekwalificeerde domeinnaam (FQDN) van SVM. Elk item in de lijst moet op een nieuwe regel worden ingevoerd of van het vorige item worden gescheiden door een puntkomma (`;`) karakter.

     Geef in de lijst met SVM-adressen alleen volledige domeinnamen (FQDN) op die overeenkomen met één IP-adres. Het gebruik van een volledig gekwalificeerde domeinnaam die overeenkomt met meerdere IP-adressen kan leiden tot fouten in de oplossing.

5. Sla uw wijzigingen op.

Configureer SVM-detectie door Light Agent in de Webconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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 **Light Agent Mode** → **SVM discovery settings**.

5. Selecteer een SVM-detectiemethode.

   - **Use Integration Server**. Voer de verbindingsinstellingen voor de Integratieserver in. Voer het IP-adres in IPv4-indeling of de volledig gekwalificeerde domeinnaam (FQDN) in van het apparaat waarop de Integratieserver is geïnstalleerd.

   - **Use a custom list of SVM addresses**. Maak een lijst met SVM's waarmee Light Agent verbinding kan maken. Geef het IP-adres op in IPv4-formaat of de volledig gekwalificeerde domeinnaam (FQDN) van SVM. Elk item in de lijst moet op een nieuwe regel worden ingevoerd of van het vorige item worden gescheiden door een puntkomma (`;`) karakter.

     Geef in de lijst met SVM-adressen alleen volledige domeinnamen (FQDN) op die overeenkomen met één IP-adres. Het gebruik van een volledig gekwalificeerde domeinnaam die overeenkomt met meerdere IP-adressen kan leiden tot fouten in de oplossing.

6. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Configureer SVM-detectie door Light Agent in de programma-interface

1. Klik in het hoofdvenster van het programma op de knop ⚙.

2. Klik in het venster met de programma-instellingen onder **Light Agent-modus** op de tegel **SVM-ontdekkingsinstellingen**.

3. Selecteer een SVM-detectiemethode.

   - **Gebruik Integratieserver**. Voer de verbindingsinstellingen voor de Integratieserver in. Voer het IP-adres in IPv4-indeling of de volledig gekwalificeerde domeinnaam (FQDN) in van het apparaat waarop de Integratieserver is geïnstalleerd.

   - **Gebruik een aangepaste lijst met SVM-adressen**. Maak een lijst met SVM's waarmee Light Agent verbinding kan maken. Geef het IP-adres op in IPv4-formaat of de volledig gekwalificeerde domeinnaam (FQDN) van SVM. Elk item in de lijst moet op een nieuwe regel worden ingevoerd of van het vorige item worden gescheiden door een puntkomma (`;`) karakter.

     Geef in de lijst met SVM-adressen alleen volledige domeinnamen (FQDN) op die overeenkomen met één IP-adres. Het gebruik van een volledig gekwalificeerde domeinnaam die overeenkomt met meerdere IP-adressen kan leiden tot fouten in de oplossing.

4. Sla uw wijzigingen op.

Het SVM-selectiealgoritme voor Light Agent configureren

De infrastructuur van de organisatie kan meerdere geïmplementeerde SVM's bevatten waarmee Light Agents verbinding kunnen maken. Om de belasting van het netwerk en de bronnen van de virtuele infrastructuur in evenwicht te brengen, moet u de Light Agents verdelen over de SVM's.

Light Agents kunnen de volgende SVM-selectiealgoritmen voor verbinding toepassen:

Standaardalgoritme (standaard)

Als dit algoritme wordt toegepast, kiest de Light Agent op de virtuele machine na de installatie en de opstart voor verbinding met een SVM die *lokaal* is ten opzichte van de Light Agent.

Of een SVM als lokaal voor een Light Agent wordt beschouwd, hangt af van het type virtuele infrastructuur:

- In een virtuele infrastructuur op basis van Basis Dynamix Enterprise is de SVM die wordt beschouwd als lokaal voor een Light Agent, de SVM die wordt geïmplementeerd op dezelfde node als de virtuele machine waarop de Light Agent is geïnstalleerd.

- In een virtuele infrastructuur op basis van Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer of Basis Dynamix Standard, de SVM die wordt beschouwd als lokaal bij een Light Agent is de SVM die is geïmplementeerd op dezelfde hypervisor als de virtuele machine waarop de Light Agent is geïnstalleerd.

- In een virtuele infrastructuur die draait op het OpenStack of VK Private Cloud-platform, kunt u opgeven hoe de SVM-lokaliteit moet worden bepaald ten opzichte van de Light Agent met behulp van de `StandardAlgorithmSvmLocality` parameter in de `HypervisorSpecificSettings:Openstack` van het configuratiebestand appsettings.json van Integration Server. Afhankelijk van de versie van de Integration Server bevindt het bestand zich op een van de volgende paden:

  - /var/opt/kaspersky/viis/common/ voor de op Linux gebaseerde Integration Server

  - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\ voor de Windows-gebaseerde Integration Server

De `StandardAlgorithmSvmLocality` parameter kan de volgende waarden aannemen:

- `ServerGroup` – als deze waarde is geselecteerd, wordt SVM als lokaal voor de Light Agent beschouwd als deze zich binnen dezelfde servergroep bevindt als de virtuele machine waarop de Light Agent is geïnstalleerd. Deze waarde wordt standaard gebruikt.

- `Project` – als deze waarde is geselecteerd, wordt SVM als lokaal voor de Light Agent beschouwd als het wordt geïmplementeerd binnen hetzelfde OpenStack project als de virtuele machine waarop de Light Agent is geïnstalleerd.

- `AvailabilityZone` – als deze waarde is geselecteerd, wordt SVM als lokaal voor de Light Agent beschouwd als deze zich in dezelfde beschikbaarheidszone bevindt als de virtuele machine waarop de Light Agent is geïnstalleerd.

Als er geen lokale SVM's beschikbaar zijn voor verbinding, selecteert de Light Agent de SVM met de minste verbonden Light Agents, ongeacht het SVM-pad in de virtuele infrastructuur.

Het programma bepaalt niet of de SVM lokaal is ten opzichte van de Light Agent als de beschermingsmodus voor grote infrastructuur is ingeschakeld voor de Protection Server op de SVM. In dit geval wordt aanbevolen om het uitgebreide SVM-selectiealgoritme te gebruiken en de Integration Server te selecteren als de SVM-detectiemethode.

Uitgebreid algoritme

Als dit algoritme wordt toegepast, kunt u de volgende instellingen voor SVM-selectie definiëren:

- of de locatie van de SVM in de infrastructuur moet worden overwogen of genegeerd bij het kiezen van SVM's voor verbinding

- als de SVM-locatie in aanmerking wordt genomen, de methode voor het bepalen van de SVM-locatie ten opzichte van de Light Agent

Als Light Agents de locatie van SVM's in de infrastructuur negeren, kunnen Light Agents verbinding maken met alle SVM's die beschikbaar zijn voor verbinding.

Als Light Agents rekening moeten houden met de locatie van SVM's in de infrastructuur, moet u het type SVM-pad selecteren waarmee rekening wordt gehouden bij het bepalen van de SVM-locatie ten opzichte van de Light Agent. Of een SVM als lokaal voor de Light Agent wordt beschouwd, hangt af van het type virtuele infrastructuur.

In een virtuele infrastructuur op basis van Basis Dynamix Enterprise kan een SVM in een van de volgende gevallen als lokaal voor de Light Agent worden beschouwd:

- Een SVM wordt geïmplementeerd op dezelfde node als de virtuele machine waarop de Light Agent is geïnstalleerd.

- Een SVM wordt geïmplementeerd in dezelfde zone als de virtuele machine waarop de Light Agent is geïnstalleerd.

- Een SVM wordt geïmplementeerd in hetzelfde datacenter als de virtuele machine waarop de Light Agent is geïnstalleerd.

In een virtuele infrastructuur op basis van Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer of Basis Dynamix Standard kan een SVM worden beschouwd als lokaal voor de Light Agent in een van de volgende gevallen:

- Een SVM wordt geïmplementeerd op dezelfde hypervisor als de virtuele machine waarop de Light Agent is geïnstalleerd.
- Een SVM wordt geïmplementeerd op hetzelfde hypervisorcluster als de virtuele machine waarop de Light Agent is geïnstalleerd.
- Een SVM wordt geïmplementeerd in hetzelfde datacenter als de virtuele machine waarop de Light Agent is geïnstalleerd.

In een virtuele infrastructuur die draait op het OpenStack of VK Private Cloud-platform, kan een SVM in een van de volgende gevallen als lokaal voor de Light Agent worden beschouwd:

- Een SVM bevindt zich in dezelfde servergroep als de virtuele machine waarop de Light Agent is geïnstalleerd.
- Een SVM wordt geïmplementeerd binnen hetzelfde OpenStack project als de virtuele machine waarop de Light Agent is geïnstalleerd.
- Een SVM bevindt zich in dezelfde beschikbaarheidszone als de virtuele machine waarop de Light Agent is geïnstalleerd.

Als Light Agents rekening houden met de locatie van SVM's in de infrastructuur bij het kiezen van de SVM waarmee ze verbinding willen maken, kunnen Light Agents alleen verbinding maken met SVM's die lokaal zijn.

Als u bijvoorbeeld een hypervisorcluster opgeeft als het SVM-padtype, worden alle SVM's die op deze hypervisorcluster zijn geïmplementeerd, beschouwd als lokaal voor de Light Agent en kan de Light Agent slechts verbinding maken met een van deze SVM's. Als er geen SVM's beschikbaar zijn voor verbinding in hetzelfde cluster waarin de Light Agent draait, maakt de Light Agent geen verbinding met een SVM.

Bij het selecteren van SVM's houden Light Agents ook rekening met het aantal verbonden Light Agents om ervoor te zorgen dat Light Agents gelijkmatig worden verdeeld over SVM's die beschikbaar zijn voor verbinding.

Als de Light Agent het uitgebreide SVM-selectiealgoritme gebruikt en de SVM-detectiemethode is ingesteld op SVM-adreslijst en de beschermingsmodus voor grote infrastructuur is ingeschakeld op de SVM, dan is het verbinden van een Light Agent met deze SVM alleen mogelijk als het SVM-pad wordt genegeerd .

Naast SVM-verbindingsalgoritmen kunt u de verbinding van Light Agents met SVM's regelen met behulp van tags.

Configureer het SVM-selectiealgoritme voor Light Agent in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Light Agent-modus** → **SVM-selectiealgoritme** in het beleidsvenster.

4. Selecteer het algoritme:

- **Gebruik het standaard SVM-selectiealgoritme**. Light Agent selecteert SVM's die in dezelfde hypervisor zijn geïmplementeerd.

- **Gebruik het uitgebreide SVM-selectiealgoritme**. Light Agent selecteert SVM's die zijn geïmplementeerd in het geselecteerde SVM-padtype (standaard **Hypervisor**).

5. Selecteer indien nodig het SVM-pad voor het uitgebreide SVM-selectiealgoritme:

- **Hypervisor**. Light Agent selecteert voor verbinding een SVM die aan een bepaald criterium voldoet (afhankelijk van het type virtuele infrastructuur):

  - De SVM wordt geïmplementeerd op dezelfde hypervisor als de virtuele machine waarop de Light Agent is geïnstalleerd (in een virtuele infrastructuur gebaseerd op Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer, of Basis Dynamix Standard).

  - De SVM bevindt zich in dezelfde servergroep als de virtuele machine waarop de Light Agent is geïnstalleerd (in een virtuele infrastructuur die draait op het OpenStack- of VK Private Cloud-platform).

  - De SVM bevindt zich op dezelfde node als de virtuele machine waarop de Light Agent is geïnstalleerd (in een virtuele infrastructuur Basis Dynamix Enterprise).

  Als er geen SVM's beschikbaar zijn voor verbinding op dezelfde hypervisor of in dezelfde servergroep als waar de virtuele machine met de Light Agent zich bevindt, maakt de Light Agent geen verbinding met de SVM.

- **Cluster**. De Light Agent selecteert een SVM om verbinding mee te maken die voldoet aan de criteria (afhankelijk van het type virtuele infrastructuur):

  - De SVM's worden geïmplementeerd op dezelfde hypervisorcluster als de virtuele machine waarop de Light Agent is geïnstalleerd (in een virtuele infrastructuur op Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis (Skala-R), HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux of Numa vServer).

  - De SVM's worden geïmplementeerd binnen hetzelfde OpenStack-project als de virtuele machine waarop de Light Agent is geïnstalleerd (in een virtuele infrastructuur die draait op het OpenStack- of VK Private Cloud-platform).

  - De SVM bevindt zich in dezelfde zone als de virtuele machine waarop de Light Agent is geïnstalleerd (in een virtuele infrastructuur Basis Dynamix Enterprise).

  Als er geen SVM's beschikbaar zijn voor verbinding in hetzelfde hypervisorcluster of binnen hetzelfde OpenStack-project waar de virtuele machine met de Light Agent zich bevindt, maakt de Light Agent geen verbinding met de SVM.

- **Datacenter**. De Light Agent selecteert een SVM om verbinding mee te maken die voldoet aan de criteria (afhankelijk van het type virtuele infrastructuur):

  - De SVM's worden geïmplementeerd in hetzelfde datacenter als de virtuele machine waarop de Light Agent is geïnstalleerd (in een virtuele infrastructuur gebaseerd op Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer of Basis Dynamix Standard).

  - De SVM's bevinden zich in dezelfde beschikbaarheidszone als de virtuele machine waarop de Light Agent is geïnstalleerd (in een virtuele infrastructuur die draait op het OpenStack- of VK Private Cloud-platform).

  - De SVM bevindt zich in hetzelfde datacenter als de virtuele machine waarop de Light Agent is geïnstalleerd (in een virtuele infrastructuur Basis Dynamix Enterprise).

  Als er geen SVM's beschikbaar zijn voor verbinding in hetzelfde datacenter of dezelfde beschikbaarheidszone waar de virtuele machine met de Light Agent zich bevindt, maakt de Light Agent geen verbinding met de SVM.

- **Negeren**. Light Agent negeert het SVM-pad voor verbinding met de Protection Server. Light Agents houdt rekening met andere criteria: tags, het aantal Light Agents dat is verbonden met een SVM, enzovoort.

6. Sla uw wijzigingen op.

Configureer het SVM-selectiealgoritme voor Light Agent in de Webconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.

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 **Light Agent Mode** → **SVM selection algorithm**.

5. Selecteer het algoritme:

   - **Use the standard SVM selection algorithm**. Light Agent selecteert SVM's die in dezelfde hypervisor zijn geïmplementeerd.

   - **Use the extended SVM selection algorithm**. Light Agent selecteert SVM's die zijn geïmplementeerd in het geselecteerde SVM-padtype (standaard **Hypervisor**).

6. Selecteer indien nodig het SVM-pad voor het uitgebreide SVM-selectiealgoritme:

- **Hypervisor**. De Light Agent selecteert een SVM om verbinding mee te maken die voldoet aan de criteria (afhankelijk van het type virtuele infrastructuur):

  - De SVM wordt geïmplementeerd op dezelfde hypervisor als de virtuele machine waarop de Light Agent is geïnstalleerd (in een virtuele infrastructuur gebaseerd op Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer, of Basis Dynamix Standard).

  - De SVM bevindt zich in dezelfde servergroep als de virtuele machine waarop de Light Agent is geïnstalleerd (in een virtuele infrastructuur die draait op het OpenStack- of VK Private Cloud-platform).

  - De SVM bevindt zich op dezelfde node als de virtuele machine waarop de Light Agent is geïnstalleerd (in een virtuele infrastructuur Basis Dynamix Enterprise).

  Als er geen SVM's beschikbaar zijn voor verbinding op dezelfde hypervisor of in dezelfde servergroep als waar de virtuele machine met de Light Agent zich bevindt, maakt de Light Agent geen verbinding met de SVM.

- **Cluster**. De Light Agent selecteert een SVM om verbinding mee te maken die voldoet aan de criteria (afhankelijk van het type virtuele infrastructuur):

  - De SVM's worden geïmplementeerd op dezelfde hypervisorcluster als de virtuele machine waarop de Light Agent is geïnstalleerd (in een virtuele infrastructuur op Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis (Skala-R), HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux of Numa vServer).

  - De SVM's worden geïmplementeerd binnen hetzelfde OpenStack-project als de virtuele machine waarop de Light Agent is geïnstalleerd (in een virtuele infrastructuur die draait op het OpenStack- of VK Private Cloud-platform).

  - De SVM bevindt zich in dezelfde zone als de virtuele machine waarop de Light Agent is geïnstalleerd (in een virtuele infrastructuur Basis Dynamix Enterprise).

  Als er geen SVM's beschikbaar zijn voor verbinding in hetzelfde hypervisorcluster of binnen hetzelfde OpenStack-project waar de virtuele machine met de Light Agent zich bevindt, maakt de Light Agent geen verbinding met de SVM.

- **Data center**. De Light Agent selecteert een SVM om verbinding mee te maken die voldoet aan de criteria (afhankelijk van het type virtuele infrastructuur):

  - De SVM's worden geïmplementeerd in hetzelfde datacenter als de virtuele machine waarop de Light Agent is geïnstalleerd (in een virtuele infrastructuur gebaseerd op Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer of Basis Dynamix Standard).

  - De SVM's bevinden zich in dezelfde beschikbaarheidszone als de virtuele machine waarop de Light Agent is geïnstalleerd (in een virtuele infrastructuur die draait op het OpenStack- of VK Private Cloud-platform).

  - De SVM bevindt zich in hetzelfde datacenter als de virtuele machine waarop de Light Agent is geïnstalleerd (in een virtuele infrastructuur Basis Dynamix Enterprise).

Als er geen SVM's beschikbaar zijn voor verbinding in hetzelfde datacenter of dezelfde beschikbaarheidszone waar de virtuele machine met de Light Agent zich bevindt, maakt de Light Agent geen verbinding met de SVM.

- **Ignore**. Light Agent negeert het SVM-pad voor verbinding met de Protection Server. Light Agents houdt rekening met andere criteria: tags, het aantal Light Agents dat is verbonden met een SVM, enzovoort.

7. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Configureer het SVM-selectiealgoritme voor Light Agent in de programma-interface

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

2. Klik in het venster met de programma-instellingen onder **Light Agent-modus** op de tegel **SVM-ontdekkingsinstellingen**.

3. Selecteer het algoritme:

   - **Gebruik het standaard SVM-selectiealgoritme**. Light Agent selecteert SVM's die in dezelfde hypervisor zijn geïmplementeerd.

   - **Gebruik het uitgebreide SVM-selectiealgoritme**. Light Agent selecteert SVM's die zijn geïmplementeerd in het geselecteerde SVM-padtype (standaard **Hypervisor**).

4. Selecteer indien nodig het SVM-pad voor het uitgebreide SVM-selectiealgoritme:

   - **Hypervisor**. De Light Agent selecteert een SVM om verbinding mee te maken die voldoet aan de criteria (afhankelijk van het type virtuele infrastructuur):

     - De SVM wordt geïmplementeerd op dezelfde hypervisor als de virtuele machine waarop de Light Agent is geïnstalleerd (in een virtuele infrastructuur gebaseerd op Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer, of Basis Dynamix Standard).

     - De SVM bevindt zich in dezelfde servergroep als de virtuele machine waarop de Light Agent is geïnstalleerd (in een virtuele infrastructuur die draait op het OpenStack- of VK Private Cloud-platform).

     - De SVM bevindt zich op dezelfde node als de virtuele machine waarop de Light Agent is geïnstalleerd (in een virtuele infrastructuur Basis Dynamix Enterprise).

     Als er geen SVM's beschikbaar zijn voor verbinding op dezelfde hypervisor of in dezelfde servergroep als waar de virtuele machine met de Light Agent zich bevindt, maakt de Light Agent geen verbinding met de SVM.

- **Cluster**. De Light Agent selecteert een SVM om verbinding mee te maken die voldoet aan de criteria (afhankelijk van het type virtuele infrastructuur):

  - De SVM's worden geïmplementeerd op dezelfde hypervisorcluster als de virtuele machine waarop de Light Agent is geïnstalleerd (in een virtuele infrastructuur op Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis (Skala-R), HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux of Numa vServer).

  - De SVM's worden geïmplementeerd binnen hetzelfde OpenStack-project als de virtuele machine waarop de Light Agent is geïnstalleerd (in een virtuele infrastructuur die draait op het OpenStack- of VK Private Cloud-platform).

  - De SVM bevindt zich in dezelfde zone als de virtuele machine waarop de Light Agent is geïnstalleerd (in een virtuele infrastructuur Basis Dynamix Enterprise).

  Als er geen SVM's beschikbaar zijn voor verbinding in hetzelfde hypervisorcluster of binnen hetzelfde OpenStack-project waar de virtuele machine met de Light Agent zich bevindt, maakt de Light Agent geen verbinding met de SVM.

- **Datacenter**. De Light Agent selecteert een SVM om verbinding mee te maken die voldoet aan de criteria (afhankelijk van het type virtuele infrastructuur):

  - De SVM's worden geïmplementeerd in hetzelfde datacenter als de virtuele machine waarop de Light Agent is geïnstalleerd (in een virtuele infrastructuur gebaseerd op Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer of Basis Dynamix Standard).

  - De SVM's bevinden zich in dezelfde beschikbaarheidszone als de virtuele machine waarop de Light Agent is geïnstalleerd (in een virtuele infrastructuur die draait op het OpenStack- of VK Private Cloud-platform).

  - De SVM bevindt zich in hetzelfde datacenter als de virtuele machine waarop de Light Agent is geïnstalleerd (in een virtuele infrastructuur Basis Dynamix Enterprise).

  Als er geen SVM's beschikbaar zijn voor verbinding in hetzelfde datacenter of dezelfde beschikbaarheidszone waar de virtuele machine met de Light Agent zich bevindt, maakt de Light Agent geen verbinding met de SVM.

- **Negeren**. Light Agent negeert het SVM-pad voor verbinding met de Protection Server. Light Agents houdt rekening met andere criteria: tags, het aantal Light Agents dat is verbonden met een SVM, enzovoort.

5. Sla uw wijzigingen op.

Distribueren van de verbindingen van Light Agents naar SVM's (tags)

Meerdere Light Agents kunnen verbinding maken met een SVM. Om de Light Agent-verbindingen in evenwicht te brengen, kunt u een aparte lijst met SVM's opgeven. Als u een Integratieserver voor SVM-detectie gebruikt, kunt u *tags* gebruiken om Light Agent-verbindingen met SVM's in evenwicht te brengen. Dat wil zeggen dat u voor een Light Agent een lijst met SVM's kunt toewijzen die verbinding moeten maken met behulp van een tag. Om dit te doen, moet u een tag toewijzen aan de Light Agent en deze tag opgeven in de SVM-instellingen. Raadpleeg de Help van Kaspersky Security for Virtualization Light Agent voor meer informatie over het opgeven van tags in SVM-instellingen.

Voorbeeld: de Kaspersky Endpoint Detection and Response Optimum-oplossing wordt in uw infrastructuur geïmplementeerd voor aangewezen virtuele machinehosts. In dit geval kunt u de tag `[EDROptimum]` aan de Light Agent toewijzen, zodat deze verbinding maakt met de SVM's waaraan de licentiesleutel voor EDR Optimum (EDR Optimum Add-on) is toegevoegd. Hierdoor kunt u de EDR Optimum-functionaliteit op de virtuele machine gebruiken met de Light Agent. Wanneer u de Light Agent verbindt met een SVM zonder EDR Optimum-licentiesleutel, is de functionaliteit van Kaspersky Endpoint Detection and Response Optimum niet beschikbaar.

Een SVM-verbindingstag toewijzen aan een Light Agent in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Light Agent-modus** → **SVM-verbindingstag** in het beleidsvenster.
4. Selecteer het selectievakje **Verbindingstag gebruiken** en voer de SVM-verbindingstag in.

   Voor een tag kunt u een tekstreeks van maximaal 255 tekens invoeren. U kunt elk teken gebruiken, behalve het teken `;`.
5. Sla uw wijzigingen op.

Een SVM-verbindingstag toewijzen aan een Light Agent in de Webconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Light Agent Mode** → **SVM connection tag**.
5. Selecteer het selectievakje **Use connection tag** en voer de SVM-verbindingstag in.

   Voor een tag kunt u een tekstreeks van maximaal 255 tekens invoeren. U kunt elk teken gebruiken, behalve het teken `;`.
6. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

een SVM-verbindingstag toewijzen aan een Light Agent in de programma-interface

1. Klik in het hoofdvenster van het programma op de knop ⚙.
2. Klik in het venster met de programma-instellingen onder **Light Agent-modus** op de tegel **SVM-verbindingstag**.
3. Selecteer het selectievakje **Verbindingstag gebruiken** en voer de SVM-verbindingstag in.

   Voor een tag kunt u een tekstreeks van maximaal 255 tekens invoeren. U kunt elk teken gebruiken, behalve het teken `;`.
4. Sla uw wijzigingen op.

Bescherming van de verbinding tussen een Light Agent en SVM

U kunt de encryptie van de verbinding tussen Light Agents en Protection Server configureren. Om dit te doen, moet u encryptie van het gegevenskanaal tussen de Light Agent en de Protection Server inschakelen in de Protection Server-instellingen op de SVM en in de Light Agent-instellingen.

Een Light Agent waarvoor verbindingsbeveiliging is ingeschakeld, kan alleen verbinding maken met SVM's waarvoor encryptie van het gegevenskanaal tussen de Light Agent en de Protection Server is ingeschakeld. Een Light Agent waarvoor verbindingsbeveiliging is uitgeschakeld, kan alleen verbinding maken met SVM's waarvoor kanaalversleuteling is uitgeschakeld of waarvoor een onveilige verbinding tussen de Protection Server en de Light Agent is toegestaan.

Raadpleeg de Help van Kaspersky Security for Virtualization Light Agent voor meer informatie over het configureren van verbindingsbeveiliging op de Protection Server.

Het beveiligen van de verbinding met encryptie kan van de prestaties van Kaspersky Security for Virtualization Light Agent verminderen.

Verbindingsbeveiliging configureren in een Light Agent in de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Light Agent-modus** → **Verbindingsbescherming** in het beleidsvenster.
4. Selecteer het selectievakje **Gegevenskanaal tussen Light Agent en de beschermingsserver encrypten**.
5. Sla uw wijzigingen op.

Verbindingsbeveiliging configureren in een Light Agent in de Webconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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 **Light Agent Mode** → **Connection protection**.
5. Selecteer het selectievakje **Encrypt data channel between Light Agent and the Protection Server**.
6. Om het beleid op computers toe te passen, sluit het hangslot-pictogram en sla uw wijzigingen op.

Verbindingsbeveiliging configureren in een Light Agent in de programma-interface

1. Klik in het hoofdvenster van het programma op de knop .
2. Klik in het venster met de programma-instellingen onder **Light Agent-modus** op de tegel **Verbindingsbescherming**.

3. Selecteer het selectievakje **Gegevenskanaal tussen Light Agent en de beschermingsserver encrypten**.

4. Sla uw wijzigingen op.

Light Agent activeren

Als Kaspersky Endpoint Security in de Light Agent-modus wordt gebruikt om virtuele omgevingen te beschermen, hoeft u het programma niet afzonderlijk te activeren. Om het programma te activeren, moet u een licentiesleutel aan de SVM toevoegen. U kunt een licentiesleutel toevoegen aan SVM via de speciale taak in de Kaspersky Security Center-console. U kunt geen licentiesleutels beheren in de Light Agent-interface, maar u kunt wel licentiegegevens bekijken (zie de onderstaande afbeelding). U kunt de licentiegegevens van Light Agent ook bekijken op de opdrachtregel (zie de onderstaande instructies). Light Agent krijgt deze informatie van SVM. Raadpleeg de Help van Kaspersky Security for Virtualization Light Agent voor meer informatie over het activeren van de oplossing en het beheren van licentiesleutels.

Om informatie over de licentie voor Light Agent te bekijken:

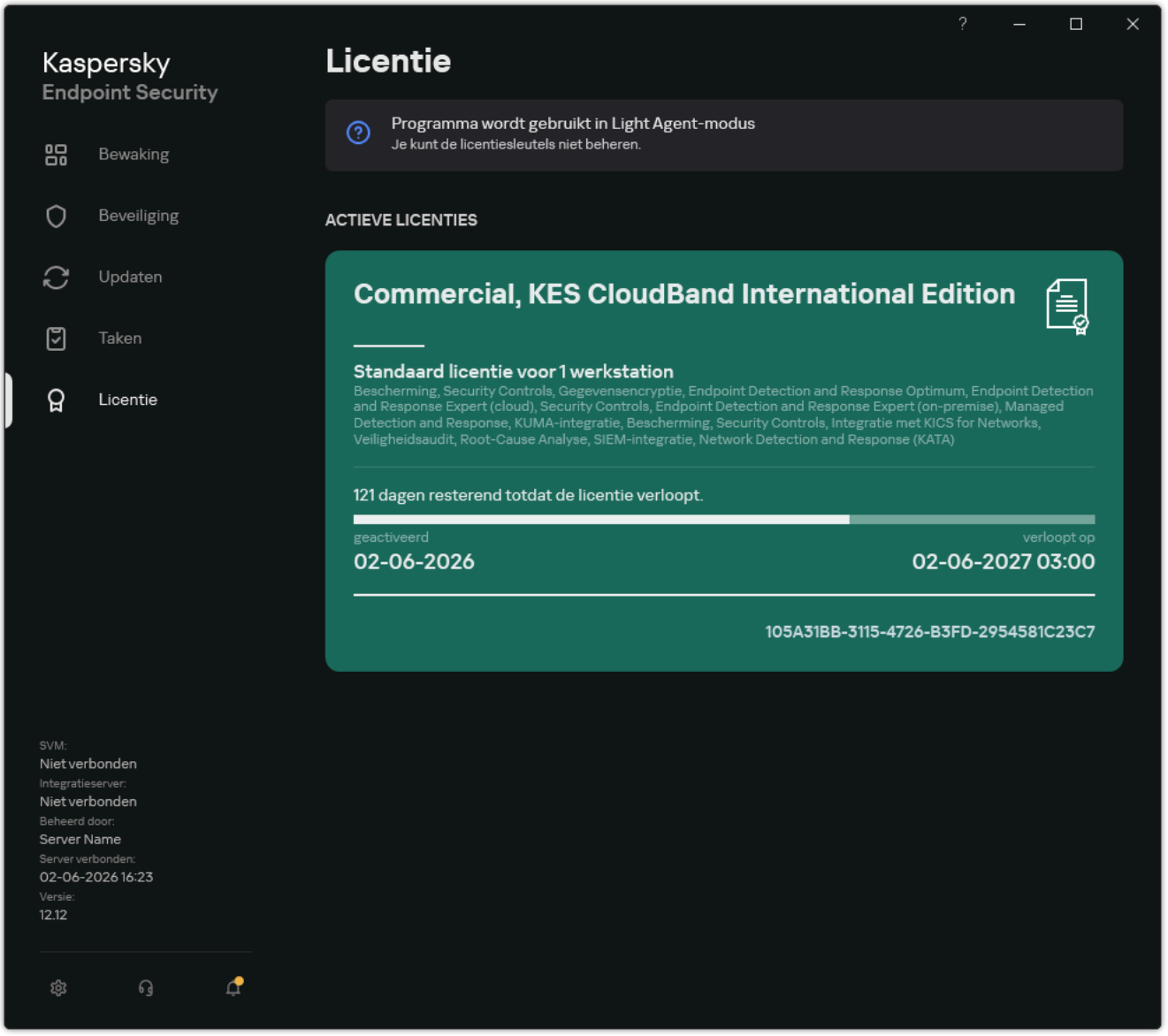
1. Voer de interpreter van de opdrachtregel (cmd) uit als een beheerder.

2. Ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen.

3. Voer de volgende opdracht uit:

```
avp.com LICENSE /CHECK
```

Kaspersky Endpoint Security geeft daarom licentie-informatie weer: het adres van de SVM waarmee de Light Agent is verbonden, het aantal dagen tot de licentie verloopt en andere informatie. Als u problemen ondervindt bij het activeren van Light Agent, raadpleeg de Knowledge Base van de Technische Support.



Het venster Licentiebeheer

Migratiegids van KSVLA Light Agent naar KES Light Agent

Kaspersky Security for Virtualization 5.2 Light Agent bevat het onderdeel Light Agent voor Windows 5.2 (hierna ook wel "KSVLA Light Agent" genoemd). In Kaspersky Security for Virtualization Light Agent 6.2 wordt Kaspersky Endpoint Security in Light Agent-modus gebruikt als Light Agent-onderdeel. Om de oplossing bij te werken naar versie 6.2, moet u migreren van KSVLA Light Agent 5.2 naar Kaspersky Endpoint Security in de Light Agent-modus (hierna ook wel 'KES Light Agent' genoemd). Raadpleeg de Help van Kaspersky Security for Virtualization Light Agent voor meer informatie over het bijwerken van de versie van de Kaspersky Security for Virtualization Light Agent-oplossing.

Softwarevereisten

Voordat u begint met de migratie van KSVLA Light Agent naar KES Light Agent, moet u ervoor zorgen dat uw virtuele machine voldoet aan de hardware- en softwarevereisten van Kaspersky Endpoint Security for Windows. De lijsten met ondersteunde besturingssysteemversies verschillen voor KES en KSWS. KES ondersteunt bijvoorbeeld geen servers met Windows Server 2003.

Minimale softwarevereisten voor migratie van KSVLA Light Agent naar KES Light Agent:

- Kaspersky Endpoint Security voor Windows 12.8.
- Kaspersky Security for Virtualization Light Agent 6.2 (inclusief de onderdelen Protection Server en Integratieserver).
- Kaspersky Security Center 14.2

  Als u een eerdere versie van Kaspersky Security Center geïnstalleerd hebt, werk deze dan bij naar 14.2 of hoger. In deze versie van Kaspersky Security Center kunt u met de wizard Batchconversie van beleid en taken een migratie uitvoeren van beleid naar een profiel in plaats van naar een beleid. In deze versie van Kaspersky Security Center kunt u met de wizard Batchconversie van beleid en taken ook een breder scala aan beleidsinstellingen migreren.

Migratiestappen

De migratie van KSVLA Light Agent naar KES Light Agent wordt semi-automatisch uitgevoerd. Dit is nodig vanwege de verschillende architecturen van de programma's.

Migreer van KSVLA Light Agent naar KES Light Agent in de volgende volgorde:

1. **Migreer KSVLA Light Agent-taken en -beleid**

   Om beleidsinstellingen te migreren, moet u de wizard Batchconversie van beleid en taken (de migratiewizard) uitvoeren. Na het migreren van beleidsinstellingen, moet u de instellingen die de migratiewizard niet automatisch kan migreren handmatig migreren (bijvoorbeeld instellingen voor database-updates). Na de migratie is het ook raadzaam om te controleren of de migratiewizard alle instellingen correct heeft gemigreerd.

   Als wachtwoordbeveiliging is ingeschakeld om de toegang tot KSVLA Light Agent te beperken, moet u de wachtwoordbeveiliging uitschakelen in het beleid van KSVLA Light Agent voordat u KES Light Agent installeert. U kunt het wachtwoord voor het verwijderen niet invoeren in de instellingen van het installatiepakket van KES Light Agent. Nadat u de installatie van KES Light Agent bovenop KSVLA Light Agent hebt voltooid, moet u wachtwoordbeveiliging inschakelen in het KES-beleid.

2. **Kaspersky Endpoint Security installeren in de Light Agent-modus**

   U kunt KES Light Agent installeren op de volgende manieren:

   - KES Light Agent installeren na het verwijderen van KSVLA Light Agent (aanbevolen)
   - KES Light Agent installeren op KSVLA Light Agent

3 Controleer of het programma na de migratie werkt

Controleer na de migratie van KSVLA Light Agent naar KES Light Agent of de programma correct werkt. Activeer het geconverteerde beleid. Controleer de status van de server in de virtual machine in de Kaspersky Security Center-console (moet *OK* zijn). Controleer of er geen fouten worden gerapporteerd voor het programma. Controleer ook het tijdstip van de laatste verbinding met SVM en de beveiligingsstatus van de virtuele machine. U hoeft Light Agent niet te activeren, omdat de licentiesleutel wordt toegevoegd aan de SVM.

KES Light Agent installeren in plaats van KSVLA Light Agent

U kunt Kaspersky Endpoint Security op de volgende manieren installeren:

- KES Light Agent installeren na het verwijderen van KSVLA Light Agent (aanbevolen)
- KES Light Agent installeren op KSVLA Light Agent

KSVLA Light Agent verwijderen

U kunt het programma op afstand verwijderen met behulp van de *Install application remotely* taak, lokaal op de virtuele machine of in de sjabloon voor de virtuele machine. Nadat u KSVLA Light Agent hebt verwijderd, moet u de virtuele machine mogelijk opnieuw opstarten.

Nadat het verwijderen van KSVLA Light Agent, installeer KES Light Agent met behulp van een geschikte methode.

Kaspersky Endpoint Security installeren

Als wachtwoordbeveiliging is ingeschakeld om de toegang tot KSVLA Light Agent te beperken, moet u de wachtwoordbeveiliging uitschakelen in het beleid van KSVLA Light Agent voordat u KES Light Agent installeert. U kunt het wachtwoord voor het verwijderen niet invoeren in de instellingen van het installatiepakket van KES Light Agent. Nadat de installatie van KES Light Agent bovenop KSVLA Light Agent is voltooid, moet u wachtwoordbeveiliging inschakelen in het KES-beleid.

Wanneer u Kaspersky Endpoint Security installeert, moet u de modus **Light Agent om virtuele omgevingen te beschermen** selecteren. Voordat KES Light Agent op een virtuele machine wordt geïnstalleerd, detecteert het installatieprogramma KSVLA Light Agent als incompatibele software en verwijdert het deze. Migratie van de KSVLA Light Agent-configuratie wordt niet ondersteund. Dat wil zeggen dat wanneer u KES Light Agent installeert, de set onderdelen die u installeert, wordt bepaald door uw selectie in de eigenschappen van het installatiepakket of in de installatiewizard. Nadat u KSVLA Light Agent hebt verwijderd, moet u de virtuele machine opnieuw opstarten.

Instellingen en taken van KSVLA Light Agent worden niet gemigreerd wanneer u KES Light Agent installeert. Om instellingen en taken te migreren, voert u de wizard Batchconversie van beleid en taken uit.

U kunt de lijst van geïnstalleerde onderdelen controleren in het gedeelte **Beveiliging** van de programma-interface, met de opdracht `status` of in de Kaspersky Security Center-console in computereigenschappen. U kunt de set componenten na installatie wijzigen met behulp van *Programmaonderdelen wijzigen*.

Correspondentie van KSVLA Light Agent en KES Light Agent onderdelen

De sets onderdelen van KSVLA Light Agent en KES Light Agent zijn vrijwel hetzelfde. KES Light Agent heeft meer instellingen dan KSVLA Light Agent. Na de migratie hebben de nieuwe instellingen de standaardwaarden.

Correspondentie van KSVLA Light Agent en KES Light Agent onderdelen

Light Agent 5.2	KES Light Agent
Scan kernel	Programmakernel
File Anti-Virus	File Threat Protection
Mail Anti-Virus	Mail Threat Protection
Web Anti-Virus	Web Threat Protection
Firewall	Firewall
Network Attack Blocker	Network Threat Protection
Application Privilege Control	Host Intrusion Prevention
Applications Launch Control	Programmacontrole
Web Control	Webcontrole
Device Control	Apparaatcontrole
System Watcher	In Kaspersky Endpoint Security is dit onderdeel onderverdeeld in de volgende onderdelen: • Exploit-preventie • Gedragsdetectie • Remediation Engine
System Integrity Monitoring	Systeemintegriteitscontrole
Integration with Kaspersky Endpoint Agent	*(niet ondersteund)* Vanaf Kaspersky Endpoint Security for Windows 11.9.0 maakt het distributiepakket Kaspersky Endpoint Agent niet langer deel uit van het distributiepakket.
AMSI Protection	AMSI-bescherming

Taken en beleid van KSVLA Light Agent migreren

U kunt de instellingen van KSVLA Light Agent-beleid en -taken migreren met behulp van de wizard Batchconversie van beleid en taken (hierna ook de 'Migratiewizard' genoemd).

De migratiewizard voor KSVLA Light Agent is alleen beschikbaar in de beheerconsole (MMC). Beleids- en taakinstellingen kunnen niet worden gemigreerd in de webconsole en cloudconsole.

Bij het migreren van beleid en taken zijn de volgende speciale overwegingen van belang:

- Een nieuw beleid heeft de naam *<Beleid> (omgezet)*.
- Het nieuwe beleid heeft de status *Inactive policy*.
- Het verbod op het wijzigen van instellingen (het 'hangslot') is niet gemigreerd. De migratiewizard stelt standaardwaarden in.

- Beleidsprofielen worden niet gemigreerd. U moet de beleidsprofielen handmatig toevoegen.

- Verbeterd vertrouwd zonebeheer. In KSVLA Light Agent kunt u vooraf gedefinieerde uitzonderingen alleen toevoegen bij het maken van een beleid. Vervolgens kunt u in de beleidseigenschappen eerder toegevoegde, vooraf gedefinieerde uitzonderingen configureren of uitzonderingen handmatig toevoegen. U kunt geen vooraf gedefinieerde uitzonderingen toevoegen aan beleidseigenschappen. In KES Light Agent zijn vooraf gedefinieerde uitzonderingen beschikbaar tijdens het maken van het beleid en in de eigenschappen van het gemaakte beleid. U kunt ook vooraf gedefinieerde uitzonderingen selecteren in het installatiepakket.

- De configuratie van de gebruikersinterface van het programma in Kaspersky Endpoint Security is verplaatst van het installatieprogramma naar het beleid. Als u bijvoorbeeld de gebruikersinterface van het programma wilt verbergen, kunt u de beleidsinstellingen beheren.

- De functionaliteiten voor het configureren van op rechten gebaseerde toegangscontrole (RBAC) verschillen in Kaspersky Endpoint Security en KSVLA Light Agent. U moet de gebruikersrechten voor functionele gebieden helemaal opnieuw configureren.

De wizard Batchconversie voor beleid en taken gebruiken om KSVLA Light Agent-taak- en -beleidsinstellingen te migreren

1. Selecteer Beheerserver in de Beheerconsole en klik met de rechtermuisknop om het contextmenu te openen.

2. Selecteer **All tasks** → **Policies and tasks batch conversion wizard**.

De wizard Batchconversie beleid en taken wordt gestart. Volg de instructies van de wizard.

Stap 1. Het programma selecteren waarvoor u beleid en taken moet converteren

Bij deze stap moet u Kaspersky Endpoint Security voor Windows selecteren. Ga naar de volgende stap.

Stap 2. Conversie van beleid

Selecteer het Kaspersky Security for Virtualization 5.2 Light Agent voor Windows-beleid dat u wilt converteren. Ga naar de volgende stap.

De migratiewizard begint dan met het converteren van het beleid. Tijdens de conversie vraagt de migratiewizard u om de voorwaarden van de KSN-verklaring te accepteren. Een nieuw beleid heeft de naam *<Beleid> (omgezet)*.

Stap 3. Conversie van taken

De migratiewizard maakt nieuwe taken voor Kaspersky Endpoint Security voor Windows. In de takenlijst selecteert u de KSVLA Light Agent-taken die u wilt maken voor Kaspersky Endpoint Security. Nieuwe taken krijgen een naam *<Taak naam> (geconverteerd)*. Ga naar de volgende stap.

Stap 4. Voltooiing van wizard

Verlaat de wizard verlaten.

Nadat u een beleid hebt gemigreerd, moet u de eigenschappen van het beleid openen, de instellingen controleren en het beleid opslaan. Als u deze stappen niet uitvoert, kan het zijn dat KES Light Agent het geconverteerde beleid negeert.

Besteed speciale aandacht aan de migratie van SVM-verbindingsinstellingen van Light Agent, lijsten met uitzonderingen, vertrouwde programma's, vertrouwde webadressen, regels van Programmacontrole.

Migreren van [KSVLA Light Agent+KEA] configuratie naar [KES Light Agent+ingebouwde agent] configuratie

Ter ondersteuning van het gebruik van Kaspersky Endpoint Security voor Windows als onderdeel van EDR (KATA), EDR Optimum en Kaspersky Sandbox is een ingebouwde agent aan het programma toegevoegd. U hebt geen apart Kaspersky Endpoint Agent-programma meer nodig om met deze oplossingen te werken.

Bij het migreren van KSVLA Light Agent naar KES Light Agent blijven de oplossingen EDR (KATA), EDR Optimum en Kaspersky Sandbox werken met de ingebouwde agenten van Kaspersky Endpoint Security. Daarnaast wordt Kaspersky Endpoint Agent van de computer verwijderd.

Voordat u van KSVLA Light Agent naar KES Light Agent migreert, moet u alle onderdelen van Kaspersky Security for Virtualization bijwerken naar versie 6.2, inclusief de Protection Server en de Integratieserver. Raadpleeg de Help van Kaspersky Security for Virtualization Light Agent voor meer informatie over het bijwerken van de versie van de Kaspersky Security for Virtualization Light Agent-oplossing.

Het migreren van de [KSVLA Light Agent+KEA]-configuratie naar de [KES Light Agent+ingebouwde agent]-configuratie omvat de volgende stappen:

1. **Het beleid en de taken migreren**

   Het migreren van de [KSVLA Light Agent+KEA]-beleid en -taken naar [KES Light Agent+ingebouwde agent] omvat de volgende stappen:

   1. Beleid en taken migreren van KSVLA Light Agent naar KES Light Agent met behulp van de wizard Batchconversie van beleid en taken (alleen beschikbaar in de Beheerconsole (MMC)).

      Hierdoor wordt een nieuw beleid aangemaakt met de naam *<Beleid> (geconverteerd)*. Nieuwe KES-taken worden ook aangemaakt met de namen *<Taak naam> (geconverteerd)*.

   2. Beleid en taken migreren van KEA naar KES met behulp van de wizard voor migratie van Kaspersky Endpoint Agent (alleen beschikbaar op de webconsole en cloudconsole).

      Als resultaat wordt een nieuw beleid gemaakt met de naam *<Naam van het Kaspersky Endpoint Security-beleid> & <Naam van het Kaspersky Endpoint Agent-beleid>*. Er worden ook nieuwe taken en KES-taken gemaakt.

2 **Migreren van KSVLA Light Agent naar KES Light Agent**

Voor de migratie van KSVLA Light Agent naar KES Light Agent moet u KES Light Agent installeren in plaats van KSVLA Light Agent.

Beheerders schakelen doorgaans wachtwoordbeveiliging in om de toegang tot KSVLA Light Agent en KEA te beperken. U kunt het wachtwoord voor het verwijderen van KEA alleen invoeren in de eigenschappen van de taak *Install application remotely*. Voor migratie moet u de wachtwoordbeveiliging voor KSVLA Light Agent uitschakelen.

Om de migratie uit te voeren, moet u de onderdelen selecteren die nodig zijn om Detection and Response-oplossingen te ondersteunen als onderdeel van Kaspersky Endpoint Security. Na het installeren van het programma schakelt Kaspersky Endpoint Security over op het gebruik van de ingebouwde agent en wordt Kaspersky Endpoint Agent verwijderd.

3 **Licentiefunctionaliteit**

Als het programma in de Light Agent-modus wordt gebruikt, hoeft u het programma niet te activeren. Om het programma te activeren, moet u een licentiesleutel aan de SVM toevoegen. U moet ook de licentiesleutel voor het activeren van extra functionaliteit (bijvoorbeeld EDR Optimum) toevoegen aan de SVM. Dat wil zeggen dat de licentieverlening voor functionaliteit automatisch plaatsvindt als onderdeel van de migratie.

4 **De status van Kaspersky Endpoint Detection and Response Optimum en Kaspersky Sandbox controleren**

Als de computer na de upgrade de status *Critical* heeft in de Kaspersky Security Center-console:

- Zorg ervoor dat op de computer Netwerkagent versie 13.2 of hoger is geïnstalleerd.
- Controleer de werkingsstatus van het ingebouwde agent door het *Report on status of application components* te bekijken. Als een onderdeel de status *Not installed* heeft, installeer dan de onderdeel met de taak *Change application components*.
- 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 *Report on status of application components* dat de EDR Optimum-functionaliteit is geactiveerd. Als een onderdeel de status *Geen onderdeel van licentie* heeft, zorg er dan voor dat de functie voor automatische distributie van licentiesleutels van EDR Optimum is ingeschakeld.
- Controleer de status van de verbinding van de virtuele machine met de SVM. U kunt informatie over de status van de verbinding van de Light Agent met de SVM opvragen in Kaspersky Endpoint Security of via de programmaopdracht.

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 `avp.com HELP` uit te voeren. Als u de syntaxis van een specifieke opdracht wilt lezen, typt u `avp.com HELP <command>`.

Speciale tekens in de opdracht moeten worden geëscaped. Als u de tekens `&`, `|`, `(`, `)`, `<`, `>`, `^` wilt escapen, gebruikt u het teken `^` (voorbeeld: als u het teken `&` wilt gebruiken, typt u `^&`). Om het teken `%` te escapen, dient u `%%` in te voeren.

De alternatieven voor de waarde `1` zijn de waarden `yes`, `on`, `enable`, `enabled`, en `true`. De alternatieven voor de waarde `0` zijn de waarden `no`, `off`, `disable`, `disabled`, en `false`.

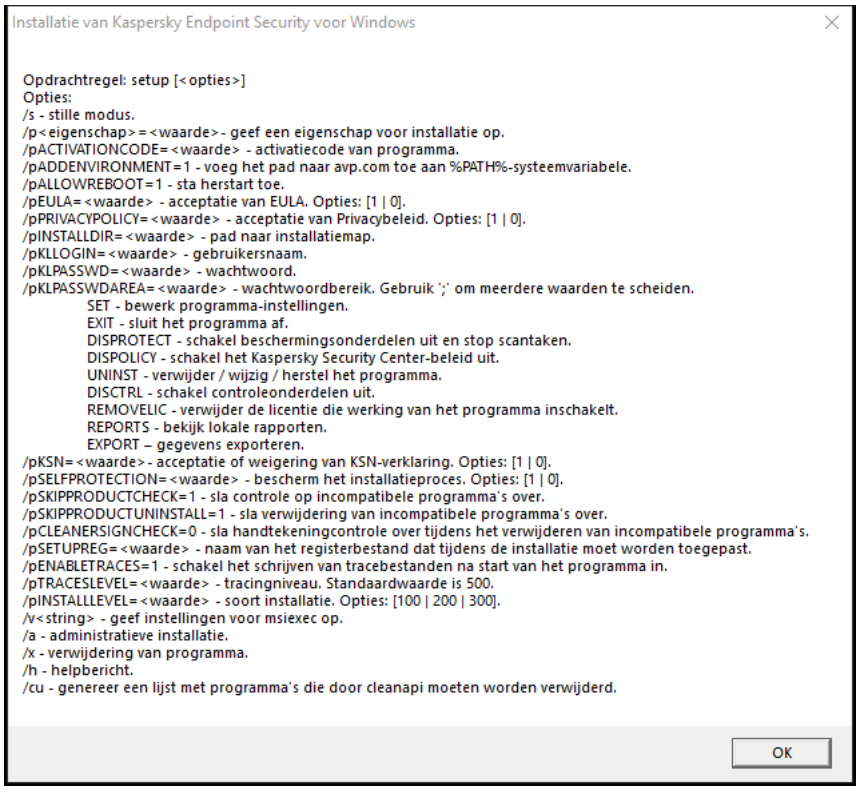
Setup. Het programma installeren

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 (stille installatie). 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.

De lijst met opdrachten voor het installeren van het programma kunt u bekijken met de opdracht `/h`. Typ `setup_kes.exe /h` voor hulp bij de syntaxis van de installatieopdracht. Als gevolg hiervan toont het installatieprogramma een venster met een beschrijving van de opdrachtopties (zie onderstaande afbeelding).



Beschrijving van opties voor installatieopdrachten

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] [/pCONFIGPATH=<path to the configuration file>]
[/pALLOWREBOOT=1] [/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<user name> /pKLPASSWD=
<password> /pKLPASSWDAREA=<password scope>] [/pENABLETRACES=1|0 /pTRACESLEVEL=<tracing level>]
[/pSKIPKB5007186CHECK=1] [/s]
```

of

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 [KSN=1|0] [CONFIGPATH=<path to the configuration
file>] [ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1] [KLLOGIN=<user name> KLPASSWD=<password> KLPASSWDAREA=<password
scope>] [ENABLETRACES=1|0 TRACESLEVEL=<tracing level>] [SKIPKB5007186CHECK=1] [/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`	Aanvaarding van de voorwaarden van de Gebruiksrechtovereenkomst. De tekst van de Gebruiksrechtovereenkomst vindt u in het distributiepakket van Kaspersky Endpoint Security. U moet akkoord gaan met de voorwaarden van Gebruiksrechtovereenkomst om het programma te installeren of de versie van het programma te upgraden.
`PRIVACYPOLICY=1`	Aanvaarding van het Privacybeleid. De tekst van het Privacybeleid wordt bij het distributiepakket van Kaspersky Endpoint Security meegeleverd. U moet akkoord gaan met het Privacybeleid om het programma te installeren of een upgrade voor de programmaversie uit te voeren.
`KSN`	Aanvaarding of weigering van deelname aan Kaspersky Security Network (KSN). Als geen waarde voor deze parameter is ingesteld, wordt u door Kaspersky Endpoint Security gevraagd of u al dan niet wilt deelnemen aan KSN wanneer Kaspersky Endpoint Security voor het eerst wordt gestart. Beschikbare waarden: • `1` – Aanvaarding van de deelname aan KSN. • `0` – Weigering van de deelname aan KSN (standaardwaarde). Het distributiepakket van Kaspersky Endpoint Security is geoptimaliseerd voor gebruik met Kaspersky Security Network. Als u ervoor hebt gekozen om niet deel te nemen aan Kaspersky Security Network, moet u Kaspersky Endpoint Security meteen na de installatie bijwerken.
`CONFIGPATH=<path to the configuration file>`	Het programma installeren met vooraf gedefinieerde instellingen. Om dit te doen, moet u een bestand uploaden dat de instellingen van Kaspersky Endpoint Security definieert. U kunt een configuratiebestand in de lokale interface van het programma maken.
`ALLOWREBOOT=1`	Computer automatisch opnieuw opstarten, indien nodig na de installatie of upgrade van het programma. Als er geen waarde is ingesteld voor deze parameter, wordt het automatisch herstarten van de computer geblokkeerd. Opnieuw opstarten is niet nodig bij de installatie van Kaspersky Endpoint Security. Opnieuw opstarten is alleen nodig als u incompatibele programma's moet verwijderen alvorens u de installatie kunt starten. De computer opnieuw opstarten is mogelijk ook vereist wanneer u de programmaversie updatet.
`SKIPPRODUCTCHECK=1`	Controle op geïnstalleerde software uitschakelen. De lijst met software die compatibiliteitsproblemen kan veroorzaken, vindt u in het bestand incompatible.txt in het distributiepakket. Als er geen waarde is ingesteld voor deze parameter en er wordt software uit de lijst gedetecteerd, wordt de installatie van Kaspersky Endpoint Security beëindigd.
`SKIPPRODUCTUNINSTALL=1`	Schakel de automatische verwijdering van gedetecteerde software uit de lijst incompatible.txt uit. Als er geen waarde is ingesteld voor deze parameter, probeert Kaspersky Endpoint Security de software te verwijderen die compatibiliteitsproblemen kan veroorzaken. Automatische verwijdering van de software kan niet worden ingeschakeld wanneer Kaspersky Endpoint Security wordt geïnstalleerd met behulp van het msiexec-installatieprogramma. Om de software die compatibiliteitsproblemen kan veroorzaken automatisch te verwijderen, gebruik het bestand setup_kes.exe.
`CLEANERSIGNCHECK=0|1`	Het verifiëren van digitale handtekeningen van de gedetecteerde softwarebestanden uit de lijst incompatible.txt. Om de software te verwijderen, voert Kaspersky Endpoint Security het software-installatiebestand uit. Als het installatiebestand geen digitale handtekening heeft, beschouwt Kaspersky Endpoint Security het bestand als onbetrouwbaar en stopt het de verwijdering van software om te voorkomen dat mogelijke schadelijke code wordt uitgevoerd. Als het programma de digitale handtekening van het gedetecteerde softwarebestand niet kan verifiëren, wordt de installatie van Kaspersky Endpoint Security gestopt met een foutmelding. De standaardwaarde is verschillend, afhankelijk van de software-installatiemethode: • `0` betekent dat verificatie van digitale handtekeningen is uitgeschakeld (standaardwaarde indien geïmplementeerd via Kaspersky Security Center). • `1` betekent dat verificatie van digitale handtekeningen is ingeschakeld (standaardwaarde als het programma lokaal wordt geïnstalleerd).
`STANDALONEMODE=1`	Het programma installeren in de Endpoint Detection and Response Agent (EDR Agent) configuratie voor integratie met de Kaspersky Endpoint Detection and Response (KATA) of Kaspersky Endpoint Detection and Response Expert (on-premises) oplossingen. Deze configuratie is nodig als de Endpoint Protection Platform (EPP) van derden wordt geïmplementeerd in uw organisatie naast de Endpoint Detection and Response oplossing. Hierdoor is Kaspersky Endpoint Security in de Endpoint Detection and Response Agent-configuratie compatibel met EPP-programma's van derden.

KLLOGIN	Stel de gebruikersnaam voor toegang tot functies en instellingen van Kaspersky Endpoint Security in (het onderdeel Wachtwoordbeveiliging). De gebruikersnaam wordt samen met de parameters KLPASSWD en KLPASSWDAREA ingesteld. De gebruikersnaam KLAdmin wordt standaard gebruikt.
KLPASSWD	Geef een wachtwoord op voor de toegang tot functies en instellingen van Kaspersky Endpoint Security (het wachtwoord wordt samen de parameters KLLOGIN en KLPASSWDAREA opgegeven). Als u wel een wachtwoord hebt opgegeven maar geen gebruikersnaam bij de parameter KLLOGIN, wordt de gebruikersnaam 'KLAdmin' standaard gebruikt.
KLPASSWDAREA	Geef het bereik van het wachtwoord op voor toegang tot functies en instellingen van Kaspersky Endpoint Security. Wanneer een gebruiker een actie uit dit bereik probeert uit te voeren, 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: • SET – voor het wijzigen van de programma-instellingen. • EXIT – voor het afsluiten van het programma. • DISPROTECT – voor het uitschakelen van beschermingsonderdelen en het stoppen van scantaken. • DISPOLICY – voor het uitschakelen van het Kaspersky Security Center-beleid. • UNINST – voor het verwijderen van het programma op de computer. • DISCTRL – voor het uitschakelen van de controleonderdelen. • REMOVELIC – voor het verwijderen van de licentie. • REPORTS – voor het bekijken van rapporten. • EXPORT – Programma-instellingen exporteren. Bijvoorbeeld KLPASSWDAREA=SET;KLPASSWDAREA=UNINST;KLPASSWDAREA=EXIT. Het KLAdmin-account is gemachtigd om alle acties uit te voeren die met een wachtwoord zijn beveiligd. Daarom is het configureren van het wachtwoordbereik voor het KLAdmin-account onmogelijk. Als u het wachtwoordbereik voor het KLAdmin-account probeert te configureren, verbiedt het programma de opgegeven acties voor de groep "Iedereen".
PROTECTOSSERVICES	Bescherming van de functionaliteit van de besturingssysteemservices. De bescherming van besturingssysteemservices voorkomt dat programma's van derden de werking van besturingssysteemservices verstoren. Dergelijke services omvatten bijvoorbeeld de programma-autostartservice. • 1 betekent dat de bescherming van de besturingssysteemservices is ingeschakeld (standaardwaarde). • 0 betekent dat de bescherming van de besturingssysteemservices is uitgeschakeld.
ENABLETRACES	Programmatracing inschakelen of uitschakelen. Nadat Kaspersky Endpoint Security is gestart, worden de tracebestanden opgeslagen in de map %ProgramData%\Kaspersky Lab\KES.14.1\Traces. Beschikbare waarden: • 1 – tracing is ingeschakeld. • 0 – tracing is uitgeschakeld (standaardwaarde).
TRACESLEVEL	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.
ENABLEAZURESUPPORT	De Azure WVD-compatibiliteitsmodus in- of uitschakelen. Beschikbare waarden: • 1 – Azure WVD-compatibiliteitsmodus is ingeschakeld. • 0 – Azure WVD-compatibiliteitsmodus is uitgeschakeld (standaardwaarde). Deze functie garandeert een correcte weergave van de status van de Azure virtuele machine in de console van Kaspersky Anti Targeted Attack Platform. Om de prestaties van de computer te controleren, verzendt Kaspersky Endpoint Security telemetrie naar KATA-servers. Telemetrie omvat een ID van de computer (Sensor ID). Met de Azure WVD-compatibiliteitsmodus kunt u een permanente unieke Sensor ID toewijzen aan deze virtuele machines. Als de compatibiliteitsmodus is uitgeschakeld, kan de Sensor ID veranderen nadat de computer opnieuw is opgestart vanwege de manier waarop virtuele Azure-machines werken. Dit kan er voor zorgen dat duplicaten van virtuele machines op de console worden weergegeven.

AMPPL	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 website van Microsoft. AM-PPL-technologie is beschikbaar voor de besturingssystemen Windows 10 versie 1703 (RS2) of hoger en Windows Server 2019. Beschikbare waarden: • 1 – Bescherming van de Kaspersky Endpoint Security-processen met AM-PPL-technologie is ingeschakeld. • 0 – Bescherming van de Kaspersky Endpoint Security-processen met AM-PPL-technologie is uitgeschakeld.
UPGRADEMODE	Upgrademodus programma: • Seamless betekent het upgraden van het programma met een herstart van de computer (standaardwaarde). • Force betekent het upgraden van het programma zonder een herstart. U kunt het programma upgraden zonder opnieuw te starten vanaf versie 11.10.0. Als u een eerdere versie van het programma wilt upgraden, moet u de computer opnieuw opstarten. U kunt patches installeren zonder opnieuw te starten vanaf versie 11.11.0. Opnieuw opstarten is niet nodig bij de installatie van Kaspersky Endpoint Security. De upgrademodus van het programma wordt dus gespecificeerd in de programma-instellingen. U kunt deze parameter veranderen in de programma-instellingen of in het beleid. Bij het upgraden van een reeds geïnstalleerd programma, is de prioriteit van de opdrachtregelparameter lager dan die van de parameter gespecificeerd in het bestand programma-instellingen of in het bestand setup.ini. Als de upgrademodus Force is gespecificeerd in de opdrachtregel en de modus Seamless gespecificeerd is in de programma-instellingen, dan wordt de upgrade geïnstalleerd met een heropstart van de computer (Seamless).
RESTAPI	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). Beschikbare waarden: • 1 – Beheer via de REST API is toegestaan. • 0 – Beheer via de REST API is niet toegestaan (standaardwaarde). 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.
RESTAPI_User	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 <DOMAIN>\<UserName> in (bijvoorbeeld, RESTAPI_User=COMPANY\Administrator). U kunt slechts één gebruiker kiezen die met de REST API mag werken. Een gebruikersnaam toevoegen is een vereiste voor het beheer van het programma via de REST API.
RESTAPI_Port	Poort die wordt gebruikt voor het beheer van het programma via de REST API. Poort 6782 wordt standaard gebruikt. Zorg ervoor dat de poort vrij is.
RESTAPI_Certificate	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. Hiervoor moet u een certificaat installeren en vervolgens de payload van elk verzoek ondertekenen.
ADMINKITCONNECTOR	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. Beschikbare waarden: • 1 – Programmabeheer met behulp van beheersystemen is toegestaan (standaardwaarde). • 0 – Programmabeheer is alleen via de lokale interface toegestaan.

`EnableUniqueSensorID`	Het aanmaken van een unieke computer-ID (Sensor ID) tijdens de installatie of update van het programma. (Sensor ID) wordt in de oplossing Kaspersky Anti Targeted Attack Platform gebruikt om computers te identificeren die telemetrie naar de server sturen. Bij het aanmaken van (Sensor ID) gebruikt het programma een algoritme dat rekening houdt met de configuratie van de computer, zoals het serienummer van het moederbord. In sommige gevallen, bijvoorbeeld wanneer het programma in een virtuele omgeving wordt gebruikt, kan (Sensor ID) worden gedupliceerd. Hierdoor kan het Kaspersky Anti Targeted Attack Platform niet identificeren vanaf welke computer de telemetrie wordt verzonden. Om een unieke (Sensor ID) te maken, moet u de parameter `EnableUniqueSensorID=1` instellen. Als gevolg hiervan zal de applicatie een ander algoritme gebruiken om de (Sensor ID) te maken, die rekening houdt met andere gegevens over de computer. Dit zorgt voor een unieke (Sensor ID). Standaard is de parameter niet ingesteld. Het programma erft de (Sensor ID) in de volgende gevallen: • De versie van het programma bijwerken; • de [KES+KEA]-configuratie migreren naar [KES+built-in agent]. Als onderdeel van het programmaherstel probeert het installatieprogramma de Sensor ID over te nemen. Als de Sensor ID niet kan worden hersteld, maakt het programma een nieuwe Sensor ID.
`SKIPKB5007186CHECK=1`	De controle op geïnstalleerde besturingssysteemupdate KB5007186 uitschakelen. Voordat het programma wordt geïnstalleerd, controleert het installatieprogramma de geïnstalleerde besturingssysteemupdates. De KB5007186 update staat op de lijst van besturingssysteemupdates die problemen kunnen veroorzaken voor het programma. Raadpleeg de Knowledge Base van de Technische Support voor gedetailleerde informatie. Daarom breekt het installatieprogramma de installatie af als deze update wordt ontdekt. Stel `SKIPKB5007186CHECK=1` in om door te gaan met de installatie.

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=Password
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.

  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.

- install.cfg – Instellingen voor de werking van Kaspersky Endpoint Security

  Om instellingen uit het configuratiebestand install.cfg toe te passen, moet u het pad naar het bestand opgeven in de volgende opdracht voor programma-installatie: `CONFIGPATH=<path to the configuration file>`.

- setup.reg – registersleutel.

  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.reg wilt toepassen, plaatst u dit bestand 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>`.

Setup /x. 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 (stille installatie). 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 vinden in de Knowledge Base van de Technische Support of 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 /pKLLOGIN=<user name> /pKLPASSWD=<password> /s /x
     ```

     of

     ```
     msiexec.exe /x <GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
     ```

U kunt ook de parameter `SAVEQB` gebruiken om bestanden op te slaan die door het programma zijn gescand en in een back-up zijn geplaatst. Back-ups van bestanden worden opgeslagen in de map `C:\ProgramData\Kaspersky Lab\KES.14.1\QB`. Standaard is het opslaan van bestanden in Back-up uitgeschakeld (`SAVEQB=0`).

Voorbeeld

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

msiexec /i. Het programma herstellen

Tijdens het herstellen controleert en herstelt het programma de integriteit van alle beschadigde programmamodules en systeemregistersleutels die tijdens de installatie van het programma zijn gemaakt.

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

- In de interactieve modus via de Installatiewizard van het programma.
- In de stille modus. Nadat het herstel in de stille modus is gestart, is uw assistentie tijdens het herstelproces niet meer vereist.

Als het installatieprogramma van Kaspersky Endpoint Security wordt uitgevoerd in de herstelmodus en het programma hoeft niet te worden hersteld, dan brengt het installatieprogramma geen wijzigingen aan.

Als het installatieprogramma van Kaspersky Endpoint Security wordt uitgevoerd in de herstelmodus en het programma niet is geïnstalleerd, start het installatieprogramma het installatieproces.

Zo herstelt 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 het herstelproces niet beveiligd is met een wachtwoord:

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL /qn
     ```

     `<GUID>` is de unieke ID van het programma. U kunt de GUID van het programma vinden in de Knowledge Base van de Technische Support of de volgende opdracht te gebruiken:

     ```
     wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
     ```

   - Als het herstelproces beveiligd is met een wachtwoord:

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL KLLOGIN=<user name> KLPASSWD=<password> /qn
     ```

Voorbeeld

```
msiexec.exe /i {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} REINSTALL=ALL KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

AVP-opdrachten

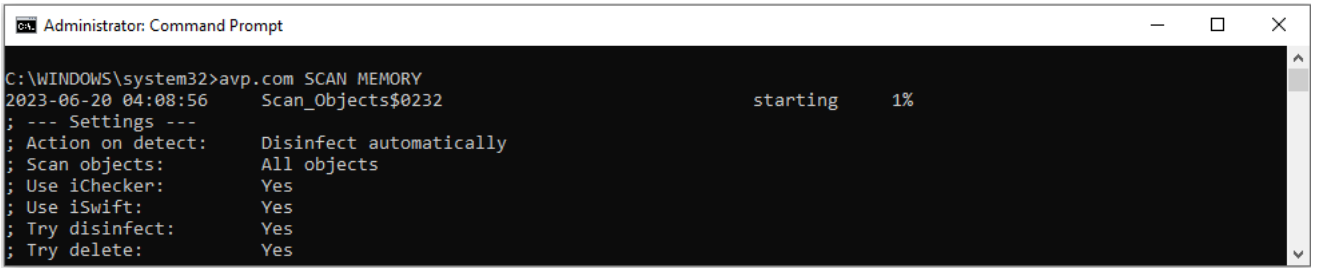
Zo beheert u Kaspersky Endpoint Security vanaf de opdrachtregel:

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.

   U kunt het pad naar het uitvoerbare bestand toevoegen aan de systeemvariabele %PATH% tijdens programma installatie.
3. Gebruik het volgende sjabloon om het commando uit te voeren:

   ```
   avp.com <command> [options]
   ```

Kaspersky Endpoint Security zal nu de opdracht uitvoeren (zie onderstaande afbeelding).



Het programma vanaf de opdrachtregel beheren

SCAN. Malware-scan

Uitvoeren van de taak *Malware-scan*.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Syntaxis van opdracht

```
avp.com SCAN [<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report
file>] [<scan technologies>] [/C:<file with scan settings>]
```

Scanbereik	
`<files to scan>`	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: • `"C:\Program Files (x86)\Example Folder"` – lang pad. • `C:\PROGRA~2\EXAMPL~1` – kort pad.
`/ALL`	Start de taak *Malware-scan*. 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 In Kaspersky Endpoint Security voor Windows 12.12 valt e-mail niet onder het scanbereik van het programma. Het scannen van inkomende en uitgaande e-mails wordt uitgevoerd door het onderdeel Mail Threat Protection. Als u een oudere versie van de beheerplug-in gebruikt, sluit het programma e-mail uit van het scanbereik, zelfs als het beleid deze wel bevat.
`/MEMORY`	Scan het kernelgeheugen
`/STARTUP`	Scan de objecten die bij de opstart van het besturingssysteem worden geladen
`/REMDRIVES`	Scan verwisselbare schijven.
`/FIXDRIVES`	Scan harde schijven.
`/NETDRIVES`	Scan netwerkschijven.
`/QUARANTINE`	Scan de bestanden in Back-up van Kaspersky Endpoint Security.
`/@:<file list.lst>`	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: • `"C:\Program Files (x86)\Example Folder"` – lang pad. • `C:\PROGRA~2\EXAMPL~1` – kort pad.

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 melden als desinfectie mislukt**. Als deze optie is geselecteerd, probeert Kaspersky Endpoint Security automatisch om alle gevonden geïnfecteerde bestanden te desinfecteren. Indien desinfectie mislukt, 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 het programma automatisch om ieder gevonden geïnfecteerd bestand te desinfecteren. Mocht de desinfectie mislukken, dan wordt het bestand door het programma verwijderd. Deze actie is standaard geselecteerd.
`/i3`	**Verwijderen indien desinfectie mislukt**. Ook samengestelde bestanden (bijvoorbeeld archieven) worden verwijderd als het geïnfecteerde bestand niet kan worden gedesinfecteerd of verwijderd.
`/i4`	**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, scant het programma alleen infecteerbare bestanden. De bestandsindeling wordt dan bepaald op basis van de bestandsextensie.

`/fi`	**Bestanden gescand op indeling**. Als deze instelling is ingeschakeld, scant het programma alleen infecteerbare bestanden. 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 het programma, 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:<file mask>`	Bestanden die overeenkomen met het bestandsmasker worden niet gescand. Bijvoorbeeld: • Het masker `*.exe` omvat alle paden naar bestanden met de EXE-extensie. • Het masker `example*` omvat alle paden naar bestanden met de naam EXAMPLE.
`-e:<seconds>`	Bestanden waarvan de scan langer duurt dan de opgegeven tijdslimiet (in seconden) worden niet gescand.
`-es:<megabytes>`	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:<report file>`	Sla alleen kritieke gebeurtenissen in het rapportbestand op.
`/RA:<report file>`	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:<file with scan settings>`	Bestand met de instellingen van de taak *Malware-scan*. Het bestand moet handmatig worden aangemaakt en in de TXT-indeling worden opgeslagen. Het bestand kan de volgende inhoud hebben: `[<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>]`.

Voorbeeld

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

UPDATE. Databases en softwaremodules van het programma bijwerken

Uitvoeren van de taak *Update van databases en programmamodules*.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Deze opdracht kan niet worden uitgevoerd als het programma is geïnstalleerd in Light Agent-modus.

Syntaxis van opdracht

```
avp.com UPDATE [local] ["<update source>"] [/R[A]:<report file>] [/C:<file with update settings>]
```

Instellingen van updatetaak	
`local`	Start van de taak *Update van databases en programmamodules* die na de installatie van het programma automatisch is gemaakt. U kunt de instellingen van de taak *Update van databases en programmamodules* 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 taak *Update van databases en programmamodules* met de standaardinstellingen of met de instellingen die in de opdracht zijn opgegeven. U kunt de taakinstellingen *Update van databases en programmamodules* als volgt configureren: • `UPDATE` start de taak *Update van databases en programmamodules* met de standaardinstellingen: de updatebron is Kaspersky-updateservers, het account is Systeem en andere standaardinstellingen. • `UPDATE local` start de taak *Update van databases en programmamodules* die automatisch werd aangemaakt na installatie (voorgedefinieerde taak). • `UPDATE <update settings>` start de taak *Update van databases en programmamodules* met handmatig gedefinieerde instellingen (zie hieronder).

Updatebron	
`"<update source>"`	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:<report file>`	Sla alleen kritieke gebeurtenissen in het rapportbestand op.
`/RA:<report file>`	Sla alle gebeurtenissen in een rapportbestand op.

Geavanceerde instellingen	
`/C:<file with update settings>`	Bestand met de instellingen van de taak *Update van databases en programmamodules*. Het bestand moet handmatig worden aangemaakt en in de TXT-indeling worden opgeslagen. Het bestand kan de volgende inhoud hebben: `["<update source>"] [/R[A]:<report file>]`.

Voorbeeld

```
avp.com UPDATE local
```

```
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.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Deze opdracht kan niet worden uitgevoerd als het programma is geïnstalleerd in Light Agent-modus.

Syntaxis van opdracht

```
avp.com ROLLBACK [/R[A]:<report file>]
```

Gebeurtenissen opslaan in een modus rapportbestand (alleen voor Scan-, Updater- en Rollback-profielen)	
`/R:<report file>`	Sla alleen kritieke gebeurtenissen in het rapportbestand op.
`/RA:<report file>`	Sla alle gebeurtenissen in een rapportbestand op.

Voorbeeld

```
avp.com ROLLBACK /RA:rollback.txt
```

TRACES. Tracing

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.14.1\Traces`. Standaard is tracing uitgeschakeld.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Syntaxis van opdracht

```
avp.com TRACES on|off [<tracing level>] [<advanced settings>]
```

Tracingniveau	
`<tracing level>`	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 `file` en `mem`.
`file`	Sla één tracebestand op (geen maximale grootte).

`rot`	Sla traces op als een beperkt aantal bestandensets met een beperkte grootte en overschrijf de oudere bestanden wanneer de maximale grootte wordt bereikt.
`mem`	Sla traces in dumpbestanden op.

Voorbeeld

```
avp.com TRACES on 500
```

```
avp.com TRACES off
```

```
avp.com TRACES on 500 mem
```

```
avp.com TRACES off file
```

START. Een profiel starten

Een profiel starten (bijvoorbeeld een database-update starten of een beschermingsonderdeel inschakelen).

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Syntaxis van opdracht

```
avp.com START <profile> [/R[A]:<report file>]
```

Profiel	
`<profile>`	Naam van profiel. Een *Profiel* is een onderdeel, taak of functie van Kaspersky Endpoint Security. U kunt de lijst met beschikbare profielen bekijken door de opdracht `HELP START` uit te voeren.

Gebeurtenissen opslaan in een modus rapportbestand (alleen voor Scan-, Updater- en Rollback-profielen)	
`/R:<report file>`	Sla alleen kritieke gebeurtenissen in het rapportbestand op.
`/RA:<report file>`	Sla alle gebeurtenissen in een rapportbestand op.

Voorbeeld

```
avp.com START Scan_Objects
```

STOP. Een profiel stoppen

De uitvoering van het profiel stoppen (bijvoorbeeld het stoppen van een scan van verwisselbare schijven of het uitschakelen van een beschermingsonderdeel).

Voor het uitvoeren van deze opdracht moet Wachtwoordbeveiliging ingeschakeld zijn. De gebruiker moet de machtigingen **Beschermingsonderdelen uitschakelen** en **Controleonderdelen uitschakelen** hebben.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Syntaxis van opdracht

```
avp.com STOP <profile> /login=<user name> /password=<password>
```

Profiel	
`<profile>`	Naam van profiel. Een *Profiel* is een onderdeel, taak of functie van Kaspersky Endpoint Security. U kunt de lijst met beschikbare profielen bekijken door de opdracht `HELP STOP` uit te voeren.

Authenticatie	
`/login=<user name> /password=<password>`	Gebruikersaccountgegevens met de vereiste machtigingen voor wachtwoordbeveiliging.

STATUS. Profielstatus

Statusinformatie weergeven voor programmaprofielen (bijvoorbeeld `running` of `completed`). 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.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Syntaxis van opdracht

```
avp.com STATUS [<profile>]
```

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.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Syntaxis van opdracht

```
avp.com STATISTICS <profile>
```

RESTORE. Bestanden vanuit Back-up terugzetten

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.14.1\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.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Syntaxis van opdracht

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Geavanceerde instellingen	
`/REPLACE`	Overschrijf een bestaand bestand.
`<file name>`	De naam van het bestand dat wordt teruggezet.

Authenticatie	
`/login=<user name> /password=<password>`	Gebruikersaccountgegevens met de vereiste machtigingen voor wachtwoordbeveiliging.

Voorbeeld

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

EXPORT. Programma-instellingen exporteren

Instellingen exporteren van Kaspersky Endpoint Security naar een bestand. Als de opdracht alleen de naam bevat van het bestand waarnaar u de instellingen wilt exporteren, plaatst het programma het bestand als volgt:

- Als het pad naar avp.com wordt toegevoegd aan de systeemvariabele %PATH%, plaatst het programma het bestand in de map `C:\Windows\SysWOW64`.
- Als u de opdracht uitvoert vanuit de installatiemap van het programma, mislukt het exporteren omdat de zelfbescherming van het programma het maken van een nieuw bestand in de programmamap blokkeert. Om programma-instellingen naar een bestand te exporteren, voer het bestandspad in.

Voor het uitvoeren van deze opdracht moet Wachtwoordbeveiliging ingeschakeld zijn. De gebruiker moet de machtiging **Instellingen exporteren** hebben.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Syntaxis van opdracht

```
avp.com EXPORT <profile> <file name> /login=<user name> /password=<password>
```

Profiel	
`<profile>`	Naam van profiel. Een *Profiel* is een onderdeel, taak of functie van Kaspersky Endpoint Security. U kunt de lijst met beschikbare profielen bekijken door de opdracht `HELP EXPORT` uit te voeren.

Te exporteren bestand	
`<file name>`	De naam van het bestand waarnaar de programma-instellingen worden geëxporteerd. U kunt ook het bestandspad invoeren. U kunt de instellingen van Kaspersky Endpoint Security exporteren naar een DAT- of CFG-configuratiebestand, een TXT-tekstbestand of een XML-document.

Authenticatie	
`/login=<user name> /password=<password>`	Gebruikersaccountgegevens met de vereiste machtigingen voor wachtwoordbeveiliging.

Voorbeeld

```
avp.com EXPORT ids ids_C:\Users\Fred123\Documents\config.dat
```

```
avp.com EXPORT fm fm_config.txt
```

IMPORT. Programma-instellingen importeren

Kaspersky Endpoint Security-instellingen importeren uit een bestand dat is gemaakt met de `EXPORT` opdracht.

Voor het uitvoeren van deze opdracht moet Wachtwoordbeveiliging ingeschakeld zijn. De gebruiker moet de machtiging **Programma-instellingen configureren** hebben.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Syntaxis van opdracht

```
avp.com IMPORT <file name> /login=<user name> /password=<password>
```

Te importeren bestand	
`<file name>`	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=<user name> /password=<password>`	Gebruikersaccountgegevens met de vereiste machtigingen voor wachtwoordbeveiliging.

Voorbeeld

```
avp.com IMPORT config.dat /login=KLAdmin /password=samplePassword
```

ADDKEY. Een licentiebestand toepassen

Kaspersky Endpoint Security activeren met een sleutelbestand. Als het programma al is geactiveerd, wordt de licentie toegevoegd als een reservelicentie.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Deze opdracht kan niet worden uitgevoerd als het programma is geïnstalleerd in Light Agent-modus.

Syntaxis van opdracht

```
avp.com ADDKEY <file name> [/login=<user name> /password=<password>]
```

Licentiebestand	
`<file name>`	Naam van licentiebestand.

Authenticatie	
`/login=<user name> /password=<password>`	Gegevens van gebruikersaccount. Deze gebruikersgegevens moeten alleen worden ingevoerd als Wachtwoordbeveiliging is ingeschakeld.

Voorbeeld

```
avp.com ADDKEY file.key
```

LICENSE. Licentiebeheer

Beheer van de licentiecodes van Kaspersky Endpoint Security, 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 **Sleutel verwijderen** hebben.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Deze opdracht kan niet worden uitgevoerd als het programma is geïnstalleerd in Light Agent-modus.

Syntaxis van opdracht

```
avp.com LICENSE <operation> [/login=<user name> /password=<password>]
```

Bewerking	
`/ADD <file name>`	Kaspersky Endpoint Security activeren met een sleutelbestand. Als het programma al is geactiveerd, wordt de licentie toegevoegd als een reservelicentie.
`/ADD <activation code>`	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 <license ID>`	Werk de status van licenties bij met behulp van licentie-ID. Met deze opdracht kunt u de status van EDR Add-on, MDR Add-on, KUMA Add-on of andere licenties bijwerken. U kunt de licentie-ID vinden op het licentiecertificaat. Als gevolg hiervan ontvangt het programma actuele licentiestatusgegevens van Kaspersky-activeringsservers.
`/CHECK`	Licentie-informatie krijgen. Kaspersky Endpoint Security geeft informatie weer over alle toegevoegde licentiesleutels, inclusief reservecodes, EDR Add-on, MDR Add-on, KUMA Add-on-sleutels en andere sleutels. Kaspersky Endpoint Security toont de volgende licentie-informatie: • licentienaam; • licentie-identificatie; • adres van de Protection Server (SVM) waarmee de virtuele machine is verbonden waarop het programma is geïnstalleerd in de Light Agent-modus; • licentietype: proefversie, commercieel, bèta, abonnement; • datum en tijd van activering van het programma; • datum en tijd van het verlopen van de licentie; • Aantal dagen tot het verlopen van de licentie.
`/CHECK <license ID>`	Verkrijg licentie-informatie via ID. Met deze opdracht kunt u licentie-informatie opvragen. U kunt de licentie-ID vinden op het licentiecertificaat.

`/DEL /login=<user name> /password=<password>`	Verwijder de licentiesleutel van het programma. De reservelicentie wordt ook verwijderd.
`/DEL <license ID> /login=<user name> /password=<password>`	Verwijder de sleutel met behulp van de licentie-ID. Met deze opdracht kunt u een sleutel verwijderen uit EDR Add-on, MDR Add-on, KUMA Add-on of andere licenties. U kunt de licentie-ID vinden op het licentiecertificaat.

Authenticatie	
`/login=<user name> /password=<password>`	Gebruikersaccountgegevens met de vereiste machtigingen voor wachtwoordbeveiliging.

Voorbeeld

```
avp.com LICENSE /ADD file.key
avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
avp.com LICENSE /DEL 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

Voorbeeld

```
avp.com LICENSE /ADD file.key
```

```
avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
```

```
avp.com LICENSE /DEL 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

RENEW. Een licentie aanschaffen

Open de Kaspersky-website om een licentie te kopen of te verlengen.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Deze opdracht kan niet worden uitgevoerd als het programma is geïnstalleerd in Light Agent-modus.

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.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

EXIT. Het programma afsluiten

Kaspersky Endpoint Security afsluiten. 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.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Syntaxis van opdracht

```
avp.com EXIT /login=<user name> /password=<password>
```

EXITPOLICY. Beleid uitschakelen

Het Kaspersky Security Center-beleid op de computer uitschakelen. 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.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Syntaxis van opdracht

```
avp.com EXITPOLICY /login=<user name> /password=<password>
```

STARTPOLICY. Beleid inschakelen

Het Kaspersky Security Center-beleid op de computer inschakelen. De programma-instellingen worden geconfigureerd volgens het beleid.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

DISABLE. Bescherming uitschakelen

File Threat Protection uitschakelen 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.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

SPYWARE. Detectie van spyware

Detectie van spyware beheren. De detectie van spyware is standaard ingeschakeld.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Syntaxis van opdracht

```
avp.com SPYWARE on|off
```

KSN. Schakelen tussen KSN / KPSN

Een Kaspersky-oplossing selecteren om de reputatie van bestanden of websites te bepalen. Kaspersky Endpoint Security ondersteunt de volgende infrastructuuroplossingen voor het werken met Kaspersky-reputatiedatabases:

- *Kaspersky Security Network (KSN)* is de oplossing die door de meeste Kaspersky-programma's wordt gebruikt. Deelnemers aan KSN ontvangen informatie van Kaspersky 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-databases die reputatie-informatie en statistische gegevens bevatten.

- *Kaspersky Private Security Network (KPSN)* is een oplossing waarmee gebruikers van computers waarop Kaspersky Endpoint Security of andere Kaspersky-programma's worden gehost toegang krijgen tot reputatiedatabases van Kaspersky en tot andere statistische gegevens zonder gegevens naar Kaspersky te versturen vanaf hun eigen computers. KPSN 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.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Deze opdracht kan niet worden uitgevoerd als het programma is geïnstalleerd in Light Agent-modus.

Syntaxis van opdracht

```
avp.com KSN /global | /private <file name>
```

Configuratiebestand Kaspersky Security Network	
`<file name>`	Naam van het configuratiebestand met Kaspersky Private Security Network-instellingen. Dit bestand heeft de extensie PKCS7 of PEM.

Voorbeeld

```
avp.com KSN /global
avp.com KSN /private C:\ksn_config.pkcs7
```

Voorbeeld

```
avp.com KSN /global
```

```
avp.com KSN /private C:\ksn_config.pkcs7
```

SERVERBINDINGDISABLE. Schakel de verbindingsbeveiliging van de server uit

Voert de taak *Administration Server verbindingsbescherming* uit, waardoor het wachtwoord van de computerverbinding met de Administration Server wordt verwijderd. Op deze manier schakelt de taak de bescherming van de Administration Server-verbinding uit.

Voor het uitvoeren van deze opdracht moet Wachtwoordbeveiliging ingeschakeld zijn.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Syntaxis van opdracht

```
avp.com SERVERBINDINGDISABLE [/password=<password>]
```

Wachtwoord	
`/password=<password>`	Het wachtwoord van de KL Admin-gebruikersaccount of het wachtwoord van de *Administration Server verbindingsbescherming* taak. Als de parameter niet is opgegeven, vraagt Kaspersky Endpoint Security u op de volgende regel om een wachtwoord in te voeren.

KESCLI-opdrachten

Met KESCLI-opdrachten kunt u informatie ontvangen over de status van computerbeveiliging met behulp van het OPSWAT-onderdeel en kunt u standaardtaken uitvoeren, zoals de taken *Malware-scan* en *Update van databases en programmamodules*.

U kunt de lijst met KESCLI-opdrachten bekijken met de opdracht `kescli --help` of de verkorte opdracht `kescli -h`.

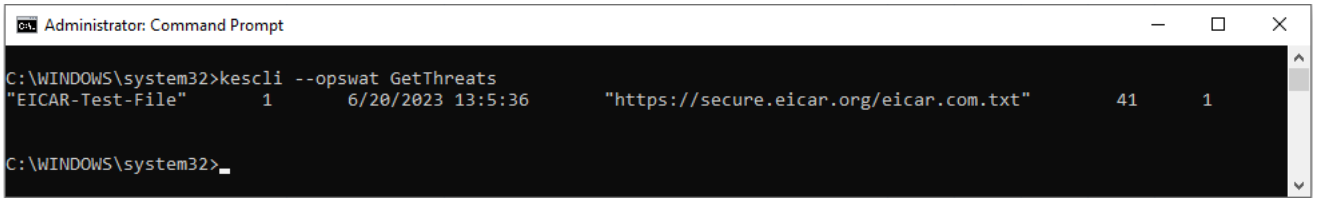
Zo beheert u Kaspersky Endpoint Security vanaf de opdrachtregel:

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.

   U kunt het pad naar het uitvoerbare bestand toevoegen aan de systeemvariabele %PATH% tijdens programma installatie.
3. Gebruik het volgende sjabloon om het commando uit te voeren:

   ```
   kescli <command> [options]
   ```

Kaspersky Endpoint Security zal nu de opdracht uitvoeren (zie onderstaande afbeelding).



Het programma vanaf de opdrachtregel beheren

Scan. Malware-scan

De taak *Malware-scan* (Volledige Scan) uitvoeren.

Om de taak uit te voeren, moet de beheerder het gebruik van lokale taken in het beleid toestaan.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen.

Syntaxis van opdracht

```
kescli --opswat Scan "<scan scope>" <action on threat detection>
```

U kunt de voltooiingsstatus van de taak *Malware-scan* controleren met de opdracht `GetScanState` en kunt de datum en tijd van de laatste voltooiing zien met de opdracht `GetLastScanTime`.

Scanbereik	
`<scan scope>`	Een lijst met bestanden en mappen, gescheiden door `;`-. Bijvoorbeeld `"C:\Program Files (x86)\Example Folder"`.

Actie bij detectie van een dreiging	
`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 het programma automatisch om ieder gevonden geïnfecteerd bestand te desinfecteren. Mocht de desinfectie mislukken, dan wordt het bestand door het programma verwijderd. 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

Informatie weergeven over de status van de taakvoltooiing van *Malware-scan* (*Volledige Scan*):

- `1` – de scan wordt uitgevoerd.
- `0` – de scan wordt niet uitgevoerd.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen.

Syntaxis van opdracht

```
kescli --opswat GetScanState
```

GetLastScanTime. De voltooiingstijd van de scan bepalen

Informatie weergeven over de datum en tijd van de laatste taakvoltooiing *Malware-scan* (*Volledige Scan*).

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen.

Syntaxis van opdracht

```
kescli --opswat GetLastScanTime
```

GetThreats. Gegevens verkrijgen over gedetecteerde bedreigingen

Een lijst met gedetecteerde bedreigingen weergeven (*Report on threats*). Dit rapport bevat informatie over bedreigingen en virusactiviteiten gedurende de laatste 30 dagen voorafgaand aan het maken van het rapport.

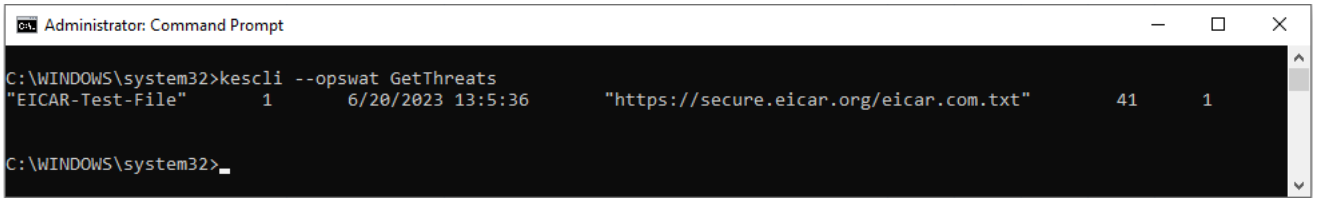
Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen.

Syntaxis van opdracht

```
kescli --opswat GetThreats
```

Wanneer deze opdracht wordt uitgevoerd, verzendt Kaspersky Endpoint Security een antwoord in de volgende indeling:

```
<name of detected object> <type of object> <detection date and time> <path to file>
<action on threat detection> <threat danger level>
```



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`	Verborgen bestanden (`Hidden`).
`23`	Programma's waarvoor aandacht vereist is (`Pupware`).
`24`	Afwijkend gedrag (`Anomaly`).
`30`	Niet bepaald (`Undetect`).
`40`	Advertentiebanners (`Banner`).
`50`	Netwerkaanval (`Attack`).
`51`	Toegang tot register (`Registry`).

52	Verdacht activiteit (`Suspicion`).
60	Kwetsbaarheden (`Vulnerability`).
70	Phishing (`Phishing`).
80	Ongewenste e-mailbijlage (`Attachment`).
90	Malware gedetecteerd door Kaspersky Security Network (`Urgent`).
100	Onbekende link (`Suspic 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 uitzonderingen (`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 *Laag*)

UpdateDefinitions. Databases en softwaremodules van het programma bijwerken

Uitvoeren van de taak *Update van databases en programmamodules*. 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.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen.

Deze opdracht kan niet worden uitgevoerd als het programma is geïnstalleerd in Light Agent-modus.

Syntaxis van opdracht

```
kescli --opswat UpdateDefinitions
```

Je kunt de uitgiftedatum en -tijd van de huidige antivirusdatabases bekijken door de opdrachtregel `GetDefinitionsetState` te gebruiken.

GetDefinitionState. Bepalen van de laatste updatedatum en -tijd van de databases

Informatie weergeven over de updatedatum en -tijd van de gebruikte antivirusdatabases.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen.

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).

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen.

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

Informatie weergeven over de status van het onderdeel File Threat Protection:

- `1` – het component is ingeschakeld.
- `0` – het component is uitgeschakeld.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen.

Syntaxis van opdracht

```
kescli --opswat GetRealTimeProtectionState
```

GetEncryptionState. Schijfversleuteling status

Informatie weergeven over de schijfversleutelingsstatus:

- `1` betekent dat de schijf wordt beschermd door disk encryption-technologie van Kaspersky of BitLocker.
- `0` betekent dat de schijf niet is versleuteld.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen.

Syntaxis van opdracht

```
kescli --opswat GetEncryptionState
```

Version. De versie van het programma bepalen

De versie van Kaspersky Endpoint Security voor Windows weergeven.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen.

Syntaxis van opdracht

```
kescli --Version
```

U kunt ook de verkorte opdracht `-v` gebruiken.

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 <command>`.

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. Gebruik het volgende sjabloon om het commando uit te voeren:

   ```
   avp.com <command> [options]
   ```

   Kaspersky Endpoint Security zal nu de opdracht uitvoeren.

SANDBOX. Sandbox beheren

Opdrachten voor het beheren van het onderdeel Sandbox:

- Schakel het onderdeel Sandbox in of uit.

  Het onderdeel Sandbox bieden interactie met de Kaspersky Sandbox-oplossing en de KATA Sandbox-onderdeel, die deel uitmaakt van het Kaspersky Anti Targeted Attack Platform.

- Het onderdeel Kaspersky Sandbox configureren:

  - Verbind de computer met de 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. Voor details over het implementeren van virtuele afbeeldingen en het configureren van Sandbox-servers, raadpleeg de Hulp bij Kaspersky Sandbox en Hulp bij Kaspersky Anti Targeted Attack Platform.

- Configureer de connectie-time-out voor de server.

  Time-out van verbinding voor de Sandbox-server (voor Kaspersky Sandbox) of Central Node-server (voor KATA). Nadat de geconfigureerde time-out is verstreken, stuurt Kaspersky Endpoint Security een verzoek naar de volgende server. U kunt de verbindingstime-out voor de server verlengen als uw verbindingssnelheid laag is of als de verbinding onstabiel is. De aanbevolen timeout voor een aanvraag is 0,5 seconden of minder.

- Configureer een vertrouwde verbinding tussen de computer en de servers.

  Als u een vertrouwde verbinding met de Sandbox-server (voor Kaspersky Sandbox) of Central Node server (voor KATA) wilt configureren, moet u een TLS-certificaat voorbereiden. Vervolgens moet u het certificaat met behulp van een beleid aan de computer toevoegen. U moet het certificaat ook toevoegen aan de Sandbox-server (voor Kaspersky Sandbox) of Central Node server (voor KATA).

- De integratiemodus configureren.

  U moet een oplossing selecteren waarvan Sandbox deel uitmaakt, namelijk Kaspersky Sandbox of KATA Sandbox. *Kaspersky Sandbox* is een zelfstandige Detection and Response-oplossing van Kaspersky. *KATA Sandbox* is een onderdeel van de Kaspersky Anti Targeted Attack Platform-oplossing. Wanneer het onderdeel is geïntegreerd met KATA Sandbox, kan het in de volgende modi werken:

  - **Manually**. De gebruiker stuurt het bestand handmatig in voor scannen vanuit het contextmenu (**Verzenden naar Sandbox**).

  - **Automatically**. Het programma detecteert automatisch objecten en stuurt ze in naar Sandbox om ze te scannen.

  - **Combined**.

- De huidige instellingen van het onderdeel tonen.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Syntaxis van opdracht

```
avp.com stop sandbox [/login=<user name> /password=<password>]
```

```
avp.com start sandbox
```

```
avp.com sandbox /set [--servers=<address:port>] [--pinned-certificate=<path to the TLS certificate>] [--client-certificate=<path to the PFX archive>] [--client-certificate-password=<password>] [--timeout=<Sandbox server connection timeout (ms)>] [--mode=<KSB|KATAManual|KATAAuto|KATAFull>] [/login=<user name> /password=<password>]
```

Bewerking	
`stop`	Het onderdeel Sandbox uitschakelen.
`start`	Het onderdeel Sandbox inschakelen.

`set`	Het onderdeel Sandbox configureren. U kunt de volgende instellingen configureren:
	• Voeg Sandbox-servers (`--servers`) toe
	• Voeg een TLS-certificaat (`--pinned-certificate`) toe
	• Voeg een crypto-container toe (`--client-certificate`)
	• Geef een wachtwoord op voor de crypto-container (`--client-certificate-password`);
	• Stel de connectie-time-out (`--timeout`) voor de server in
	• Selecteer een integratiemodus (`--mode`):
	  • `KSB` – integratie met Kaspersky Sandbox;
	  • `KATAManual` – handmatige integratie met KATA Sandbox;
	  • `KATAAuto` – automatische integratie met KATA Sandbox;
	  • `KATAFull` – gecombineerde integratie met KATA Sandbox.

`show`	Toon de huidige instellingen van het component. U krijgt de volgende reactie:
	`sandbox.timeout=<Sandbox server connection timeout (ms)>`
	`sandbox.servers=<list of Sandbox servers>`
	`sanbox.mode=<integration mode>`
	`sandbox.tls=<trusted connection status>`

Authenticatie	
`/login=<user name> /password=<password>`	Gebruikersaccountgegevens met de vereiste machtigingen voor wachtwoordbeveiliging.

Voorbeeld

```
avp.com SANDBOX /SET --servers=127.0.0.1:8080;127.0.0.2:8080 --pinned-certificate=c:\my_certs\my.cer --mode=KSB
/login=login /password=password
```

PREVENTION. Preventie van uitvoering beheren

Het onderdeel Preventie van uitvoering uitschakelen of de huidige instellingen van het onderdeel weergeven, inclusief de lijst met regels voor preventie van uitvoering.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Syntaxis van opdracht

```
avp.com prevention disable
```

```
avp.com 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: <rule ID>
target: script|process|document
```

`md5: <MD5 hash of the file>`

`sha256: <SHA256 hash of the file>`

`pattern: <path to the object>`

`case-sensitive: true|false`

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.
- `9` – verkeerde werking (bijvoorbeeld een poging om het component uit te schakelen wanneer het al is uitgeschakeld).

ISOLATION. Netwerkisolatie beheren

Netwerkisolatie van de computer uitschakelen of de huidige instellingen van het onderdeel weergeven. Componentinstellingen bevatten ook een lijst met netwerkverbindingen die zijn toegevoegd aan uitzonderingen.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Syntaxis van opdracht

```
avp.com isolation /OFF /login=<user name> /password=<password>
```

```
avp.com isolation /STAT
```

Als resultaat van de opdracht `stat` ontvangt u de volgende reactie: `Network isolation on|off`.

RESTORE. Bestanden terugzetten vanuit quarantaine

Een bestand uit quarantaine herstellen naar de oorspronkelijke map. *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 wanneer het is geïntegreerd met Kaspersky Detection and Response-oplossingen. 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, Kaspersky Endpoint Detection and Response Expert Help, Kaspersky Anti Targeted Attack Platform Help, en Kaspersky Endpoint Detection and Response Expert (on-premises) 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).

Het herstellen van bestanden vanuit Quarantaine brengt de volgende speciale overwegingen met zich mee:

- Als de doelmap is verwijderd of als de gebruiker geen toegangsrechten tot die map heeft, plaatst het programma het bestand in de map `%DataRoot%\QB\Restored`. Daarna moet u het bestand handmatig naar de bestemmingsmap verplaatsen.
- Het programma behandelt de naam van het bestand dat wordt hersteld als hoofdlettergevoelig. Als u de hoofdletters in de bestandsnaam niet correct invoert, herstelt het programma het bestand niet.
- Als de doelmap al een bestand met dezelfde naam heeft, annuleert het programma het terugzetten van het bestand.
- Als u de KATA (EDR)-oplossing gebruikt, slaat het programma een kopie van het bestand op in quarantaine nadat het bestand is hersteld. U moet de quarantaine handmatig wissen. Voor EDR Optimum- en EDR Expert-oplossingen verwijdert het programma het bestand na herstel.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Syntaxis van opdracht

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Geavanceerde instellingen	
`/REPLACE`	Overschrijf een bestaand bestand.
`<file name>`	De naam van het bestand dat wordt teruggezet.

Authenticatie	
`/login=<user name> /password=<password>`	Gebruikersaccountgegevens met de vereiste machtigingen voor wachtwoordbeveiliging.

Voorbeeld

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

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.

IOCSCAN. Scannen op IoC's (Indicators of Compromise)

Uitvoeren van de taak *IOC Scan*. 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*-taak kunnen Indicators of Compromise op de computer worden gevonden en maatregelen als respons op deze dreiging worden genomen.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

De IOC-scan wordt afgebroken na 128 overeenkomsten met compromitterende indicatoren die worden beschreven in de IOC-bestanden. Dit is nodig om het aantal items in het rapport IOC-scantaak te beperken om de analyse ervan te vergemakkelijken en om te voorkomen dat het rapport overloopt vanwege onnauwkeurig geformuleerde indicatorren van compromise die een groot aantal overeenkomsten kunnen genereren.

Syntaxis van opdracht

```
avp.com IOCSCAN <full path to the IOC file>|/path=<path to the IOC files folder> [/process=on|off] [/hint=<full
path to executable file of a process|full file path>] [/registry=on|off] [/dnsentry=on|off] [/arpentry=on|off]
[/ports=on|off] [/services=on|off] [/system=on|off] [/users=on|off] [/volumes=on|off] [/eventlog=on|off]
[/datetime=<event publication date>] [/channels=<list of channels>] [/files=on|off] [/drives=
<all|system|critical|custom>] [/excludes=<list of exclusions>][/scope=<list of folders to scan>]
```

IOC-bestanden	
`<full path to the IOC file>`	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`. Bijvoorbeeld `C:\Users\Admin\Desktop\IOC\file1.ioc`
`/path=<path to the folder with IOC files>`	Pad naar de map met IOC-bestanden die u wilt gebruiken voor het scannen. *IOC-bestanden* 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 OpenIOC-norm. Bijvoorbeeld `C:\Users\Admin\Desktop\IOC`

Gegevenstype voor IOC-scannen	
`/process=on|off`	Analyseer procesgegevens tijdens het uitvoeren van de IOC-scan (ProcessItem-term). Als de waarde van het argument `off` is, analyseert Kaspersky Endpoint Security de processen die tijdens de scan op de computer worden uitgevoerd niet. Als het IOC-bestand IOC-termen van het ProcessItem-IOC-document bevat, worden deze genegeerd (aangemerkt als 'geen hit'). 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.
`/hint=<full path to the executable file of the process|full path to the file>`	Bestandsgegevens analyseren bij het uitvoeren van de IOC-scan (ProcessItem en FileItemterms). U kunt op een van de volgende manieren een bestand selecteren: • `<full path to the executable file of the process>` – ProcessItem term; • `<full path to the file>` – FileItem term.
`/registry=on|off`	Analyseer Windows-registergegevens tijdens het uitvoeren van een IOC-scan (RegistryItem-term). Als de waarde van het argument `off` is, scant Kaspersky Endpoint Security het Windows-register niet. Als het IOC-bestand termen uit het RegistryItem-IOC-document bevat, worden deze genegeerd (aangemerkt als 'geen hit'). 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. Voor het gegevenstype RegistryItem scant Kaspersky Endpoint Security een reeks registersleutels.
`/dnsentry=on|off`	Analyseer de gegevens over records in de lokale DNS-cache tijdens het uitvoeren van de IOC-scan (DnsEntryItem-term). Als de waarde van het argument `off` is, scant Kaspersky Endpoint Security de lokale DNS-cache niet. Als het IOC-bestand termen uit het DnsEntryItem-IOC-document bevat, worden deze genegeerd (aangemerkt als 'geen hit'). 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.
`/arpentry=on|off`	Analyseer de gegevens over records in de ARP-tabel tijdens het uitvoeren van de IOC-scan (ArpEntryItem-term). Als de waarde van het argument `off` is, scant Kaspersky Endpoint Security de ARP-tabel niet. Als het IOC-bestand termen uit het ArpEntryItem-IOC-document bevat, worden deze genegeerd (aangemerkt als 'geen hit'). Als er geen argument wordt opgegeven, analyseert Kaspersky Endpoint Security de ARP-tabel alleen als het ArpEntryItem-IOC-document is gedefinieerd in het IOC-bestand dat voor de scan wordt gebruikt.
`/ports=on|off`	Analyseer gegevens over poorten die openstaan voor luisteren tijdens het uitvoeren van de IOC-scan (PortItem-term). Als de waarde van het argument `off` is, scant Kaspersky Endpoint Security de tabel met actieve verbindingen op het apparaat niet. Als het IOC-bestand termen uit het PortItem-IOC-document bevat, worden deze genegeerd (aangemerkt als 'geen hit'). Als er geen argument wordt opgegeven, analyseert Kaspersky Endpoint Security de tabel met actieve verbindingen alleen als het PortItem-IOC-document is gedefinieerd in het IOC-bestand dat voor de scan wordt gebruikt.

`/services=on|off`	Analyseer gegevens over services die zijn geïnstalleerd op het apparaat tijdens het uitvoeren van de IOC-scan (ServiceItem-term). Als de waarde van het argument `off` is, scant Kaspersky Endpoint Security de gegevens over services die zijn geïnstalleerd op het apparaat niet. Als het IOC-bestand termen uit het ServiceItem-IOC-document bevat, worden deze genegeerd (aangemerkt als 'geen hit'). Als er geen argument wordt opgegeven, analyseert Kaspersky Endpoint Security servicegegevens alleen als het ServiceItem-IOC-document is gedefinieerd in het IOC-bestand dat voor de scan wordt gebruikt.
`/system=on|off`	Analyseer omgevingsgegevens tijdens het uitvoeren van de IOC-scan (SystemInfoItem-term). Als de waarde van het argument `off` is, analyseert Kaspersky Endpoint Security omgevingsgegevens niet. Als het IOC-bestand termen uit het SystemInfoItem-IOC-document bevat, worden deze genegeerd (aangemerkt als 'geen hit'). Als er geen argument wordt opgegeven, analyseert Kaspersky Endpoint Security omgevingsgegevens alleen als het SystemInfoItem-IOC-document is gedefinieerd in het IOC-bestand dat voor de scan wordt gebruikt.
`/users=on|off`	Analyseer gegevens over gebruikers tijdens het uitvoeren van de IOC-scan (UserItem-term). Als de waarde van het argument `off` is, analyseert Kaspersky Endpoint Security gegevens over gebruikers die zijn aangemaakt op het systeem niet. Als het IOC-bestand termen uit het UserItem-IOC-document bevat, worden deze genegeerd (aangemerkt als 'geen hit'). 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.
`/volumes=on|off`	Analyseer gegevens over volumes tijdens het uitvoeren van de IOC-scan (VolumeItem-term). Als de waarde van het argument `off` is, scant Kaspersky Endpoint Security de gegevens over volumes op het apparaat niet. Als het IOC-bestand termen uit het VolumeItem-IOC-document bevat, worden deze genegeerd (aangemerkt als 'geen hit'). Als er geen argument wordt opgegeven, analyseert Kaspersky Endpoint Security volumegegevens alleen als het VolumeItem-IOC-document is gedefinieerd in het IOC-bestand dat voor de scan wordt gebruikt.
`/eventlog=on|off`	Analyseer de gegevens over records in het Windows Event-logboek tijdens het uitvoeren van de IOC-scan (EventLogItem-term). Als de waarde van het argument `off` is, scant Kaspersky Endpoint Security de records in het Windows-gebeurtenislogboek niet. Als het IOC-bestand termen uit het EventLogItem-IOC-document bevat, worden deze genegeerd (aangemerkt als 'geen hit'). 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.
`/datetime=<event publication date>`	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. 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. 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. Als er geen argument wordt opgegeven, scant Kaspersky Endpoint Security gebeurtenissen zonder rekening te houden met de publicatiedatum. De `TaskSettings::BaseSettings::EventLogItem::datetime` instelling kan niet worden bewerkt. De instelling wordt alleen gebruikt als het EventLogItem-IOC-document is gedefinieerd in het IOC-bestand dat voor de scan wordt gebruikt.
`/channel=<list of channels>`	Lijst met (logboek)namen van kanalen waarvoor u een IOC-scan wilt uitvoeren. 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. 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 `<Channel></Channel>` -parameter in het xml-schema van de gebeurtenis). U kunt meerdere kanalen opgeven, gescheiden door spaties. Als er geen argument wordt opgegeven, scant Kaspersky Endpoint Security records op de kanalen `Application`, `System` en `Security`.

`/files=on|off`	Analyseer bestandsgegevens tijdens het uitvoeren van de IOC-scan (Fileltem-term). Als de waarde van het argument `off` is, analyseert Kaspersky Endpoint Security bestandsgegevens niet. Als het IOC-bestand termen uit het Fileltem-IOC-document bevat, worden deze genegeerd (aangemerkt als 'geen hit'). Als er geen argument wordt opgegeven, analyseert Kaspersky Endpoint Security bestandsgegevens alleen als het Fileltem-IOC-document is gedefinieerd in het IOC-bestand dat voor de scan wordt gebruikt.
`/drives=<all|system|critical|custom>`	Stel IOC-scanbereik in bij het analyseren van gegevens voor het Fileltem-IOC-document. U kunt de volgende waarden instellen voor het scanbereik: • `<all>` voor alle beschikbare bestandsbereiken. • `<system>` voor bestanden in mappen waarin het besturingssysteem is geïnstalleerd. • `<critical>` voor tijdelijke bestanden in gebruiker- en systeemmappen. • `<custom>` voor bestanden in bereiken die door de gebruiker zijn gedefinieerd (`/scope=<list of folders to scan>`). Als er geen argument wordt opgegeven, wordt de scan uitgevoerd voor kritieke gebieden.
`/excludes=<list of exclusions>`	Stel uitzonderingsbereik in bij het analyseren van gegevens voor het Fileltem-IOC-document. U kunt meerdere paden opgeven, gescheiden door spaties.
`/scope=<list of folders to scan>`	Door gebruiker gedefinieerd IOC-scanbereik bij het analyseren van gegevens voor het Fileltem IOC-document (`/drives=custom`). U kunt meerdere paden opgeven, gescheiden door spaties.
`/retro /<number of days>`	*Retrospectieve IOC-scan* is een modus van de *IOC Scan* taak waarbij Kaspersky Endpoint Security gedurende een bepaalde periode scant op indicatoren van besmetting met behulp van gegevens. Deze modus is bedoeld voor het zoeken naar indicatoren van besmetting door de telemetrie van de beschermde computer, zoals netwerkactiviteit, processen, bestanden en andere telemetriegegevens. U kunt een periode van 1 tot 14 dagen instellen. Het programma scant standaard één dag op indicatoren voor een besmetting.
`/network=on|off`	Analyse van netwerkgegevens (de NetworkItem termijn).
`/url=on|off`	Analyse van gegevens in browserlogboeken (de UrlHistoryItem termijn). De Retrospective IOC Scan analyseert logboeken van de volgende browsers: Google Chrome, Mozilla Firefox, Microsoft Edge (versie 79 of hoger).
`/email`	Analyse van e-mailobjecten (de EmailItem termijn).
`/route`	Analyse van routerings- en doorstuurtabellen (de RouteEntryItem termijn).

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="">`)
`Name`	Beschrijving van het IOC-bestand in de header van de IOC-bestandsstructuur (de tag `<description></description>`)
`Matched Indicator Items`	Lijst met ID's van alle indicatoren die een hit opleverden.
`Matched objects`	Gegevens van elk IOC-document waarvoor een hit werd gevonden.

MDRLICENSE. MDR-activering

Het BLOB-configuratiebestand toevoegen om Managed Detection and Response te activeren. Het BLOB-bestand bevat de client-ID en informatie over de licentie voor Kaspersky Managed Detection and Response. Het BLOB-bestand bevindt zich in het ZIP-archief van het MDR-configuratiebestand. U kunt het Ziparchief verkrijgen in de Kaspersky Managed Detection and Response-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. Managed Detection and Response instellingen in het beleid moeten ook beschikbaar zijn voor bewerking ().

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Syntaxis van opdracht

```
avp.com MDRLICENSE <operation> [/login=<user name> /password=<password>]
```

Bewerking	
`/ADD <file name>`	Pas het BLOB-configuratiebestand toe voor integratie met Kaspersky Managed Detection and Response (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=<user name> /password=<password>`	Gebruikersaccountgegevens met de vereiste machtigingen voor wachtwoordbeveiliging.

Voorbeeld

```
avp.com MDRLICENSE /ADD file.key
avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword
```

Voorbeeld

```
avp.com MDRLICENSE /ADD file.key
```

```
avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword
```

EDRKATA. Integratie met EDR (KATA)

Opdrachten voor het beheren van het onderdeel Endpoint Detection and Response (KATA):

- Het EDR (KATA)-onderdeel in- of uitschakelen.

  Het EDR-onderdeel (KATA) biedt interoperabiliteit met de Kaspersky Anti Targeted Attack Platform-oplossing.

- Configureer de verbinding met Kaspersky Anti Targeted Attack Platform-servers.
- De huidige instellingen van het onderdeel tonen.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Syntaxis van opdracht

```
avp.com START EDRKATA
```

```
avp.com STOP EDRKATA
```

```
avp.com edrkata /set /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=
<Central Node server connection timeout (s)>] [/sync-period=<Central Node server synchronization period (min)>]
```

```
avp.com edrkata /show
```

Bewerking	
`stop`	Schakel het EDR (KATA)-onderdeel uit.
`start`	Schakel het EDR (KATA)-onderdeel in.
`set`	Configureer het EDR (KATA)-onderdeel. U kunt de volgende instellingen configureren: • Voeg central node-servers (`servers=<server address>:<port>`) • Voeg een TLS-certificaat (`server-certificate=<path to the TLS certificate>`)toe • Stel de time-out in voor de verbinding van de Central Node-server (`/timeout=<Central Node server connection timeout (s)>`) • Stel de periode in voor synchronisatie met de Central Node-server (`/sync-period=<Central Node server synchronization period (min)>`)
`show`	Toon de huidige instellingen van het component.

KUMA. Integratie met KUMA

Opdrachten voor het beheer van de ingebouwde KUMA-agent:

- KUMA-integratie aan- of uitzetten.

  De ingebouwde KUMA-agent levert interoperabiliteit met de Kaspersky Unified Monitoring and Analysis Platform-oplossing.
- De verbinding met Kaspersky Unified Monitoring and Analysis Platform-servers instellen.
- De huidige instellingen van het onderdeel tonen.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Syntaxis van opdracht

```
avp.com START KUMA
```

```
avp.com STOP KUMA [/login=<user name> /password=<password>]
```

```
avp.com KUMA /SET /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=<KUMA server connection timeout (s)>] [/client-certificate=<path to the crypto-container>] [ /client-certificate-password=<password>] [/maximum-data-transfer-time=<maximum events transmission delay (sec)>]
```

```
avp.com KUMA /SHOW
```

Bewerking	
`stop`	KUMA-integratie uitschakelen.
`start`	KUMA-integratie inschakelen.
`set`	De ingebouwde KUMA-agent instellen. U kunt de volgende instellingen configureren: • Voeg KUMA-servers toe (`/servers=<protocol>://<server address>:<port>`) Het programma ondersteunt de volgende serververbindingsprotocollen: `tcp`, `udp`, `http`, `https`. • Voeg een TLS-certificaat (`/server-certificate=<path to the TLS certificate>`) toe • Stel de connectie-time-out (`/timeout=<KUMA server connection timeout (s)>`) voor de server in • Voeg een crypto-container toe (`/client-certificate=<path to the crypto-container> /client-certificate-password=<password>`) • De overdrachtsvertraging van evenementen configureren (`/maximum-data-transfer-time=<maximum events transmission delay (sec)`)
`show`	Toon de huidige instellingen van het component.

Authenticatie	
`/login=<user name> /password=<password>`	Gebruikersaccountgegevens met de vereiste machtigingen voor wachtwoordbeveiliging.

Voorbeeld

```
avp.com start kuma
```

```
avp.com KUMA /SET /servers=https://127.0.0.1:8080 /server-certificate=c:\\folder\\certificate.cer /timeout=15 /login=login /password=password
```

```
avp.com KUMA /SET /servers=https://kuma.server.com:8000 /server-certificate=c:\\folder\\certificate.cer /login=login /password=password
```

YARA. YARA-scan starten

De taak *Run YARA Scan*. Het programma scant bestanden en objecten op aanwijzingen voor gerichte aanvallen op de IT-infrastructuur van het bedrijf met behulp van databases met YARA-regels. *YARA-regels* zijn beschrijvingen van kenmerken van gerichte aanvallen en inbraken in de IT-infrastructuur van het bedrijf die Kaspersky Endpoint Security gebruikt om objecten te scannen.

Als u een YARA-scan wilt uitvoeren, moet u YARA-bestanden voorbereiden die regels beschrijven. Houd bij het maken van YARA-bestanden rekening met de volgende vereisten:

- Kaspersky Endpoint Security ondersteunt YARA-bestanden met de extensies .YARA en .YAR die voldoen aan de open YARA 4.2.3-standaard voor het beschrijven van indicatoren van compromis.
- Alleen bestanden met YARA-regels kan voor de taak worden opgegeven. De *YARA-scan uitvoeren* taak ondersteunt geen andere soorten regels.
- Als u YARA-bestanden hebt toegevoegd die Kaspersky Endpoint Security niet ondersteunt, of als de regels syntaxisfouten bevatten, wordt de taak afgebroken met het bijbehorende foutbericht.
- De ID's van alle IOC files gebruikt in een enkele taak moeten uniek zijn. Als er YARA-bestanden zijn met dezelfde ID, kan dit van invloed zijn op de resultaten van de taakuitvoering.
- Een YARA-scan wordt afgebroken na 128 overeenkomsten met indicatoren die worden beschreven in de YARA-regels. Dit is nodig om het aantal items in het YARA-scanrapport te beperken om de analyse ervan te vergemakkelijken en om te voorkomen dat het rapport overloopt vanwege onnauwkeurig geformuleerde YARA-regels die een groot aantal overeenkomsten kunnen genereren.

Kaspersky raadt aan om één regel per YARA-bestand aan te maken. Hierdoor zijn de scanresultaten beter leesbaar.

Een YARA-scan kan behoorlijk wat tijd in beslag nemen. Afhankelijk van de grootte van de schijf, de taakinstellingen en het aantal objecten op de schijf, kan een YARA-scan enkele minuten tot enkele uren duren. Het programma toont geen voortgangsindicator. Het is niet mogelijk om een YARA-scan te stoppen of te annuleren. U wordt geadviseerd te wachten tot de resultaten van een YARA-scan beschikbaar zijn.

Syntaxis van opdracht

```
avp.com YARA <full path to the YARA file>|/path=<path to the folder with YARA files> [<advanced settings>]
```

YARA-bestanden	
`<full path to the YARA file>`	Volledig pad naar het YARA-bestand dat u wilt gebruiken voor het scannen. U kunt paden naar meerdere YARA-bestanden opgeven, gescheiden door spaties. Vereist argument als de `/path=<path to the folder with YARA files>` waarde is niet opgegeven. Voorbeeld: `C:\Users\Admin\Desktop\YARA\file1.yar C:\Users\Admin\Desktop\YARA\file2.yar`
`/path=<path to the folder with YARA files>`	Volledige pad naar een map met YARA-bestanden die u wilt gebruiken voor de scan. Vereist argument als de `<full path to the YARA file>` waarde is niet opgegeven. Voorbeeld: `/path=C:\Users\Admin\Desktop\YARA`

Geavanceerde instellingen	
`/fastScan=<on|off>`	Snelle YARA-scan. Voor elk object registreert het programma één exemplaar van de gedetecteerde indicator. Het programma verbergt ook duplicaten van gedetecteerde indicatoren in het logboek. Met Snelle YARA-scan kunt u grote bestanden sneller scannen. Als deze instelling niet wordt opgegeven, voert het programma een standaard YARA-scan uit. In deze modus registreert het programma duplicaten van gedetecteerde indicatoren.
`/maxRules=<maximum number of scan rules>`	Limiet voor het aantal unieke geactiveerde regels waarbij het programma de YARA-scan stopt zodra dit aantal wordt bereikt. Als de waarde van deze instelling niet is opgegeven of als `0` is opgegeven, voert het programma de YARA-scan zonder beperkingen uit.
`/timeOut=<stop scan after the specified time in seconds>`	Hoelang een YARA-scan kan duren, in seconden. Wanneer deze tijd om is, stopt het programma de YARA-scan. Als de waarde van deze instelling niet is opgegeven of als `0` is opgegeven, voert het programma de YARA-scan zonder beperkingen uit.
`/recursive=<on|off>`	Dit argument start een recursieve scan van submappen in de `/scanFolders` Aangepaste Scan.
`/scanFolders=<list of folders to be scanned>`	Dit argument start een YARA-scan van bestanden in de opgegeven lijst met mappen. U kunt meerdere waarden opgeven, gescheiden door spaties. Kaspersky Endpoint Security biedt geen ondersteuning voor de tekens `*` en `?` bij het invoeren van een padmasker. Als deze instelling niet is opgegeven, voert het programma een YARA-scan uit op alle lokale schijven, behalve gedeelde netwerkschijven, cloudstations en verwisselbare media.
`/scanMemory=<on|off>`	Scan het geheugen van alle actieve processen.
`/scanProcess=<process name>`	Alleen geheugen scannen voor opgegeven processen. Geef door spaties gescheiden volledige paden op naar uitvoerbare bestanden van processen. U kunt ook `*` en `?` tekens om een masker in te voeren.
`/maxSize=<file size in bytes>`	Beperk de bestandsgrootte voor de YARA-scan. Het programma slaat grotere bestanden over.
`/includes=<list of objects to be scanned>>`	Scanbereik bewerken. U kunt meerdere waarden opgeven, gescheiden door spaties. De volgende waarden zijn beschikbaar: • Bestandsnaam • Bestandsextensie Scanbereik moet worden opgegeven met de `/scanFolders` parameter. Voorbeeld: `/scanFolders C:\*.* /includes=*.exe *.dll` – het programma scant alle bestanden met de extensie .EXE en .DLL op schijf C.
`/excludes=<list of objects to be scanned>`	Bestanden uitsluiten van de YARA-scan. U kunt meerdere waarden opgeven, gescheiden door spaties. De volgende waarden zijn beschikbaar: • Het bestandspad • Masker van het bestandspad Uitzonderingen moeten worden opgegeven met de `/scanFolders` parameter. Voorbeeld: `/scanFolders C:\*.* /excludes readme.txt C:\trusted\*.* *.xml` – het programma slaat de readme.txt bestand over, alle bestanden van de C:\trusted map en alle bestanden met de extensie xml in de hoofdmap op schijf C.
`/scanAutoruns=<on|off>`	YARA scant automatisch gestarte puntobjecten.
`/excludeAutoruns=<list of autorun point areas to skip>`	Automatisch uitgevoerde puntobjecten worden uitgesloten van het scanbereik. Geef door spaties gescheiden volledige paden op naar uitvoerbare bestanden van processen. U kunt ook `*` en `?` tekens om een masker in te voeren.
`/logFolder=<path to the folder for saving the scan results in a TXT file>`	Als u een pad naar een map opgeeft, slaat het programma de scanresultaten op het opgegeven pad op in een bestand met de naam yara_<computer name> _<scan completion time> .txt. Als u een pad naar een specifiek TXT-bestand opgeeft, slaat het programma de scanresultaten in dat bestand op. Bijvoorbeeld: `/logFolder=C:\test` of `/logFolder=C:\test\abc.txt`. Scanresultaten worden naar de opdrachtregel uitgevoerd, ongeacht of de `/logFolder` optie is opgegeven.

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.
- `5` betekent dat een of meer bestanden met de opgegeven YARA-regels in de parameter niet zijn gevonden.

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:

`Started at <time>` `Finished at <time>`	Begintijd en voltooiingstijd van een scan.
`Host name: <computer name>`	De naam van de computer waarop het object is gedetecteerd.
`Result: <error>`	Foutcode voor de fout die is opgetreden tijdens het uitvoeren van de taak. Als er geen fouten zijn, voert het programma uit `0x00000000`.
`Comment: <comment text>`	Foutbeschrijving voor de fout die is opgetreden tijdens het uitvoeren van de taak. Bijvoorbeeld `Operation timeout`.
`Object Name:` of `Process:` (tijdens het scannen van het procesgeheugen)	De naam van het object of proces waarvoor de YARA-regel is geactiveerd.
`Md5: <md5 hash>` `Sha256: <sha256 hash>`	Hashes van het object waarvoor de YARA-regel is geactiveerd.
`Rule Name`	De naam van de geactiveerde YARA-regel.

`Meta:`
`Author: <author>`
`Date: <date>`
`Description: <description>`
	Metagegevens opgegeven in de YARA-regel.

`Detects:`
`Offset : String name : String data`
`<offset> : <string name> : <string data>`
	Gevonden overeenkomsten binnen het object die voldoen aan de voorwaarden van de YARA-regel:
	• Offset in het procesgeheugen of bestand waar een overeenkomst is gevonden (`Offset`).
	• De naam van de overeenkomende tekenreeks in de YARA-regel (`String name`).
	• De overeenkomende tekenreeks in het procesgeheugen of bestand (`String data`).

TELEMETRIEFILTERS. Gebeurtenissen filteren die naar KUMA moeten worden verzonden

Standaard is het verzenden van gebeurtenissen naar de KUMA-server uitgeschakeld. Om ervoor te zorgen dat KUMA correct werkt, moet u de verzending van telemetrie inschakelen. U kunt een gebeurtenisbron selecteren uit de standaardlogboeken: *Application*, *Security* or *System*. Om de prestaties te verbeteren en de gegevensoverdracht naar de KUMA-server te optimaliseren, kunt u handmatig afzonderlijke gebeurtenissen toevoegen aan of uitsluiten van telemetrie. U kunt bijvoorbeeld Sysmon-gebeurtenissen uitsluiten.

U kunt de lijst met uitzonderingen vanuit de opdrachtregel exporteren naar een JSON-bestand.

Als de opdracht alleen de naam bevat van het bestand waarnaar u de instellingen wilt exporteren, plaatst het programma het bestand als volgt:

- Als het pad naar avp.com wordt toegevoegd aan de systeemvariabele %PATH%, plaatst het programma het bestand in de map `C:\Windows\SysWOW64`.

- Als u de opdracht uitvoert vanuit de installatiemap van het programma, mislukt het exporteren omdat de zelfbescherming van het programma het maken van een nieuw bestand in de programmamap blokkeert. Om programma-instellingen naar een bestand te exporteren, voer het bestandspad in.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Syntaxis van opdracht

```
avp.com TELEMETRYFILTERS /export <file name>
```

```
avp.com TELEMETRYFILTERS /import <file name>
```

Bewerking	
`export`	Gebeurtenisfilters exporteren om te versturen naar KUMA.
`import`	Gebeurtenisfilters importeren om te versturen naar KUMA. Als er al regels voor het filteren van gebeurtenissen op de computer bestaan, vervangt Kaspersky Endpoint Security deze tijdens het importeren.

Bestand voor export of import	
`<file name>`	Naam van het bestand met gebeurtenisfilters dat naar KUMA moet worden verstuurt. U kunt ook het bestandspad invoeren. U kunt filters voor versturing naar KUMA exporteren naar een JSON-bestand.

Opdrachten voor beheer van Light Agent

U kunt het programma beheren in Light Agent modus om virtuele omgevingen op de opdrachtregel te beschermen. U kunt het programma beheren in de Light Agent-modus als beheer via 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 <command>`.

Om het programma in de Light Agent-modus te beheren 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. Gebruik het volgende sjabloon om het commando uit te voeren:

   ```
   avp.com <command> [options]
   ```

   Kaspersky Endpoint Security zal nu de opdracht uitvoeren.

Het programma die in de Light Agent-modus is geïnstalleerd, ondersteunt bijna alle AVP-opdrachten van het programma die in de Standaardmodus is geïnstalleerd. In de Light Agent-modus zijn de taken voor het bijwerken van de antivirusdatabase en het beheren van licentiesleutels beperkt.

KSVLAINFO. De Light Agent-modus bepalen

De Light Agent-modus bepalen.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Syntaxis van opdracht

```
avp.com KSVLAINFO
```

De opdracht stuurt de volgende informatie naar de console:

- Light Agent-modus voor het beschermen van virtuele omgevingen: ingeschakeld of uitgeschakeld.

  Als de Light Agent-modus is ingeschakeld, wordt het programma gebruikt als onderdeel van de Kaspersky Security for Virtualization Light Agent-oplossing.

- VDI-beschermingsmodus: ingeschakeld of uitgeschakeld.

  De VDI-beschermingsmodus helpt de prestaties van Kaspersky Endpoint Security op niet-permanente virtuele machines te optimaliseren. Als de VDI-beschermingsmodus is ingeschakeld, worden updates waarvoor de beschermde virtuele machine opnieuw moet worden opgestart, niet geïnstalleerd op niet-permanente virtuele machines. Bij het ontvangen van updates waarvoor opnieuw opstarten vereist is, stuurt Light Agent die op een niet-permanente virtuele machine is geïnstalleerd, een bericht naar Kaspersky Security Center met de melding dat de beveiligde sjabloon voor de virtuele machine moet worden bijgewerkt.

- Type van de beveiligde virtuele machine: persistent of niet-persistent.

- Rol van de beveiligde virtuele machine in de virtuele infrastructuur: server of werkstation.

- Identificatie: UUID.

VIISINFO. Status van de Light Agent-verbinding met de Integrationserver

Informatie bekijken over de Light Agent-verbinding met de Integratieserver.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Syntaxis van opdracht

```
avp.com VIISINFO
```

De opdracht stuurt de volgende informatie naar de console:

- Adres en poort van de Integratieserver waarmee de Light Agent is verbonden.
- Integratieserver verbindingsstatus.
- Datum en tijd van de laatste verbinding van de Light Agent met de Integratieserver.

SVMINFO. Status van de Light Agent-verbinding met de Protection Server

Informatie bekijken over de Light Agent-verbinding met de Protection Server.

Om een opdracht uit te voeren, ga naar de map waar het uitvoerbare bestand van Kaspersky Endpoint Security is opgeslagen. U kunt ook het uitvoerbare bestandspad toevoegen aan de systeemvariabele %PATH% en de opdracht uitvoeren zonder naar de programmamap te navigeren.

Syntaxis van opdracht

```
avp.com SVMINFO
```

De opdracht stuurt de volgende informatie naar de console:

- Adres van de SVM waarmee de Light Agent is verbonden en de locatie van de SVM in de virtuele infrastructuur ten opzichte van de Light Agent: lokaal of niet-lokaal.
- SVM-detectiemethode die de Light Agent gebruikt: met behulp van een Integratieserver of met behulp van een aangepaste lijst met SVM-adressen.
- Lijst met SVM-adressen als de SVM-adreslijst is geselecteerd als de SVM-detectiemethode.
- Tag voor het verbinden van Light Agent met SVM.
- SVM-selectiealgoritme: standaard of uitgebreid. Als het uitgebreide SVM-selectiealgoritme wordt gebruikt, wordt ook het SVM-padtype in de virtuele infrastructuur weergegeven.
- Beschermingsstatus van de verbinding tussen de Light Agent en de Protection Server.

Foutcodes

Er kunnen fouten optreden wanneer u het programma met de opdrachtregel gebruikt. Wanneer er fouten optreden, toont Kaspersky Endpoint Security een foutbericht zoals `Error: Cannot start task 'EntAppControl'`. Kaspersky Endpoint Security kan ook aanvullende informatie tonen in de vorm van een code, zoals `error=8947906D` (zie onderstaande tabel).

Foutcodes

Foutcode	Beschrijving
`09479001`	Deze sleutel wordt al gebruikt
`0947901D`	Licentie verlopen. Database-updates zijn niet beschikbaar

Foutcode	Beschrijving
89479002	Sleutel niet gevonden
89479003	Digitale handtekening ontbreekt of is beschadigd
89479004	Gegevens zijn beschadigd
89479005	Sleutelbestand is beschadigd
89479006	Licentie is verlopen
89479007	Sleutelbestand is niet opgegeven
89479008	Ongeldig sleutelbestand
89479009	Gegevens opslaan is mislukt
8947900A	Gegevens lezen 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 sleutelbestand gebruiken om een reservesleutel 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 sleutel voor proeflicentie niet gebruiken als sleutel voor commerciële licentie
89479016	De bètalicentie is vereist om de bètaversie van de app te gebruiken
89479017	Het sleutelbestand is niet compatibel met dit programma. Kaspersky Endpoint Security voor Windows kan niet worden geactiveerd met een licentiebestand voor een ander programma. Controleer het geïnstalleerde programma
89479018	Licentiesleutel is geblokkeerd door Kaspersky
89479019	Het programma is al gebruikt met een proeflicentie. Er kan geen nieuwe sleutel voor een proeflicentie worden toegevoegd
8947901A	Sleutelbestand is beschadigd
8947901B	Digitale handtekening ontbreekt, is beschadigd of stemt niet overeen met de digitale handtekening van Kaspersky
8947901C	Sleutel kan niet worden toegevoegd als de bijbehorende niet-commerciële licentie is verlopen
8947901E	De datum waarop het sleutelbestand is gemaakt of gebruikt, is ongeldig. Controleer de systeemdatum
8947901F	Kan geen sleutel voor proeflicentie toevoegen: er is al een andere sleutel voor een proeflicentie actief
89479020	Denylist van licenties is beschadigd of ontbreekt
89479021	Updatebeschrijving ontbreekt of is beschadigd
89479022	Sleutel is niet geschikt voor dit programma
89479023	Kan geen ongeldig sleutelbestand gebruiken om een reservesleutel toe te voegen
89479025	Fout bij verzending van verzoek naar activatieserver. Mogelijke redenen: fout bij internetverbinding of tijdelijke problemen met de activatieserver. Activeer het programma later (over 1 tot 2 uur) met de activatiecode. Als deze fout aanhoudt, neem je contact op met de internetprovider
89479026	Verzoek bevat onjuiste activatiecode
89479027	Reactiestatus kan niet worden verkregen
89479028	Fout bij opslaan van tijdelijk bestand
89479029	Er is een onjuiste activatiecode ingevoerd of een ongeldige systeemdatum op de computer ingesteld. Controleer de systeemdatum op de computer
8947902A	Sleutel niet compatibel met dit programma of licentie verlopen

Foutcode	Beschrijving
8947902B	Ontvangst van sleutelbestand is mislukt. Er is een onjuiste activatiecode ingevoerd
8947902C	Activatieserver gaf fout 400
8947902D	Activatieserver gaf fout 401
8947902E	Activatieserver gaf fout 403
8947902F	Noodzakelijke resource is niet beschikbaar op de activatieserver. Activatieserver gaf fout 404. Controleer de instellingen van je internetverbinding
89479030	Activatieserver gaf fout 405
89479031	Activatieserver gaf fout 406
89479032	Proxyverificatie is vereist. Controleer de netwerkinstellingen
89479033	Time-out bij verzoek
89479034	Activatieserver gaf fout 409
89479035	Noodzakelijke resource is niet beschikbaar op de activatieserver. Activatieserver gaf fout 410. Controleer de instellingen van je internetverbinding
89479036	Activatieserver gaf fout 411
89479037	Activatieserver gaf fout 412
89479038	Activatieserver gaf fout 413
89479039	Activatieserver gaf fout 414
8947903A	Activatieserver gaf fout 415
8947903C	Interne serverfout
8947903D	Functionaliteit wordt niet ondersteund
8947903E	Ongeldige gatewayreactie. Controleer je netwerkinstellingen
8947903F	Bron tijdelijk niet beschikbaar
89479040	Gatewayreactie vertoonde time-out. Controleer je netwerkinstellingen
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 geheugentoewijzing
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	Sleutelbestand is niet gevonden op activatieserver
8947904E	Sleutel is geblokkeerd
8947904F	Interne fout bij activatieserver
89479050	Onvoldoende gegevens in activatieverzoek
89479053	De licentie die hoort bij de toegevoegde sleutel is al verlopen
89479054	Er is een ongeldige systeemdatum ingesteld op de computer. Controleer de systeemdatum
89479055	Proeflicentie is verlopen
89479056	Periode voor programma-activiteit is verlopen

Foutcode	Beschrijving
89479057	Het maximale aantal programma-activaties is voor de opgegeven code overschreden
89479058	Activeringsprocedure voltooid met systeemfout
89479059	Kan sleutel voor proeflicentie niet gebruiken als sleutel voor commerciële licentie
8947905C	Activatiecode is vereist
89479062	Geen verbinding met activatieserver mogelijk
89479064	Activatieserver is niet beschikbaar. Controleer de instellingen van de internetverbinding en probeer het opnieuw
89479065	Licentie is verlopen
89479066	Actieve sleutel kan niet door een verlopen sleutel worden vervangen
89479067	Reservesleutel kan niet worden toegevoegd als de bijbehorende licentie vóór de huidige licentie verloopt
89479068	Geüpdatete abonnementsleutel ontbreekt
8947906A	Ongeldige activatiecode
8947906B	Sleutel is al actief
8947906C	Licentietypen die horen bij actieve en reservesleutels komen niet overeen
8947906D	Onderdeel niet ondersteund door licentie
8947906E	Abonnementsleutel kan niet als reservesleutel worden toegevoegd
89479213	Algemene fout bij transportlaag
89479214	Kon geen verbinding maken met activatieserver
89479215	Ongeldige structuur van webadres
89479216	Conversie van proxyserveradres is mislukt
89479217	Conversie van serveradres is mislukt. Controleer de instellingen van de internetverbinding
89479218	Poging tot verbinding met server is mislukt
89479219	Toegang op afstand geweigerd
8947921A	Time-out bij bewerking
8947921B	Fout bij verzending van HTTP-aanvraag
8947921C	SSL-verbindingsfout
8947921D	Bewerking onderbroken door callback
8947921E	Te veel omleidingen
8947921F	Controle van ontvanger is mislukt
89479220	Lege reactie van server
89479221	Fout bij verzending van gegevens
89479222	Fout bij ontvangst van gegevens
89479223	Probleem met SSL-certificaat
89479224	Probleem met SSL-encryptie
89479225	Probleem met SSL-certificeringscentrum
89479226	Ongeldige inhoud van netwerkpakket
89479227	Toegang tot account geweigerd
89479228	Ongeldig SSL-certificaatbestand
89479229	Kan SSL-verbinding niet verbreken
8947922A	Terugkerende fout
8947922B	Ongeldig bestand met ingetrokken certificaten

Foutcode	Beschrijving
8947922C	Fout bij SSL-certificaataanvraag
89479401	Onbekende serverfout
89479402	Interne serverfout
89479403	Geen sleutel beschikbaar voor de ingevoerde activatiecode
89479404	Actieve sleutel geblokkeerd
89479405	Vereiste parameters van activatieverzoek ontbreken
89479406	Ongeldig klantnummer of wachtwoord
89479407	Ongeldige activatiecode
89479408	De activatiecode is niet compatibel met dit programma. Kaspersky Endpoint Security for Windows kan niet worden geactiveerd met een activatiecode voor een ander programma. Controleer het geïnstalleerde programma
89479409	Activatiecode is vereist
8947940B	Activatieperiode verstreken
8947940C	Het aantal activaties met deze code is overschreden
8947940D	Ongeldige structuur van verzoeknummer
8947940E	Activatiecode al in gebruik
8947940F	Verlenging van activatiecode is mislukt
89479410	Activatiecode is ongeldig in deze regio
89479411	Deze activatiecode kan niet worden gebruikt voor deze taalversie van het programma
89479412	De activatiecode is bedoeld voor de nieuwe versie van dit programma. Koop een andere activatiecode om de geïnstalleerde versie van het programma te activeren
89479413	Activatieserver geeft fout 643
89479414	Activatieserver geeft fout 644
89479415	Activatieserver geeft fout 645
89479416	Activatieserver geeft fout 646
89479417	Versie 1.0 van de activatieserver is vereist
89479418	Onjuiste structuur van activatiecode
89479419	Tijd op computer komt niet overeen met tijd op activatieserver
8947941A	Verkeerde programmaversie
8947941B	Abonnement is verlopen
8947941C	Aantal activaties overschreden
8947941D	Ongeldige handtekening van ticket
8947941E	Er zijn aanvullende gegevens nodig
8947941F	Verificatie van gegevens is mislukt
89479420	Abonnement is inactief
89479421	Activatieserver ondergaat onderhoud
89479501	Onverwachte fout
89479502	Ongeldige parameter overgezet. Bijvoorbeeld: een lege lijst met adressen van activatieservers
89479503	Ongeldige activatiecode (ongeldige hash)
89479504	Ongeldig gebruikers-ID
89479505	Ongeldig gebruikerswachtwoord
89479506	Ongeldige reactie van activatieserver

Foutcode	Beschrijving
89479507	Activatieverzoek is onderbroken
89479509	Activatieserver 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`, en `EXPORT` 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
- `AntiCryptor`
- `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
- `LogInspector` – Log Inspectie
- `Mail_Monitoring` of `EM` – Mail Threat Protection
- `Rollback` – Update rollback (het profiel kan niet worden toegepast als het programma is geïnstalleerd in Light Agent-modus)
- `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` – Bijwerken (het profiel kan niet worden toegepast als het programma is geïnstalleerd in Light Agent-modus)
- `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 `<DOMAIN>\<UserName>` in (bijvoorbeeld, `RESTAPI_User=COMPANY\Administrator`). 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=<port>`

     Poort die wordt gebruikt voor het beheer van het programma via de REST API. Poort 6782 wordt standaard gebruikt. Zorg ervoor dat de poort vrij is. Optionele parameter.
   - `RESTAPI_Certificate=<path to certificate>`

     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\RestAp`

     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_kes.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 verwijdert of de instellingen *Serviceregel voor REST API* niet verandert. 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 beheren wilt beheren via de REST API, 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 beheren:

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

In deze sectie worden de informatiebronnen over het programma beschreven.

U kunt de meest geschikte informatiebron kiezen, afhankelijk van het belang en de urgentie van uw probleem.

Kaspersky Endpoint Security-pagina op de Kaspersky-website

Op de Kaspersky Endpoint Security-pagina, kunt u algemene informatie bekijken over het programma en de functies en eigenschappen ervan.

De Kaspersky Endpoint Security-pagina bevat een link naar de online winkel. Daar kunt u het programma kopen of verlengen.

Kaspersky Endpoint Security-pagina in de Knowledge Base

Knowledge Base is een sectie op de website voor Technische Support.

Op de Kaspersky Endpoint Security-pagina in de Knowledge Base, kunt u artikelen lezen met nuttige informatie, aanbevelingen en antwoorden op veelgestelde vragen over het aanschaffen, installeren en gebruiken van het programma.

Knowledge Base-artikelen kunnen vragen beantwoorden die niet alleen betrekking hebben op Kaspersky Endpoint Security, maar ook op andere Kaspersky-programma's. Artikelen in de Knowledge Base kunnen ook nieuws van de Technische Support bevatten.

Bespreking van Kaspersky-programma's in het Forum

Als uw vraag niet dringend is, kunt u het onderwerp bespreken met Kaspersky-experts en andere gebruikers in ons Forum.

In het forum kunt u bestaande onderwerpen bekijken, uw eigen opmerkingen plaatsen en nieuwe discussieonderwerpen maken.

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 tracen 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.14.1\Traces`.

Tracebestanden krijgen de volgende naam: `KES<14.1_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.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.

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 traceerbestanden 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 verbindingsmodule van Kaspersky Security Center voordoen.

Inhoud van bestanden met prestatietraces

Bestanden met tracebestanden krijgen de volgende naam:
`KES<14.1_dateXX.XX_timeXX.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 `shellex.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 of trace file>.DESKTOP-<date of file update>.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 System Volume Information 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 acties die door het programma zijn uitgevoerd en van berichten over gebeurtenissen tijdens de werking van het programma. Tijdens het traceringsproces maakt het programma een set bestanden met gegevens over de werking van verschillende programmacomponenten (bijvoorbeeld SRV.log, WD.log en andere).

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 omvangsbeperking**. Sla traces op als een beperkt aantal bestandensets met een beperkte grootte en overschrijf de oudere bestanden wanneer de maximale grootte wordt bereikt. Als deze modus is geselecteerd, kunt u het maximale aantal bestandensets voor rotatie en de maximale grootte voor elk set bestanden definiëren.

     Standaard slaat het programma vijf sets traceerbestanden op. De grootte van elke set bestanden is 3072 MB. Op deze manier heeft u 15 GB vrije schijfruimte nodig om de traceerbestanden op te slaan.
   - **Zonder beperkingen**. Sla één tracebestand op (geen maximale grootte).

5. Selecteer in de vervolgkeuzelijst **Niveau** het tracingniveau:

   - **Normaal** betekent dat het tracebestand berichten over alle fouten, waarschuwingen en informatie over de normale werking van het programma opslaat (standaard).
   - **Gedetailleerd** betekent dat het tracebestand alle informatie over de werking van het programma opslaat.

   Extra traceringsniveaus zijn beschikbaar als u de instellingen voor de tracering van programma's beheert op de opdrachtregel. 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**.

   > Als programmatracing was ingeschakeld op de opdrachtregel en een ander traceringsniveau is ingesteld dan **Normaal** of **Gedetailleerd**, de **Niveau** vervolgkeuzelijst is ingesteld op **Normaal**.

6. Om het traceringsproces te stoppen, keer terug naar het venster **Tools voor ondersteuning** en schakel tracering uit.

> U kunt ook tracebestanden maken wanneer u het programma vanaf de opdrachtregel installeert, inclusief met het bestand setup.ini.

Hierdoor worden tracebestanden gemaakt van de programmawerking in de map `%ProgramData%\Kaspersky Lab\KES.14.1\Traces`. Nadat het tracebestanden zijn aangemaakt, verstuur de bestandem 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 omvangsbeperking**. 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.

   - **Zonder beperkingen**. 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 tracering uit.

   Hierdoor wordt een prestatietracebestand in de map `%ProgramData%\Kaspersky Lab\KES.14.1\Traces` gemaakt. Nadat het tracebestand is aangemaakt, verstuurt 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.14.1\Traces`.

Dump schrijven inschakelen via de Beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Algemene instellingen** → **Programma-instellingen** in het beleidsvenster.
4. In het blok **Foutopsporingsgegevens**, klikt u op de knop **Instellingen**.
5. In het geopende venster gebruik het selectievakje **Schrijven naar dump inschakelen** om het schrijven van programma-dump in of uit te schakelen.
6. Sla uw wijzigingen op.

Dump schrijven inschakelen via de Webconsole en Cloudconsole

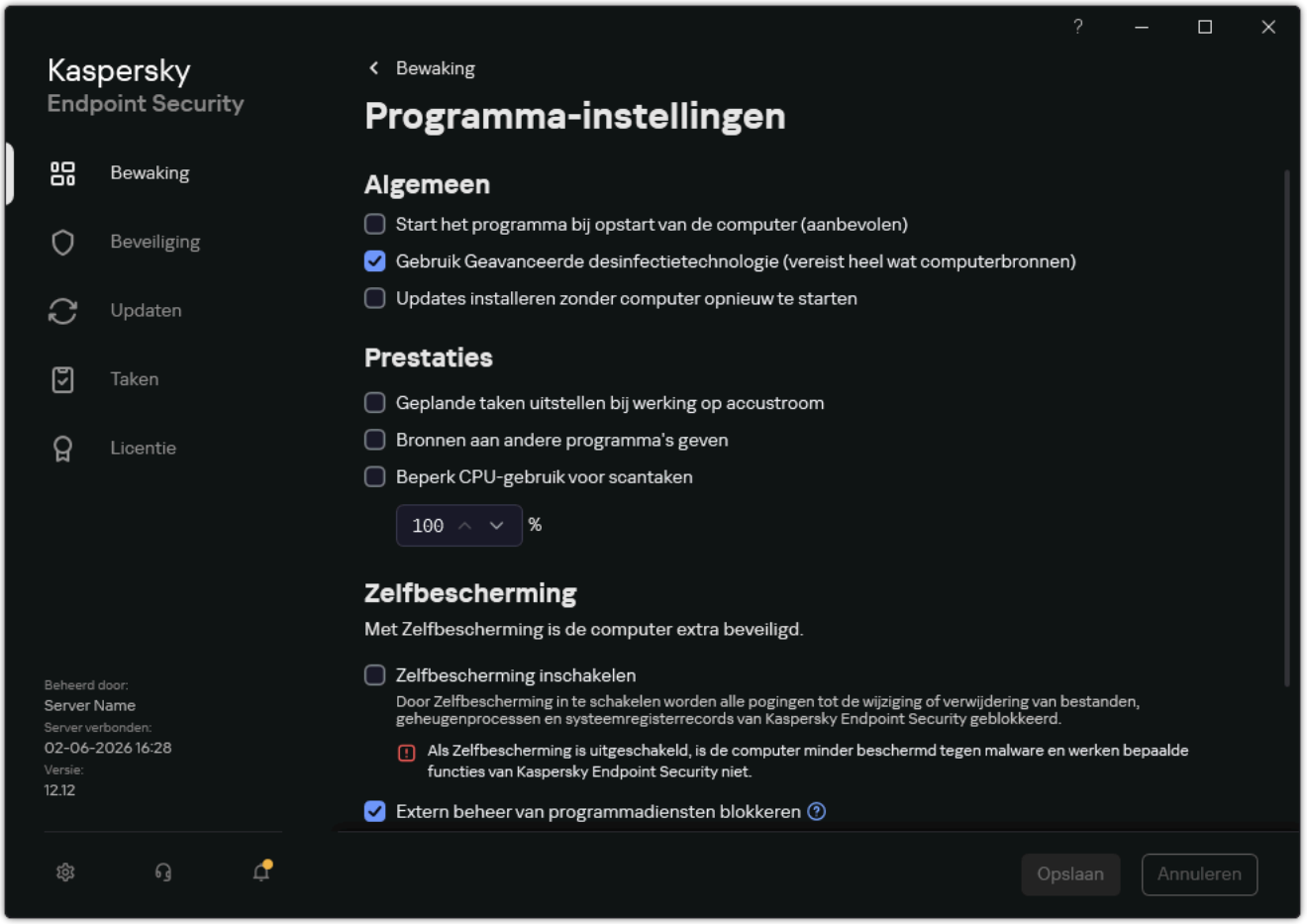
1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
2. Klik op de naam van het Kaspersky Endpoint Security-beleid.

   U ziet nu het venster met de beleidseigenschappen.
3. Selecteer het tabblad **Application settings**.
4. Ga naar **General Settings** → **Technical Support**.
5. Gebruik in het blok **Debug information** het selectievakje **Dump writing ENABLED** om het schrijven van programma-dump in of uit te schakelen.
6. Sla uw wijzigingen op.

Dump schrijven inschakelen via 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.



Instellingen Kaspersky Endpoint Security voor Windows

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.

Beveiliging van dumpbestanden en traceerbestanden inschakelen in de beheerconsole (MMC)

1. Selecteer **Policies** in de structuur van de Beheerconsole van Kaspersky Security Center.
2. Selecteer het noodzakelijke beleid en dubbelklik om de beleidseigenschappen te openen.
3. Selecteer **Algemene instellingen** → **Programma-instellingen** in het beleidsvenster.
4. In het blok **Foutopsporingsgegevens**, klikt u op de knop **Instellingen**.
5. In het geopende venster gebruik het selectievakje **Bescherming voor dump- en tracebestanden inschakelen** om de bestandsbeveiliging in- of uit te schakelen.
6. Sla uw wijzigingen op.

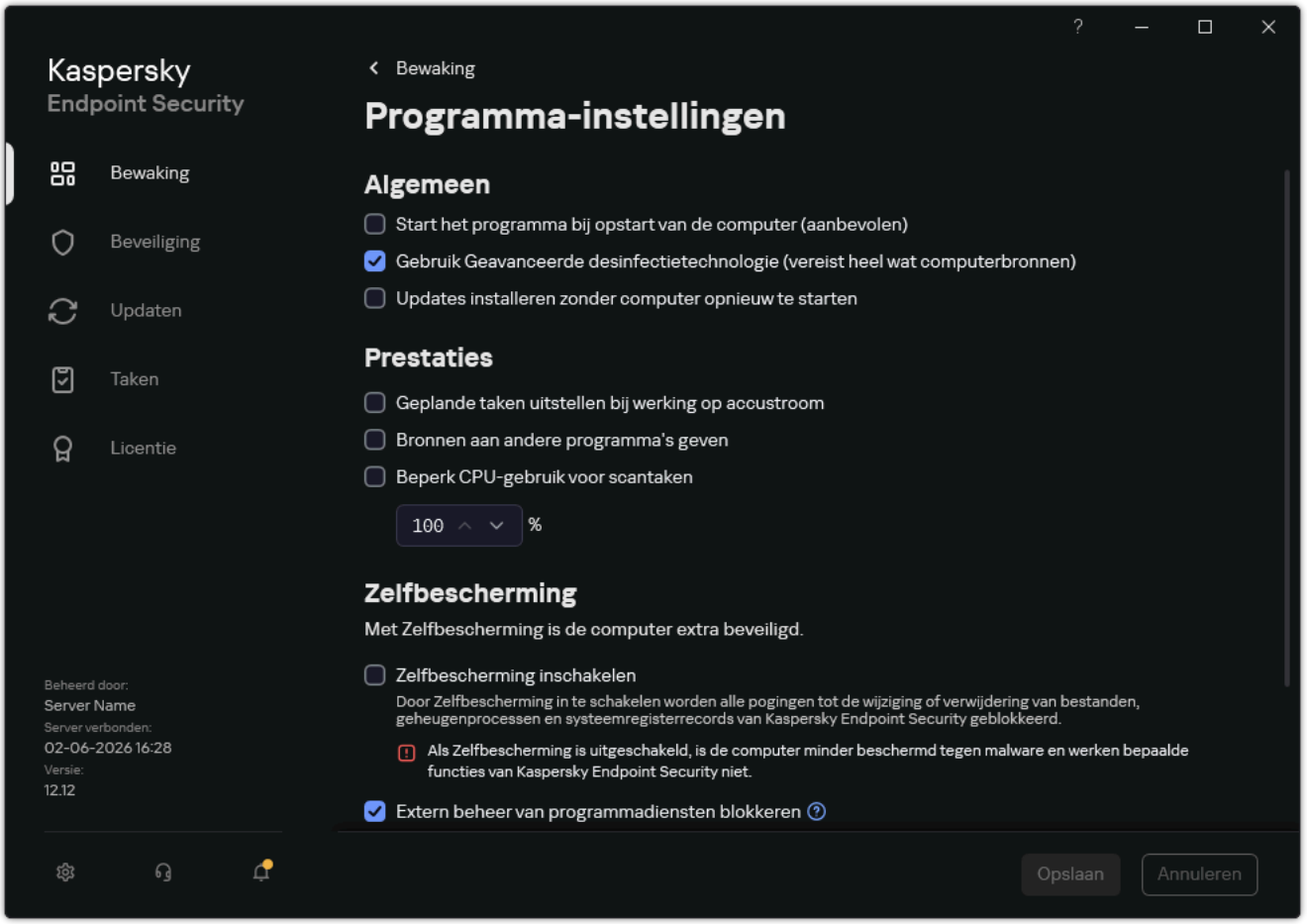
Beveiliging van dumpbestanden en traceerbestanden inschakelen in Webconsole en Cloudconsole

1. Selecteer in het hoofdvenster van de webconsole achtereenvolgens **Asset management** → **Policies**.
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** → **Technical Support**.
5. Gebruik in het blok **Debug information** het selectievakje **Dump and trace files protection ENABLED** om bestandsbeveiliging in of uit te schakelen.
6. Sla uw wijzigingen op.

Beveiliging van dumpbestanden en traceerbestanden inschakelen 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.



Instellingen Kaspersky Endpoint Security voor Windows

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.

Gegevens van het besturingssysteem verkrijgen (Kaspersky Get System Info)

Nadat het Kaspersky Endpoint Security programma is geïnstalleerd, werkt het besturingssysteem of een programma mogelijk niet correct. Er is een conflict tussen het programma en de software of stuurprogramma's van de computeronderdelen.

Om de oorzaak van het probleem te achterhalen, heeft de Technische Support van Kaspersky een rapport van het hulpprogramma Kaspersky Get System Info (hierna GSI genoemd) nodig. Raadpleeg de Kaspersky Knowledge Base voor gedetailleerde informatie over het gebruik van het hulpprogramma.

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.
- Bij het verwijderen van individuele programmaonderdelen (bijvoorbeeld de taak *Programmaonderdelen wijzigen* gebruiken), kan het opnieuw opstarten van de computer vereist zijn.
- In de eigenschappen van de taak *Programmaonderdelen wijzigen*, bij het wisselen van de installatiemodus (**Aparte modus** / **Gecombineerde modus**), wordt synchronisatie van de set onderdelen tussen modi niet ondersteund. Het programma synchroniseert de set onderdelen tussen modi nadat u de taakeigenschappen opnieuw opent.
- 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 Kaspersky Endpoint Security hebt geannuleerd, start het herstel van het programma nadat u de computer opnieuw hebt opgestart.

- 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.

- 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.

- Wanneer u Kaspersky Endpoint Security voor Windows installeert op een server waarop Kaspersky Security for Windows Server (KSWS) en Windows Defender-programma's zijn geïnstalleerd, moet u het systeem opnieuw opstarten. Het systeem moet opnieuw worden opgestart, zelfs als u de installatie van programma's hebt ingeschakeld zonder dat het systeem opnieuw moet worden opgestart. Windows Defender voor Windows Server is opgenomen in de lijst met software die incompatibel is met Kaspersky Endpoint Security voor Windows. Voor het installeren van het programma, verwijdert het installatieprogramma Windows Defender voor Windows Server. Voor het verwijderen van incompatibele software moet het systeem opnieuw worden opgestart.

- Voordat u Kaspersky Endpoint Security voor Windows (KES) installeert op een server waarop Kaspersky Security for Windows Server (KSWS) is geïnstalleerd, moet u KSWS Password Protection uitschakelen. Na het migreren van KSWS naar KES moet u wachtwoordbeveiliging inschakelen in de programma-instellingen.

- Als u de applicatie wilt installeren op computers met Windows 7 of Windows Server 2008 R2 waarop Veeam Backup & Replication-software is geïmplementeerd, moet u mogelijk uw computer opnieuw opstarten en de installatie opnieuw uitvoeren.

- Migratie van Kaspersky Small Office Security (KSOS) naar Kaspersky Endpoint Security (KES) met ingeschakelde Wachtwoordbeveiliging is beschikbaar vanaf KSOS build 21.16.*.*. Om eerdere versies van KSOS te migreren, moet u Wachtwoordbeveiliging uitschakelen of KSOS handmatig verwijderen. De migratie van KSOS naar KES met uitgeschakelde Wachtwoordbeveiliging wordt correct uitgevoerd.

- U kunt Kaspersky Endpoint Security niet installeren op een opstartbare verwisselbare schijf. Tijdens de installatie toont Kaspersky Endpoint Security een foutmelding: *Je hebt een ongeldige map of schijf geselecteerd. Het programma moet op een lokale harde schijf worden geïnstalleerd.* Als het u lukt om het programma te installeren op een verwisselbare schijf met hulpprogramma's van derden, kan het besturingssysteem crashen (BSOD) tijdens het opstartproces. Dit betekent dat Kaspersky Endpoint Security geen ondersteuning biedt voor Windows To Go en vergelijkbare oplossingen. Als u een computer wilt scannen vanaf een verwisselbare schijf, kunt u het gratis Kaspersky Rescue Disk programma gebruiker.

- Het installeren van Kaspersky Endpoint Security met netwerkonderdelen op een terminalserver met RDP-sessies voor meerdere gebruikers omvat enkele speciale overwegingen. Het besturingssysteem dwingt alle gebruikerssessies te beëindigen nadat de beheerderssessie eindigt. Als u verbinding wilt maken met de terminalserver, moet u de server opnieuw opstarten of u lokaal aanmelden bij het systeem. Dergelijk gedrag wordt gedicteerd door eigenaardigheden in hoe het Windows-besturingssysteem werkt.

- Als de webplug-ins Kaspersky Endpoint Security voor Windows (build 12.11.0.2004) en Kaspersky Endpoint Security voor Linux (build 12.4.0.1354) zijn geïnstalleerd in Kaspersky Security Center 16.0 of Kaspersky Security Center 16.1, kan het updaten van Kaspersky Endpoint Security voor Windows webplug-in naar versie 12.11.0.6004 leiden tot storingen in het beleid van Kaspersky Endpoint Security voor Linux .

  Mogelijke oplossing: ga naar de **Settings** → **Web plug-ins** en verwijder de webplug-in Kaspersky Endpoint Security voor Windows en de webplug-in Kaspersky Endpoint Security voor Linux en Unified Protection and Management Plug-in uit de lijst. Installeer vervolgens eerst de webplug-in Kaspersky Endpoint Security voor Linux en daarna de webplug-in Kaspersky Endpoint Security voor Windows.

- In de webconsole wordt de lijst met onderdelen onjuist weergegeven in de eigenschappen van het installatiepakket van Kaspersky Endpoint Security 12.11 voor Windows. Een afzonderlijk onderdeel, Anti-Cryptor, is niet beschikbaar in deze versie van het programma. De bescherming van gedeelde mappen tegen externe versleuteling maakt deel uit van het onderdeel Gedragsdetectie. In Kaspersky Endpoint Security 12.12 voor Windows is deze functionaliteit een afzonderlijk onderdeel. Tegelijkertijd wordt in de Beheerdersconsole (MMC) de lijst met onderdelen correct weergegeven.

Het programma upgraden

- 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 *Update van databases en programmamodules*, *Kritieke Gebiedenscan*, *Aangepaste Scan* en *Programma 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.

- 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 *Critical* 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.

- Na het upgraden van Kaspersky Endpoint Security naar versie 11.10.0 of hoger zonder opnieuw opstarten, zijn op de computer twee Kaspersky Endpoint Security-programma's geïnstalleerd. Verwijder de vorige versie van het programma niet handmatig. De vorige versie wordt automatisch verwijderd wanneer de computer opnieuw wordt opgestart.

- Na het upgraden van Kaspersky Endpoint Security op een computer met Microsoft Windows 11 kan het contextmenu van het bestand items weergeven voor zowel eerdere als nieuwe programmaversies. Start de computer twee keer opnieuw op om ervoor te zorgen dat het contextmenu van het bestand correct werkt.

- Als de zelfverdediging van het programma is uitgeschakeld en alle netwerkadapters zijn gestopt, zullen de netwerkonderdelen van het programma niet werken tussen het einde van de upgrade van het programma en het opnieuw opstarten van de computer. De netwerkonderdelen van het programma omvatten Web Threat Protection, Mail Threat Protection, Network Threat Protection, Firewall, Host Intrusion Prevention en Webcontrol. Start de computer opnieuw op zodat het programma correct werkt.

- Het BadUSB Attack Prevention onderdeel werkt niet tussen het einde van de programma-upgrade en het opnieuw opstarten van de computer. Start de computer opnieuw op zodat het programma correct werkt.

- Het programma kan niet worden bijgewerkt als het vorige upgradeproces niet is voltooid. Start de computer opnieuw op zodat het programma correct werkt.

- Nadat het programma is geüpgraded van eerdere versies dan Kaspersky Endpoint Security 11 voor Windows, moet de computer opnieuw worden opgestart.

- Als u Kaspersky Endpoint Security beheert met Kaspersky Security Center Cloud Console, is het lokaal updaten van het programma niet toegestaan. Wanneer u het programma lokaal updatet, is het niet mogelijk om de Gegevensverwerkingsupdate voor Kaspersky Security Center Cloud Console te accepteren.

Ondersteuning voor Arm-architectuur

- De installatie van Kaspersky Endpoint Security in de Light Agent-modus op virtuele machines met Arm wordt niet ondersteund.

- Kaspersky Disk Encryption wordt niet ondersteund op Arm-computers.

- Bestandsencryptie wordt niet ondersteund op Arm-computers.

- Versleuteling van verwisselbare schijven wordt niet ondersteund op Arm-gebaseerde computers.

- Op computers met Windows 11 voor Arm64 is EDR Agent niet compatibel met: Bitdefender Endpoint Security Tools.

- De functies voor bescherming van audiosignalen en bescherming van webcamtoegang worden niet ondersteund op Arm-computers.

- Op Arm-computers ondersteunt de Mail Threat Protection-extensie de 32-bit en 64-bit versies van Outlook 2016, Outlook 2021, Outlook 2024 en Outlook 365 voor Arm64.

- Kaspersky Endpoint Security verstuurt geen objecten die zijn bedoeld voor de Arm-architectuur naar Kaspersky Sandbox.

- Afdrukbeheer wordt niet ondersteund op Arm-computers.

- Integratie met Kaspersky Endpoint Detection and Response Expert (cloud) wordt niet ondersteund op Arm-computers.

- Op Arm-computers wordt de taak *IOC Scan* alleen ondersteunt van e-mailbestanden van de volgende e-mailclients: 32-bits en 64-bits versies van Outlook 2016 en Outlook 2021, 2024 en 365 voor Arm64.

Ondersteuning voor serverplatforms

- Op servers waarop *gegevensdeduplicatie* is ingeschakeld, moet u het bestand fsdmhost.exe toevoegen aan de lijst met vertrouwde programma's. Hiermee worden de prestaties van het programma geoptimaliseerd en wordt overmatige belasting van de CPU voorkomen.

- 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 malware-scan correct.

  - Nadat de taak *Malware-scan* is gestart, worden de met uitzonderingen toegevoegd met iChecker 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.

- Kaspersky Endpoint Security geïnstalleerd op een server waarop Microsoft Data Protection Manager (DPM) is geïmplementeerd, kan ervoor zorgen dat DPM niet goed werkt. Dit heeft te maken met beperkingen in de werking van DPM. Om storingen te voorkomen, moet u lokale serverstations toevoegen aan uitzonderingen voor de onderdelen File Threat Protection en *Malware-scan*-taken.

- De Server 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 de compatibiliteit van Kaspersky Endpoint Security voor Windows met Citrix PVS te ondersteunen, voer de installatie uit met de optie **Zorg voor compatibiliteit met Citrix PVS** 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 Lab\**\*"
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.
- Kaspersky Endpoint Security is compatibel met de VMware ESXi-hypervisor met de volgende beperkingen:
  - Kaspersky Endpoint Security is mogelijk niet compatibel met Guest Introspection-stuurprogramma's (vnetWFP.sys, vnetFLT.sys en andere). Om de incompatibiliteit op te lossen, werk de drivers bij naar de nieuwste versie of verwijder de drivers.
  - In sommige gevallen mislukt een poging om een verwijderbare schijf veilig van een virtuele machine te verwijderen. Probeer het apparaat nogmaals veilig los te koppelen.
- Het installeren van Kaspersky Endpoint Security op virtuele machines met de Citrix VDA-agent kan eindigen met een compatibiliteitsfout. Dit gebeurt omdat Citrix Provisioning Services een beperkte compatibiliteit met antivirusoplossingen heeft. Voor beste werkwijzen bij het gebruik van antivirusoplossingen met Citrix Provisioning Services raadpleegt u de: Citrix-ondersteuningswebsite.
- Kaspersky Endpoint Security slaat de scan van een verwisselbare schijf over als de schijf is verbonden met een virtuele machine op de Citrix-hypervisor (de taak *Scan van Verwisselbare Schijven*). Op dergelijke apparaten detecteert het besturingssysteem het aangesloten verwisselbare station als een netwerkstation. In dergelijke gevallen kunt u de taak *Aangepaste Scan*. Het programma werkt in de standaardmodus en in de Light Agent-modus hetzelfde.
- Als Kaspersky Endpoint Security is geïnstalleerd op een virtuele machine in een infrastructuur die gebruikmaakt van Citrix App Layering-technologie, worden bestanden die door het programma worden gedetecteerd als geïnfecteerd met de status *Object wordt verwijderd bij herstart* niet automatisch verwijderd wanneer de virtuele machine wordt opnieuw gestart.

  Om dergelijke bestanden te verwijderen, moet u het VHDX-bestand dat de gebruikerslaag bevat mounten op de computer van de beheerder van de Citrix App Layering en een malwarescan uitvoeren op de gemounte schijf.

Compatibiliteit met Kaspersky Security Center

- In Kaspersky Security Center Web Console versie 14.1 en eerder worden de namen van functionele gebieden voor de onderdelen Logboekinspectie en Bestandsintegriteitsmonitor niet correct weergegeven in het gedeelte met instellingen voor machtigingen voor gebruikerstoegang van de eigenschappen van Administration Server.
- Na het repareren van het programma wordt de bescherming van de computerverbinding met de Administration Server uitgeschakeld. Na het repareren van het programma, voer de *Administration Server verbindingsbescherming* taak opnieuw uit.
- In de Beheerconsole van Kaspersky Security Center toont het venster: **Selecteer een gebruiker of een groep gebruikers** alleen de eerste 50.000 gebruikers uit de lijst met Kaspersky Security Center-gebruikers weergegeven. Zie Help van Kaspersky Security Center voor meer informatie.

- Wanneer u in de beheerconsole van Kaspersky Security Center naar beheerde apparaten zoekt, kan het tabblad **Application components** meerdere varianten van de naam van dezelfde programmaonderdelen tegelijk weergeven, waaronder namen die verwijzen naar oudere versies van Kaspersky Endpoint Security. De namen van sommige onderdelen kunnen ook worden gedupliceerd.

  Om op onderdeel te zoeken, hoeft u alleen maar een van de weergegeven varianten te selecteren. Voor meer informatie over het detecteren van apparaten raadpleeg de Help van Kaspersky Security Center.

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.

- 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 wordt veroorzaakt doordat tijdens het installatieproces het programma eerst de ingesloten proeflicentie activeert. Het vereist internettoegang.

- 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 wordt veroorzaakt door het feit dat tijdens het installatieproces van de update het programma eerst de ingesloten proeflicentie activeert. Het vereist internettoegang.

- 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 14.1 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.

Mail Threat Protection

- 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).

- Kaspersky Endpoint Security biedt geen ondersteuning voor de 64-bits versie van de Microsoft Outlook-mailclient. Dit betekent dat Kaspersky Endpoint Security geen Microsoft Outlook-bestanden (PST- en OST-bestanden) scant als een 64-bit versie van Microsoft Outlook op de computer is geïnstalleerd, zelfs als e-mail is opgenomen in het scanbereik.

- Kaspersky Endpoint Security ondersteunt de Microsoft Outlook Nieuwe e-mailclient niet.

Remediation Engine

- Het programma herstelt alleen bestanden op apparaten met een NTFS- of FAT32-bestandssysteem.

- Het programma herstelt bestanden tot 100 MB groot.

- Het programma kan bestanden met de volgende extensies herstellen: odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls, xlsx, xlsm, 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, srw, 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.

Firewall

- Als een regel voor netwerkpakketten of netwerkregels voor programma's DNS-namen specificeert, kan Kaspersky Endpoint Security verzoeken naar de DNS-server sturen om de IP-adressen van deze bronnen te bepalen. De firewall gebruikt IP-adressen om de netwerkactiviteit te bewaken. Daarom zet het programma DNS-namen om in IP-adressen. Het wordt aanbevolen om DNS-namen alleen te gebruiken in regels voor LAN-computers of interne services.

- Als u een regel voor alle IPv6-adressen wilt opgeven, voegt u het adresbereik ::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff toe. Firewall ondersteunt het ::/0-masker niet.

- 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.

- 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 vertrouwd* 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 **Naam programma** 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 **Naam programma** leeg.

- Als u alle netwerkactiviteit hebt verboden met Firewall, detecteert het onderdeel Network Threat Protection mogelijk een aanval van het type Port Scanning. Dit kan gebeuren omdat het programma Network Threat Protection vóór Firewall start om verdachte activiteit in het netwerk te detecteren.

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.

Kaspersky Security Network

- Kaspersky Endpoint Security ondersteunt geen HTTPS bij verbinding met KSN Proxy (**Use HTTPS** selectievakje in KSN Proxy-verbindingsinstellingen aangevinkt) als het adres van de server niet-Latijnse letters bevat (niet ASCII-symbolen).

- 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 (KPSN) 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.

- Vanaf Kaspersky Endpoint Security 12.9 voor Windows moet u bij het overschakelen van KPSN naar wereldwijd KSN opnieuw bevestigen dat u akkoord gaat met de Kaspersky Security Network-verklaring. Hiervoor moet u het gebruik van Kaspersky Security Network inschakelen in de eigenschappen van het beleid of in de programma-interface en moet u bevestigen dat u akkoord gaat met de Kaspersky Security Network-verklaring. Als u de algemene KSN al hebt gebruikt, moet u eerst KSN-gebruik uitschakelen en vervolgens opnieuw inschakelen en bevestigen dat u akkoord gaat met de Kaspersky Security Network-verklaring. Als u niet akkoord gaat met de Kaspersky Security Network-verklaring, heeft het programma geen toegang tot de gegevens van Kaspersky Security Network.

- Kaspersky Endpoint Security verstuurt geen tekstbestanden (zoals TXT-, CSV-, LOG- en DOCX-bestanden zonder macro's) naar Kaspersky Security Network om ze te scannen. Het programma stuurt bestanden die een risico kunnen vormen naar KSN om te worden gescand. Deze bestanden bevatten uitvoerbare bestanden of bestanden die uitvoerbare code kunnen bevatten (zoals macro's in DOCX-bestanden). Andere onderdelen van het programma zijn verantwoordelijk voor het scannen van tekstbestanden. U kunt ook de reputatie van een tekstbestand handmatig controleren vanuit het contextmenu van het bestand. Als een tekstbestand de reputatie *Niet vertrouwd (Kaspersky Security Network)* heeft, negeert het programma de gedefinieerde actie voor gedetecteerde dreigingen.

Programmacontrole

- Als u met de Programmacontroleregels werkt, wordt het niet aanbevolen om meer dan 100.000 inclusie- en uitzonderingsvoorwaarden voor programma's in verschillende categorieën toe te voegen, op voorwaarde dat Kaspersky Endpoint Security actief is op een computer die voldoet aan de minimale hardwarevereisten en werkt op Microsoft Windows 10.

- Alleen ZIP-formaat archieven worden ondersteund bij het werken met Programmacontrole-regels in Kaspersky Security Center Web Console. 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).

- Wanneer u werkt met Programmacontrole-regels in Kaspersky Security Center Web Console, is de maximaal ondersteunde grootte van een geüpload bestand 104 MB. 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.

- Als u nieuwe *vooraf gedefinieerde regels van programmacontrole* hebt toegevoegd tijdens het upgraden van Kaspersky Endpoint Security, kunt u deze regels niet toepassen op eerdere versies van het programma.

- 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, dat zich in de map bevindt `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 programmanaam en de bestandshash specificeren vanuit de eigenschappen van het actieve programma.

- Bij het migreren van het KSWS-beleid naar het KES-beleidsprofiel hernoemt de wizard Beleid en taken batchconversie (Migratiewizard) programmacategorieën als categorienamen verboden tekens bevatten: `'` `*` `<` `>` `?` `\` `:` `|`. De Migratiewizard vervangt deze tekens door: `_` karakters. Bijvoorbeeld de `KSWS::\Everyone:[C61F-3B7C-4D89-96A1]` programmacategorie wordt hernoemd naar `KSWS_Everyone_[C61F-3B7C-4D89-96A1]`.

Apparaatcontrole

- Kaspersky Endpoint Security kan gebeurtenissen registreren waarbij externe apparaten verbinding maken en de verbinding verbreken. Windows-services gebruiken het systeemgebruikersaccount om apparaten te verbinden of los te koppelen. Hierdoor is het onmogelijk om te weten welke gebruiker het apparaat aansluit of loskoppelt. Kaspersky Endpoint Security specificeert het SYSTEEM-gebruikersaccount in de gebeurtenis.

- 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 verbindingsbewerkingen 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.

- Wanneer het programma wordt geüpgraded zonder dat de computer opnieuw wordt opgestart, past Apparaatbeheer geen toegangsregels toe op apparaten die opnieuw worden verbonden. Als het apparaat echter vóór de upgrade was aangesloten, past Apparaatbeheer de regels correct toe. Start de computer opnieuw op, zodat het programma correct werkt met apparaten die opnieuw zijn aangesloten.

- Op computers waarop Kaspersky Endpoint Security versie 12.0 is geïnstalleerd, wordt de printertoegangsmodus **Sta toe en registreer niet** voor het apparaattype **Netwerkprinters Afhankelijk van verbindingsbus** genoemd, als het beleid van Kaspersky Endpoint Security versie 12.1 wordt toegepast op de computer. In deze modi voert het programma dezelfde acties uit. In Kaspersky Endpoint Security versie 12.1 heeft de toegangsmodus voor netwerkprinters de juiste naam **Sta toe en registreer niet**.

- Vanaf Kaspersky Endpoint Security 12.0 voor Windows kunt u met het programma afdrukregels voor printers configureren (afdrukbeheer). Na het installeren van het programma met afdrukbeheer of het upgraden van het programma naar een versie met afdrukbeheer, moet u de computer opnieuw opstarten. Totdat de computer opnieuw is opgestart, past Kaspersky Endpoint Security geen afdrukregels toe en kan het alleen de toegang tot printers regelen. Als het herstarten van de computer nadelige gevolgen heeft voor de workflows in uw organisatie, kunt u alleen de spoolsv-service (Print Spooler) opnieuw opstarten. Afdrukbeheer wordt niet ondersteund op Arm-computers.

- Vanaf Kaspersky Endpoint Security voor Windows versie 12.0 is WPA3-protocolondersteuning aan het programma voor **Wifi**-apparaten. Als een beleid van Kaspersky Endpoint Security versie 12.2 wordt toegepast op een computer, wordt het WPA2-protocol geselecteerd op computers met Kaspersky Endpoint Security versie 11.11.0 en eerder; WPA2 / WPA3 is geselecteerd voor versies 12.0 tot 12.1; WPA3 is geselecteerd voor versie 12.2 en later.

- Apple-apparaten worden geclassificeerd als draagbare apparaten (MTP) en iTunes-apparaten. Het besturingssysteem kan de verbinding van het Apple-apparaat verkeerd identificeren en het Apple-apparaat niet herkennen als een draagbaar apparaat (MTP). Daardoor zal het Apple-apparaat niet beschikbaar zijn in bestandsbeheer, maar wel toegankelijk in de iTunes-applicatie. Als gevolg hiervan beheert Kaspersky Endpoint Security alleen de toegang tot het Apple-apparaat in het iTunes-programma. Om toegang te krijgen tot uw Apple-apparaat als een draagbaar apparaat (MTP), moet u naar Apparaatbeheer gaan en het USB-stuurprogramma van het Apple Mobile Device verwijderen uit de lijst met USB-controllers. Na het opnieuw opstarten van de computer, identificeert het besturingssysteem het Apple-apparaat als een draagbaar apparaat (MTP) en een iTunes-apparaat. Kaspersky Endpoint Security beheert de toegang tot het apparaat zowel in het iTunes-programma als in bestandsbeheer.

- In Kaspersky Endpoint Security 12.3 voor Windows, zijn de toegangsinstellingen verschillend voor het **Bluetooth** apparaattype. Als u de **Afhankelijk van verbindingsbus** waarde in de vorige versie van het programma hebt opgegeven, veranderd de geconfigureerde waarde, na het upgraden van het programma naar versie 12.3, vervolgens in **Toestaan en niet registreren**. Dit verandert niets aan het gedrag van het apparaat.

- Apparaatcontrole ondersteunt Bluetooth apparaten alleen via de Microsoft Windows Bluetooth-stack. Apparaatcontrole werkt mogelijk niet correct met Bluetooth-stacks van derden.

- Als het Bluetooth apparaat de Apparaatklasse (COD) verbergt of vervalst, werkt Apparaatcontrole mogelijk niet correct.

- Op Windows 7- of Windows 8-computers met bepaalde Realtek Bluetooth dongle stuurprogramma's is het misschien niet mogelijk om alleen Bluetooth-apparaten als invoerapparaat (HID-klasse) aan te sluiten. Dat wil zeggen: als u de toegang tot Bluetooth-apparaten verbiedt in de programma-instellingen en invoerapparaten toevoegt aan uitzonderingen, kan Apparaatbeheer in plaats daarvan de toegang tot alle Bluetooth-apparaten verhinderen.

Webcontrole

- De indelingen OGV en WEBM worden niet ondersteund.

- Het RTMP-protocol wordt niet ondersteund.

- Webcontrole ondersteunt alleen WSL1. Het programma heeft geen controle over WSL2-verkeer.

Adaptieve controle op afwijkingen

- Het wordt aanbevolen om automatisch uitzonderingen 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.

- Kaspersky Security Center 15.1 kan geen gedetailleerd **Rapport over de status van de regels van Adaptieve controle op afwijkingen**-rapport voor een specifieke regel aanmaken.

Drive Encryption (FDE)

- Kaspersky Disk Encryption wordt niet ondersteund op Arm-computers.

- BitLocker-stationsversleuteling wordt niet ondersteund op computers met Windows Home.

- 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.
- Er kunnen niet meerdere downloadagents naast elkaar bestaan op één geëncrypte computer.
- Bij een poging tot het herstellen van een afbeelding van een opstartbare GPT-schijf in een niet-geëncrypte staat, kan het besturingssysteem het besturingssysteem onbruikbaar maken. Volg deze aanbevelingen om dit te voorkomen:
  - Decrypt de schijf volledig voordat u de afbeelding vanaf een back-up terugzet.
  - Gebruik sector per sector kopiëren bij het maken van de afbeelding.
  - Verwijder gegevens van de eerste sectoren van de versleutelde schijf voordat u de image herstelt en initialiseer de schijf opnieuw.
- 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 account name>` 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)

- Bestandsencryptie wordt niet ondersteund op Arm-computers.

- Versleuteling van bestanden en mappen wordt niet ondersteund op Microsoft Windows Embedded-besturingssystemen.

- Nadat u het programma hebt geïnstalleerd, moet u het besturingssysteem opnieuw opstarten om te zorgen dat de encryptie van bestanden en mappen correct werkt.

- Het programma ondersteunt alleen bestandsencryptie op apparaten met NTFS- en FAT32-bestandssystemen. Als een geëncrypt bestand wordt overgebracht naar een apparaat met een niet-ondersteund bestandssysteem (bijvoorbeeld exFAT), wordt het bestand op dat apparaat niet geëncrypt en kan het worden gewijzigd.

- Als een geëncrypt bestand is opgeslagen op een computer met beschikbare encryptiefunctionaliteit 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 encryptiefunctionaliteit, wordt in geëncrypte vorm gekopieerd naar een computer die geen beschikbare encryptiefunctionaliteit 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 is voorzien, wordt het kenmerk *Archief* ingesteld in de bestandseigenschappen.

- Wanneer u het gedëcrypte bestand kopieert, bijvoorbeeld naar verwisselbare media, blijft het bestand mogelijk geëncrypt. Dit kan gebeuren omdat wanneer bestandsbeheerder (bijvoorbeeld explorer.exe) probeert toegang te krijgen tot het geëncrypte bestand, het de hash van het bestand opslaat in een speciale lijst van het proces. Wanneer de bestandsbeheerder na het decrypten van het bestand probeert toegang te krijgen tot het bestand, zoekt het proces naar de hash van het bestand in de lijst. Als de hash wordt gevonden, laat Kaspersky Endpoint Security het bestand geëncrypt achter. Om dit te voorkomen, moet u de lijst met het proces wissen. Het besturingssysteem wist automatisch de lijst met het proces wanneer deze vol raakt. U kunt de lijst ook handmatig wissen. Hiervoor kunt u de computer opnieuw opstarten, het proces herstarten dat u gebruikt om toegang tot het bestand te krijgen (bijvoorbeeld explorer.exe), of u kunt een ander programma voor bestandsbeheer gebruiken dat u niet hebt gebruikt voor toegang tot het geëncrypte bestand.

- 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. Encryption van offline bestanden of de Branch Caching technologie via SMB voor servers worden ook 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.

- 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 Subsystem for 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.

Detection and Response (EDR, NDR, MDR, XDR, Sandbox)

- U kunt geen objecten scannen die in quarantaine zijn geplaatst met de taak *Move file to Quarantine*.

- Het is niet mogelijk om een Alternate Data Stream (ADS) van meer dan 4 MB in quarantaine te plaatsen. Kaspersky Endpoint Security slaat elke gegevensstroom van dit volume over zonder de gebruiker op de hoogte te stellen.

- 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 Scan* taken op netwerkstations. Bijvoorbeeld `\\server\shared_folder`.

- Om ervoor te zorgen dat de taak *IOC Scan* met de termen van Emailltem correct werkt, moet de webplug-in van Kaspersky Endpoint Security worden bijgewerkt naar de nieuwste versie.

- Op Arm-computers wordt de taak *IOC Scan* alleen ondersteunt van e-mailbestanden van de volgende e-mailclients: 32-bits en 64-bits versies van Outlook 2016 en Outlook 2021, 2024 en 365 voor Arm64.

- 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.

- Bij het importeren van een beleid uit een KLP-bestand wordt de parameterwaarde die bepaalt of de algemene voorwaarden van de Kaspersky Detection and Response Expert-overeenkomst worden aanvaard, niet toegepast. Als gevolg hiervan vervult Kaspersky Endpoint Security, nadat het beleid is geïmporteerd, niet de functies van de EDR-agent. Om de EDR-agent te laten werken, moet u het beleid openen, een parameter wijzigen en de beleidsinstellingen opslaan.

- 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.

- De webplug-in Kaspersky Endpoint Security voor Windows 11.7.0 of hoger is vereist voor het beheren van IOC-incidentkaart. IOC-incidentkaarten zijn nodig bij het werken met Endpoint Detection and Response-oplossing (EDR Optimum en EDR Expert). Detectiegegevens zijn alleen beschikbaar in Kaspersky Security Center Web Console en Kaspersky Security Center Cloud Console.

- 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.

- De configuratie [KES+KEA+ingebouwde agent] wordt niet ondersteund. Deze configuratie verstoort de interactie tussen programma's en de Detection and Response-oplossing die in uw organisatie wordt ingezet. Bovendien kan het gebruik van Kaspersky Endpoint Agent en de ingebouwde agent op dezelfde computer leiden tot duplicatie van telemetrie en een verhoogde belasting op de computer en het netwerk. Zorg ervoor dat Kaspersky Endpoint Agent van de computer is verwijderd nadat u bent gemigreerd naar de [KES+ingebouwde agent]-configuratie. Als Kaspersky Endpoint Agent na de migratie blijft werken, verwijdert u het programma handmatig (bijvoorbeeld met behulp van de taak *Uninstall application remotely*).

  Met het installatieprogramma kunt u Kaspersky Endpoint Agent implementeren op een computer waarop Kaspersky Endpoint Security en de ingebouwde agent zijn geïnstalleerd. Kaspersky Endpoint Agent en de ingebouwde agent kunnen ook op één computer worden geïnstalleerd dankzij de taak *Programmaonderdelen wijzigen*. Het gedrag hangt af van de versies van Kaspersky Endpoint Security en Kaspersky Endpoint Agent.

- Bij het genereren van waarschuwingsdetails verstrekt het programma informatie over de gedetecteerde bedreiging, inclusief hashes van gewijzigde bestanden. Kaspersky Endpoint Security berekent de hash van het bestand tijdens het genereren van waarschuwingsdetails. Bedenk dat de oorspronkelijke hash van het bestand op het moment dat de bestandswijziging werd gegenereerd mogelijk niet dezelfde is als de hash die werd berekend toen de waarschuwingsdetails werden gegenereerd.

- De ingebouwde agent, EDR (KATA), hervat de netwerkisolatie van een computer nadat de computer opnieuw is opgestart, zelfs als de isolatieperiode is verstreken. Om herhaalde isolatie van de computer te voorkomen, moet u netwerkisolatie uitschakelen in de Kaspersky Anti Targeted Attack Platform-console.

- We raden u aan het programma te upgraden nadat de netwerkisolatie is voltooid. Na het upgraden van Kaspersky Endpoint Security kan netwerkisolatie worden gestopt.

- Ingebouwde agents voor EDR (KATA), EDR Optimum en EDR Expert zijn niet compatibel met elkaar. Daarom kan de activering van de ingebouwde EDR-agent met een zelfstandige Kaspersky Endpoint Detection and Response Add-on-licentie worden overgeslagen als u Kaspersky Endpoint Security met verschillende EDR-functionaliteit hebt geactiveerd. De activering van de ingebouwde EDR(KATA)-agent met een zelfstandige licentie wordt bijvoorbeeld overgeslagen als u Kaspersky Endpoint Security hebt geactiveerd met de licentie [KES+EDR Optimum].

- In Kaspersky Endpoint Security versie 12.1 ondersteunt de ingebouwde EDR-agent (KATA) de volgende metabestanden voor de *NTFS-metabestanden ophalen* taak: $Secure:$SDH:$INDEX_ROOT; $Secure:$SDH:$INDEX_ALLOCATION; $Secure:$SDH:$BITMAP; $Secure:$SII:$INDEX_ROOT; $Secure:$SII:$INDEX_ALLOCATION; $Secure:$SII:$BITMAP; $Extend\$UsnJrnl:$J:$DATA; $Extend\$UsnJrnl:$Max:$DATA. Beperkte ondersteuning voor deze metabestanden werd toegevoegd aan Kaspersky Endpoint Security versie 12.2.

- Tijdens het migreren van Kaspersky Endpoint Agent naar Kaspersky Endpoint Security voor de Kaspersky Anti Targeted Attack Platform (EDR)-oplossing, kunnen er fouten optreden tijdens het verbinden van de computer met de Central Node servers. De reden is dat de migratiewizard in Web Console de volgende beleidsinstellingen overslaat en deze niet migreert:

  - Verbod op wijzigen van de instellingen **Connection settings** ("hangslot").

    Standaard kunnen de instellingen gewijzigd worden (het "hangslot" is open). De instellingen zijn daarom niet toegepast op de computer. U zult de wijziging van de instellingen moeten verbieden en het "hangslot" sluiten.

  - Crypto-container.

    Als u twee-weg verificatie gebruikt om contact te maken met de Central Node servers, moet u de crypto-container opnieuw toevoegen. De migratiewizard migreert correct het TLS-certificaat van de server.

  De wizard Beleids- en Taakmigratie in Beheerconsole (MMC) migreert alle instellingen voor het Kaspersky Anti Targeted Attack Platform (EDR)-oplossing.

- De activatiestatus van het programma wordt onjuist weergegeven wanneer het programma wordt geïnstalleerd in de Endpoint Detection and Response Agent-modus ter ondersteuning van de Kaspersky Managed Detection and Response-oplossing zonder verbinding met Kaspersky Security Center. Na het downloaden van het BLOB-bestand geeft het systeemvak van de taakbalk van Windows een onjuiste status weer: *Programma is niet geactiveerd*. Het programma-interface geeft de activatiesstatus echter correct weer. Start de computer opnieuw op zodat het programma correct werkt.

- Kaspersky Endpoint Security maakt integratie met de Kaspersky Anti Targeted Attack Platform-oplossing mogelijk met behulp van de EDR (KATA)-onderdeel of Endpoint Sensor (niet ondersteund). Houd er rekening mee dat u slechts één van de onderdelen kunt gebruiken voor interactie met Kaspersky Anti Targeted Attack Platform. Om de status van het onderdeel te bekijken, opent u computereigenschappen in de Beheerconsole (MMC), in het gedeelte **Applications**, open de eigenschappen van Kaspersky Endpoint Security voor Windows en ga naar het gedeelte **Components**. De volgende speciale overwegingen zijn van toepassing op de weergave van het onderdeelstatus voor de interactie met Kaspersky Anti Targeted Attack Platform:

  - Voor de beheerplug-in 12.0 en eerdere versies geeft het programma de huidige status van **Endpoint Sensor** weer. In Kaspersky Endpoint Security 12.0 en eerder is het EDR (KATA)-onderdeel niet beschikbaar. Het EDR (KATA)-onderdeel is geïntroduceerd in versie 12.1.

  - Voor de beheerplug-in 12.1 en latere versies geeft het programma de algemene status van **Endpoint Detection and Response (KATA)** weer, wat zowel de Endpoint Sensor status als de status van EDR (KATA)-onderdeel kan betekenen. Dit is afhankelijk van de versie van het programma die op de computer van de gebruiker is geïnstalleerd en van de beschikbare onderdelen die u kunt gebruiken voor interactie met Kaspersky Anti Targeted Attack Platform.

- Vanaf Kaspersky Endpoint Security versie 12.6 en hoger geeft Kaspersky Security Center Webconsole versie 14.2 en lager de naam van de **Endpoint Detection and Response (KATA)**-onderdeel niet correct weer in de computereigenschappen. In plaats van het onderdeel **Endpoint Detection and Response (KATA)** wordt in het programma de naam van het onderdeel **Endpoint Detection and Response Expert (KATA EDR)** weergegeven. Om de lijst met onderdelen te bekijken, open computereigenschappen in de Webconsole, in het gedeelte **Applications**, open de eigenschappen van Kaspersky Endpoint Security voor Windows en ga naar het gedeelte **Components**. Vanaf Kaspersky Security Center Web Console versie 15.1 en hoger geeft het programma de naam van het onderdeel correct weer.

- Bij het bijwerken van de Kaspersky Endpoint Detection and Response beheerplug-in naar versie 15.3 die is geïnstalleerd in Weconsole-versies 14.0–14.2, worden waarschuwingsdetails onjuist weergegeven. Start de Beheerserver van Kaspersky Security Center opnieuw om de details van de waarschuwingen correct te laten werken.

- Kaspersky Endpoint Detection and Response beheerplug-in versie 15.4 en hoger biedt geen ondersteuning voor Kaspersky Security Center versie 14.0. Na het bijwerken van de beheerplug-in worden waarschuwingsdetails onjuist weergegeven.

- De klasseoplossingen van Kaspersky Extended Detection and Response (XDR) versie 1.4 bieden geen ondersteuning voor de webplug-in Kaspersky Endpoint Security voor Windows versie 12.12 of nieuwer. U kunt de huidige versie van de webplug-in behouden of de XDR-oplossing bijwerken naar versie 2.0 of nieuwer.

- Kaspersky Endpoint Security verstuurt geen objecten die zijn bedoeld voor de Arm-architectuur naar Kaspersky Sandbox.

- Integratie met Kaspersky Endpoint Detection and Response Expert wordt niet ondersteund op Arm-computers.

- Kaspersky Endpoint Security ondersteunt in totaal tot 10.000 EDR Expert (on-premises) filterregels voor opname en uitzonderingen van gebeurtenissen.

- EDR Expert (on-premises) filterregels voor gebeurtenissen worden niet door het beleid doorgegeven aan beheerde apparaten met Kaspersky Endpoint Security versie 14.0 of lager als de ondersteunde limiet voor opgeslagen filterregels wordt overschreden. Het programma toont een overeenkomstige waarschuwing.

Andere beperkingen

- Windows-besturingssystemen, vanaf versie 11 24H2, ondersteunen de UDP Receive Segment Coalescing Offload (URO) technologie. De technologie is standaard ingeschakeld als een compatibele netwerkkaart en drivers op de computer zijn geïnstalleerd. Het uitschakelen van URO op de computer van een gebruiker kan de prestaties van het programma aanzienlijk verminderen.

- Kaspersky Endpoint Security ondersteunt het WSL-subsysteem (Windows Subsystem for Linux) met beperkingen:

  - WSL 1 Het programma bewaakt het netwerkverkeer en detecteert dreigingen via HTTP/HTTPS. Omdat Kaspersky Endpoint Security zijn eigen certificaat gebruikt om beveiligde HTTPS-verbindingen te scannen, kan de werking van sommige programma's van derden worden onderbroken.

  - WSL 2 Het programma biedt geen ondersteuning voor WSL 2.

- 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 encryptiefunctionaliteit blijft ingeschakeld).

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

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

- 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 waardes 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 volgzaam 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.

- Er kunnen TLS-verbindingsfouten optreden wanneer software van derden met de Libcurl-bibliotheek werkt. Dit kan te maken hebben met het Kaspersky-certificaat dat Kaspersky Endpoint Security gebruikt om gecodeerde verbindingen te scannen. Om verder te werken, kunt u certificaatvalidatie voor software van derden uitschakelen (niet aanbevolen) of een Kaspersky-certificaatlichaam toevoegen aan het cURL-certificaatarchief. Raadpleeg de Kaspersky Knowledge Base voor gedetailleerde informatie.

- 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.

- 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 programmarapport en in het Kaspersky Security Center-rapport.

- 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 Beheerconsole (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 beleidshiërarchie 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 de Safe Mode van Windows.

- 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 geroteerde 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.

- 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:\folder1\folder2`, wordt de scan uitgevoerd voor het pad `C:\folder1\`.

- Als u een softwarerestrictiebeleid (Software Restriction Policies, SRP) gebruikt, wordt de computer mogelijk niet geladen (zwart scherm). Om defecten te voorkomen, moet u het gebruik van programmabibliotheken toestaan in de SRP-eigenschappen. Voeg in de SRP-eigenschappen de regel toe met **Onbeperkte** beveiligingsniveau voor het bestand khkum.dll (**New Hash Rule** menu-item). Dit bestand bevindt zich in de map `C:\Program Files (x86)\Common Files\Kaspersky Lab\KES.14.1\klhk\klhk_x64\`. Als u deze methode hebt geselecteerd, moet u bovendien het selectievakje **Updates voor programmamodules downloaden** uitschakelen in de *Updaten*-taakinstellingen voor Kaspersky Endpoint Security. Voor meer informatie over het gebruik van SRP raadpleegt u de Microsoft-documentatie.

  U kunt SRP ook uitschakelen en het onderdeel Programmacontrole van Kaspersky Endpoint Security gebruiken om het programmagebruik te controleren.

- Als de computer deel uitmaakt van een domein onder Windows Group Policy Object (Group Policy Object, GPO) met de parameter DriverLoadPolicy ingesteld op 8 (Good only), 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 (Good and unknown). ELAM-instellingen bevinden zich in het beleid onder: **Computer Configuration** → **Administrative Templates** → **System** → **Early Launch Antimalware**.

- Beheer van Outlook-plug-in-instellingen via Rest API wordt niet ondersteund.

- Taakuitvoerinstellingen 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.

- 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).

- Als Kaspersky Endpoint Security is geïnstalleerd op een server van de SQL Server DBMS verstuurt het programma verzoeken naar het exemplaar van de server. Dit is nodig om de taken van SQL Server Agent en voorkom dat schadelijke taken worden uitgevoerd. Kaspersky Endpoint Security gebruikt de: SQL Server gebruikersaccount om taken te scannen. Het programma verstuurt verzoeken naar de server tijdens het scannen van het systeemgeheugen en na het bijwerken van antivirusdatabases.

- 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.

  - Het Kaspersky Endpoint Security-programma is niet compatibel met het onderdeel Schijfbescherming en gegevensversleuteling van Secret Net Studio-software.

    Het programma kan niet worden geïnstalleerd op een computer waar Secret Net Studio is ingezet met het onderdeel Schijfbescherming en gegevensversleuteling. Om interoperabiliteit mogelijk te maken, moet u het onderdeel Schijfbescherming en gegevensversleuteling 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.

- Bij het importeren van regels voor Systeemintegriteitscontrole, controleert het programma de ID en naam van de regel. Als de regel-ID's hetzelfde zijn, vervangt Kaspersky Endpoint Security de bestaande regels door de nieuwe regel. Bij het exporteren van regels wijst het programma automatisch ID's toe. Regel met identieke ID's kan bestaan, bijvoorbeeld als u handmatig geëxporteerde XML-bestanden voor regels hebt bewerkt. Als regel-ID's uniek zijn, maar de regelnamen hetzelfde, voegt Kaspersky Endpoint Security toe: `(1)` en zo verder naar de naam van de regel.

- Vanaf versie 12.11 van Kaspersky Endpoint Security for Windows is het niet mogelijk om de instellingen te bekijken van een bovenliggend beleid dat open staat in een onderliggende groep in de Web Console. De webconsole toont ook een waarschuwing: *This policy is inherited. You can edit the policy settings only in the administration group in which it was created*.

- Pop-upmeldingen die langer zijn dan 256 tekens worden niet weergegeven in de Beheerconsole (MMC).

- De namen van de onderdelen in het beleid en in het installatiepakket kunnen verschillen. De Endpoint Detection and Response Expert (on-premises) kan bijvoorbeeld Endpoint Detection and Response (KATA), Endpoint Detection and Response Expert (on-premises), Kaspersky Anti Targeted Attack Platform Integration heten. De namen van onderdelen kunnen ook verschillen afhankelijk van de versie van het programma.

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.

Cloud Discovery

Cloud Discovery beheert gebruikerstoegang tot cloudservices. Cloudservices omvatten bijvoorbeeld Microsoft Teams, Salesforce en Microsoft Office 365. Cloudservices zijn gegroepeerd in categorieën, bijvoorbeeld *Bestandsdeling*, *Messengers*, *E-mail*.

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.

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.

Integratieserver

Kaspersky Endpoint Security for Virtualization Light Agent. Communiceert tussen Kaspersky Endpoint Security-onderdelen en de virtuele infrastructuur.

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.

Kerberos-authenticatie

Mechanisme van wederzijdse authenticatie door de client en de server voordat een verbinding tussen beide tot stand wordt gebracht, waardoor communicatie via onveilige netwerken mogelijk is. Het mechanisme is gebaseerd op een ticket dat de gebruiker verkrijgt bij een vertrouwd authenticatiecentrum.

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.

Light Agent

Kaspersky Endpoint Security for Virtualization Light Agent. Het wordt geïnstalleerd op elke virtuele machine die beschermd moet worden.

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:\Folder\**\*.txt` omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen bevinden genest in de `Folder`, uitgezonderd de `Folder` zelf. 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:\Folder\???.txt` omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam `Folder` 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 encryptiefunctionaliteit op de computer beschikbaar is.

Scanbereik

Objecten die Kaspersky Endpoint Security scant wanneer het een scantaak uitvoert.

SVM

Beveiligde virtuele machine – een speciale virtuele machine waarop de scanserver-service (Protection Server, een onderdeel van Kaspersky Endpoint Security for Virtualization Light Agent) is geïnstalleerd.

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 gelijkt 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 kunt u infectie van het bestandssysteem van een computer voorkomen. Het onderdeel File Threat Protection bevindt zich standaard permanent in het RAM van de computer en scant alle bestanden die worden geopend, opgeslagen en uitgevoerd in realtime. Dit onderdeel scant bestanden op alle computerschijven, inclusief aangesloten schijven. Het onderdeel biedt computerbescherming met behulp van antivirusdatabases, de Kaspersky Security Network-cloudservice en heuristische analyse.

Het onderdeel scant de bestanden waartoe een 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 zich in de OneDrive-cloudopslag bevindt, downloadt en scant Kaspersky Endpoint Security de bestandsinhoud.

Instellingen van het onderdeel File Threat Protection

Parameter	Beschrijving
Beveiligingsniveau *(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)*	Voor File Threat Protection kan Kaspersky Endpoint Security verschillende groepen instellingen toepassen. Deze groepen van instellingen die in het programma zijn opgeslagen, worden *beveiligingsniveaus* genoemd: • **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. • **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.
Bestandstypen *(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)*	**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, scant het programma alleen infecteerbare bestanden. 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, scant het programma alleen infecteerbare bestanden. De bestandsindeling wordt dan bepaald op basis van de bestandsextensie.

Parameter	Beschrijving
Scanbereik	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. 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 alleen voorkomen dat een object (zoals een verwisselbare schijf) wordt gescand.
Machine learning en analyse op basis van definities *(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)*	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. Op aanbeveling van Kaspersky-experts is machine learning en analyse op basis van definities altijd ingeschakeld.
Heuristische analyse *(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)*	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.
Actie bij detectie van een dreiging	**Desinfecteren of verwijderen als desinfectie mislukt**. Als deze optie is geselecteerd, probeert het programma automatisch om ieder gevonden geïnfecteerd bestand te desinfecteren. Mocht de desinfectie mislukken, dan wordt het bestand door het programma verwijderd. **Desinfecteren of blokkeren als desinfectie mislukt**. Als deze optie is geselecteerd, probeert het programma automatisch om ieder gevonden geïnfecteerd bestand te desinfecteren. Als de desinfectie mislukt, blokkeert het programma dit bestand. **Blokkeren**. Als deze optie is geselecteerd, blokkeert het programma het geïnfecteerde bestand automatisch zonder te proberen het te desinfecteren of te verwijderen. Voordat u probeert een geïnfecteerd bestand te desinfecteren of te verwijderen, maakt het programma een reservekopie van het bestand voor het geval u het bestandmoet herstellen of als het in de toekomst kan worden gedesinfecteerd.
Scan alleen nieuwe en aangepaste 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.
Scan archieven	ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE en andere bestanden scannen. Het programma 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 (een archief in een archief).
Scan distributiepakketten	Distributiepakketten van programma's van derden scannen.
Scan Microsoft Office-bestanden	Scant Microsoft Office-bestanden (DOC, DOCX, XLS, PPT en andere Microsoft-extensies). Bestanden in Office-indeling bevatten ook OLE-objecten. Het programma scant office-bestanden die kleiner zijn dan 1 MB, ongeacht of het selectievakje is ingeschakeld of niet.
Bestanden in e-mailindeling scannen	Scant bestanden in e-mailformaat. Het programma scant MSG- en EML-bestanden. Bestanden in e-mailformaat bevatten ook OLE-objecten en MHT-bestanden. Kaspersky Endpoint Security scant bestanden in e-mailformaat die kleiner zijn dan 1 MB, ongeacht of het selectievakje is ingeschakeld of niet.
Pak grote samengestelde bestanden niet uit	Als dit selectievakje is ingeschakeld, scant het programma geen samengestelde bestanden als ze groter zijn dan de opgegeven waarde. Als dit selectievakje is uitgeschakeld, worden samengestelde bestanden van alle grootten gescand door het programma. Het programma scant grote bestanden die uit archieven worden gehaald, ongeacht of het selectievakje is ingeschakeld of niet.

Parameter	Beschrijving
Pak samengestelde bestanden op de achtergrond uit	Als het selectievakje is ingeschakeld, verleent het programma 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. Het programma 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 het programma pas toegang tot samengestelde bestanden nadat bestanden van elke grootte zijn uitgepakt en gescand.
Scanmodus *(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)*	Kaspersky Endpoint Security scant bestanden waartoe de gebruiker, het besturingssysteem of een programma dat onder het gebruikersaccount wordt uitgevoerd, toegang heeft. **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.
Gebruik iSwift-technologie *(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)*	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.
Gebruik iChecker-technologie *(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)*	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).
File Threat Protection pauzeren *(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)*	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.
Scan van bestandsbewerkingen uitgevoerd in Windows-containers	Als er een bedreiging in een container wordt gedetecteerd, voert het programma de actie uit die is geselecteerd voor het onderdeel File Threat Protection. **Stop de container als desinfectie mislukt**. Het programma beschikt mogelijk niet over voldoende lees- en schrijfrechten voor het gedetecteerde object. In dat geval is het niet mogelijk om het gedetecteerde object te desinfecteren of te verwijderen. Als dit selectievakje is ingeschakeld, blokkeert het programma het gedetecteerde object en stopt de container. Als dit selectievakje is uitgeschakeld, blokkeert het programma alleen het gedetecteerde object. **Scan geen bestandsbewerkingen die worden uitgevoerd in Windows-containers**. Als het selectievakje is ingeschakeld, scant het programma de container alleen wanneer de container wordt gestart. Als het selectievakje is uitgeschakeld, scant het programma de container continu in realtime.

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.

Om Web Threat Protection te kunnen gebruiken, moet u de initiële configuratie van het programma voltooien:

- Voor de bewaking van HTTPS-verkeer, schakel het scannen van versleutelde verbindingen in (standaard ingeschakeld).
- Selecteer de poorten die: Kaspersky Endpoint Security moet monitoren (standaard bewaakt het programma alle poorten).
- Selecteer het programma waarvan u wilt dat Kaspersky Endpoint Security het verkeer bewaakt. De meeste browsers staan al in de lijst met door Kaspersky aanbevolen programma's. Als uw browser niet in de lijst staat, kunt u deze handmatig toevoegen.
- Wij adviseren om een script voor webpagina-interactie in het webverkeer te injecteren (scriptinjectie is standaard uitgeschakeld). Met dit script kunnen Web Threat Protection-gebeurtenissen voor het programmagebeurtenislogboek, het OS-gebeurtenislogboek en rapporten worden geregistreerd.

Wanneer een gebruiker een schadelijke website of phishingwebsite probeert te openen, blokkeert Kaspersky Endpoint Security de toegang en wordt er een waarschuwing weergegeven.

Instellingen van het onderdeel Web Threat Protection

Parameter	Beschrijving
Beveiligingsniveau *(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)*	Voor Web Threat Protection kan het programma verschillende groepen instellingen toepassen. Deze groepen van instellingen die in het programma zijn opgeslagen, worden *beveiligingsniveaus* genoemd: • **Hoog**. Het beveiligingsniveau waarop het onderdeel Web Threat Protection het webverkeer dat een computer via HTTP en FTP ontvangt, maximaal scant. 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 het programma 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. • **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 oppervlakkige scan uit.
Actie bij detectie van een dreiging	**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.
Controleer of het webadres voorkomt in de database met schadelijke webadressen *(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)*	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.
Gebruik heuristische analyse *(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)*	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. 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.

Parameter	Beschrijving
Controleer of het webadres voorkomt in de database met phishingadressen *(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)*	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.
Scan geen internetverkeer van vertrouwde webadressen	Als deze optie 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. 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 onderdelen Web Threat Protection, Mail Threat Protection en Webcontrole hun werk doen.

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
- Windows Mail
- MyOffice Mail
- R7-Office Organizer

Om verkeer in Mozilla Thunderbird, MyOffice Mail en R7-Office Organizer e-mailprogramma's te scannen, moet u het Kaspersky-certificaat toevoegen aan het certificaatarchief en het eigen certificaatarchief selecteren.

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 Mail Threat Protection-extensie ondersteunt de 32-bit en 64-bit versies van Outlook 2010, 2013, 2016, 2019, 2021, 2024 en 365. Op Arm-computers ondersteunt de Mail Threat Protection-extensie de 32-bit en 64-bit versies van Outlook 2016, Outlook 2021, Outlook 2024 en Outlook 365 voor Arm64.

Het onderdeel Mail Threat Protection scant geen berichten als de e-mailclient in een browser is geopend.

Wanneer een schadelijk bestand wordt gedetecteerd in een bijlage, voegt Kaspersky Endpoint Security informatie over de uitgevoerde actie toe aan het onderwerp van het bericht, bijvoorbeeld *[Bericht is verwerkt] <onderwerp van bericht>*.

Parameter	Beschrijving
Beveiligingsniveau *(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)*	Voor Mail Threat Protection kan het programma verschillende groepen instellingen toepassen. Deze groepen van instellingen die in het programma zijn opgeslagen, worden *beveiligingsniveaus* genoemd: • **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 het programma 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. • **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.
Actie bij detectie van een dreiging	**Desinfecteren of verwijderen als desinfectie mislukt**. Wanneer een geïnfecteerd object wordt gedetecteerd in een inkomend of uitgaand bericht, probeert het programma 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 het programma het geïnfecteerde object. Het programma voegt informatie over de uitgevoerde actie toe aan het onderwerp van het bericht, bijvoorbeeld *[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 het programma een waarschuwing toe aan het onderwerp van het bericht. De gebruiker krijgt dan toegang tot het bericht met de originele bijlage. Wanneer een geïnfecteerd object wordt gedetecteerd in een inkomend bericht, probeert Kaspersky Endpoint Security het gedetecteerde object te desinfecteren. Als het object niet kan worden gedesinfecteerd, blokkeert het programma de verzending van het bericht en toont het e-mailprogramma een fout. **Blokkeren**. Als een geïnfecteerd object wordt gedetecteerd in een inkomend bericht, voegt het programma een waarschuwing toe aan het onderwerp van het bericht. De gebruiker krijgt dan toegang tot het bericht met de originele bijlage. Als een geïnfecteerd object wordt gedetecteerd in een uitgaand bericht, blokkeert het programma de verzending van het bericht en toont het e-mailprogramma een fout.
Beschermd bereik *(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)*	Het *Beschermd bereik* omvat objecten die door het onderdeel worden gecontroleerd wanneer het wordt uitgevoerd: inkomende en uitgaande berichten of 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.
Scan POP3-, SMTP-, NNTP- en IMAP-verkeer	Scannen door het onderdeel Mail Threat Protection van verkeer dat wordt overgebracht via de POP3-, SMTP-, NNTP- en IMAP-protocollen.
Verbind Microsoft Outlook-extensie	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. Als e-mail wordt gescand met de extensie voor Microsoft Outlook, wordt u aanbevolen de Cached Exchange Mode te gebruiken. Voor meer gedetailleerde informatie over de Exchange-modus met cache en aanbevelingen voor het gebruik ervan, raadpleegt u de Microsoft Knowledge Base.
Heuristische analyse *(beschikbaar in de Beheerconsole (MMC) en in de Kaspersky Endpoint Security-interface)*	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.

Parameter	Beschrijving
Scan toegevoegde archieven	ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE en andere bestanden scannen. Het programma 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 (een archief in een archief). Als het programma tijdens de scan een wachtwoord voor een archief detecteert in de tekst van het bericht, wordt dit wachtwoord gebruikt om de inhoud van het archief te scannen op schadelijke programma's. In dit geval wordt het wachtwoord niet opgeslagen. Tijdens het scannen wordt een archief uitgepakt. Als er een programmafout optreedt tijdens het uitpakken, kunt u de uitgepakte bestanden die zijn opgeslagen op het volgende pad handmatig verwijderen: %systemroot%\temp. De bestanden hebben de PR-prefix.
Scan Microsoft Office-bijlagen	Scant Microsoft Office-bestanden (DOC, DOCX, XLS, PPT en andere Microsoft-extensies). Bestanden in Office-indeling bevatten ook OLE-objecten. Het programma scant office-bestanden die kleiner zijn dan 1 MB, ongeacht of het selectievakje is ingeschakeld of niet.
Scan geen archiefbestanden groter 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.
Scan archieven niet langer dan N sec	Als het selectievakje is ingeschakeld, is de toegestane scanduur voor archieven die aan e-mailberichten zijn toegevoegd beperkt tot de opgegeven tijd.
Filter voor bijlagen	Het bijlagenfilter wordt niet toegepast op uitgaande e-mailberichten. **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 onderstrepingsteken (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. In de lijst met bestandsmaskers kunt u opgeven welke soorten bijlagen moeten worden hernoemd of verwijderd uit e-mailberichten.

Network Threat Protection

Het onderdeel *Network Threat Protection* (ook wel Intrusion Detection System (IDS) genoemd) controleert inkomend netwerkverkeer op activiteiten die kenmerkend zijn voor netwerkaanvallen. Wanneer het programma 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 het programma 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
Behandel poortscans en flooding als aanvallen	*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. 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. 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.
Blokkeer aanvallende apparaten voor N min	Als deze optie is ingeschakeld, voegt de Network Threat Protection-component de aanvallende computer toe aan de geblokkeerde lijst. 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 999 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.
Uitzonderingen	De lijst bevat IP-adressen die Network Threat Protection niet blokkeert als er netwerkaanvallen vanaf die IP-adressen plaatsvinden. U kunt een IP-adres toevoegen met opgegeven poort en protocol. Het programma registreert geen informatie over netwerkaanvallen vanaf de IP-adressen die op de lijst met uitzonderingen staan.
MAC spoofing-bescherming	Bij een *MAC-spoofing-aanval* wordt het MAC-adres van een netwerkapparaat (netwerkkaart) 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.

Firewall

Het onderdeel Firewall blokkeert ongeautoriseerde verbindingen met een 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. Plaatst het programma in een van de vertrouwensgroepen: *Vertrouwd*, *Deels beperkt*, *Zeer beperkt*, *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 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 op een bepaalde manier. Netwerkregel voor programma's omvat toegangsregels op basis van de netwerkstatus: *Openbaar netwerk*, *Lokaal netwerk*, *Vertrouwd netwerk*. 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.

Typen netwerkverbinding

U kunt met de Firewall de netwerkactiviteit beheren, afhankelijk van het type van de netwerkverbinding. Kaspersky Endpoint Security ontvangt het type netwerkverbinding van het besturingssysteem van de computer. Het type van de netwerkverbinding in het besturingssysteem wordt door de gebruiker ingesteld bij het opzetten van de verbinding. U kunt het type van de netwerkverbinding wijzigen in de instellingen van Kaspersky Endpoint Security. De firewall controleert de netwerkactiviteit afhankelijk van het type netwerk gespecificeerd in de Kaspersky Endpoint Security-instellingen en niet in het besturingssysteem.

De volgende typen netwerkverbindingen zijn beschikbaar:

- **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 het type *Openbaar netwerk* toe aan het internet. U kunt het type 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 een computer niet wordt blootgesteld aan aanvallen of pogingen tot onbevoegde gegevenstoegang. Firewall staat alle netwerkactiviteit in netwerken met deze status toe.

Instellingen van het onderdeel Firewall

Parameter	Beschrijving
Pakketregels	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. 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. 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. Regels voor netwerkpakketten hebben een hogere prioriteit dan netwerkregels voor programma's.
Beschikbare netwerken	Deze tabel bevat informatie over netwerkverbindingen die Firewall op de computer detecteert. De status *Openbaar netwerk* wordt standaard toegewezen aan het internet. U kunt de status van het internet niet wijzigen.
Regels voor programma's	**Programma**. 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. 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. **Netwerkregels**. Een tabel met netwerkregels voor programma's die in een vertrouwensgroep zijn geplaatst. Firewall 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.

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 een 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.

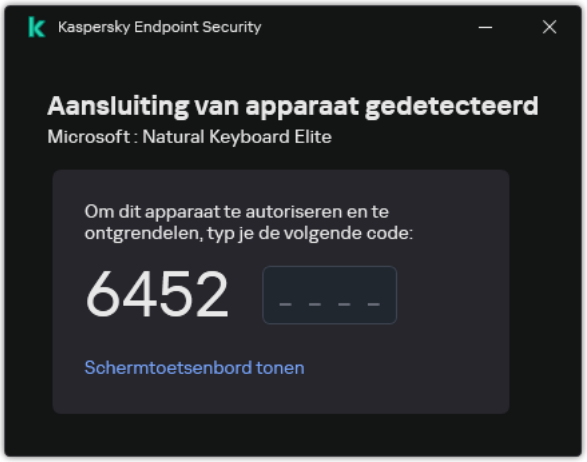
Als de code juist is ingevoerd, slaat het programma de identificatieparameters op (VID/PID van het toetsenbord en het nummer van de poort waarop het is aangesloten) in de lijst met geautoriseerde toetsenborden. U hoeft de toetsenbordautorisatie niet te herhalen wanneer het toetsenbord opnieuw wordt aangesloten of wanneer het besturingssysteem opnieuw wordt opgestart.

Wanneer het geautoriseerde toetsenbord op een andere USB-poort van de computer wordt aangesloten, wordt 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

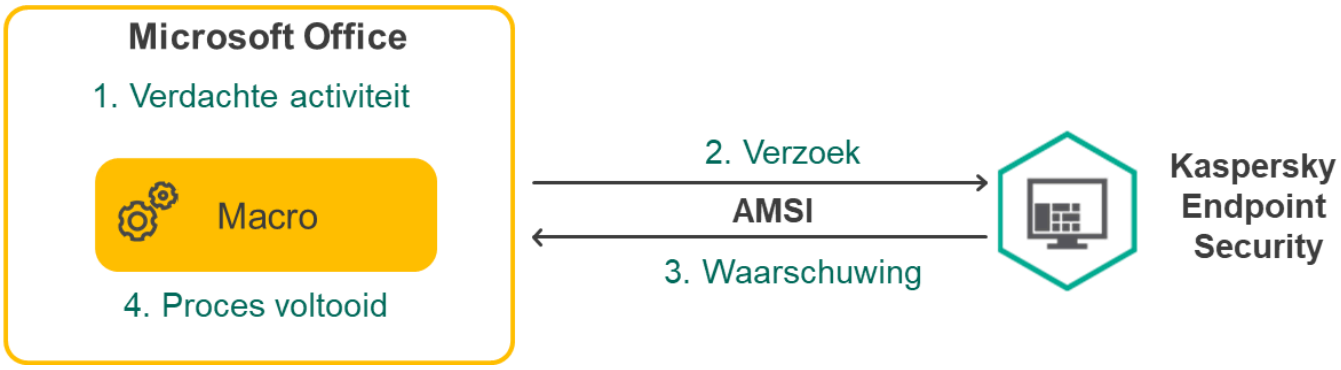
Instellingen van het onderdeel BadUSB Attack Prevention

Parameter	Beschrijving
Gebruik van Schermtoetsenbord voor autorisatie van USB-apparaten verbieden	Als de schakelaar is ingeschakeld, wordt het gebruik van Schermtoetsenbord voor de autorisatie van een USB-apparaat waarmee geen autorisatiecode kan worden ingevoerd geblokkeerd door het programma.
Verbied het gebruik van een streepjescode voor de autorisatie van USB-apparaten	Als het schakelaar is ingeschakeld, toont het programma de streepjescode niet in de verificatiemelding van de barcodescanner.
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 vijf pogingen voor de invoer van de autorisatiecode toestaat, blokkeert het programma het USB-apparaat na de vijfde mislukte poging. Kaspersky Endpoint Security toont hoelang het USB-apparaat geblokkeerd is. Na deze tijd krijgt u opnieuw vijf pogingen om de autorisatiecode in te voeren.
Time-out als het maximale aantal pogingen is bereikt	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. Een programma van een derde partij staat, na ontvangst van een melding van een dreiging, de kwaadaardige acties niet toe (bijvoorbeeld door de actie te beëindigen).



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 verstuurt 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 / Enterprise multi-sessie
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise
- Windows Server 2016 Essentials / Standard / Datacenter (including Server Core mode)
- Windows Server 2019 Essentials / Standard / Datacenter (including Server Core mode)
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (including Server Core mode)
- Windows Server 2025 Standard / Datacenter

Instellingen van AMSI-bescherming

Parameter	Beschrijving
Scan archieven	ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE en andere bestanden scannen. Het programma 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 (een archief in een archief).
Scan distributiepakketten	Distributiepakketten van programma's van derden scannen.
Scan Microsoft Office-bestanden	Scant Microsoft Office-bestanden (DOC, DOCX, XLS, PPT en andere Microsoft-extensies). Bestanden in Office-indeling bevatten ook OLE-objecten. Het programma scant office-bestanden die kleiner zijn dan 1 MB, ongeacht of het selectievakje is ingeschakeld of niet.
Pak grote samengestelde bestanden niet uit	Als dit selectievakje is ingeschakeld, scant het programma geen samengestelde bestanden als ze groter zijn dan de opgegeven waarde. Als dit selectievakje is uitgeschakeld, worden samengestelde bestanden van alle grootten gescand door het programma. Het programma 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.

Het onderdeel Exploit-preventie bewaakt bovendien netwerkpoorten op processen van programma's die de beveiliging van de computer kunnen bedreigen. Het programma verkrijgt informatie over dergelijke processen met antivirusdatabases.

Instellingen van het onderdeel Exploit-preventie

Parameter	Beschrijving
Bij detectie van exploit	**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.
Bescherming voor systeemprocessen in geheugen inschakelen	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 is gebaseerd op de definities van gedragspatronen en levert een proactieve bescherming voor de computer.

Het onderdeel Gedragsdetectie bewaakt bovendien netwerkpoorten op processen van programma's die de beveiliging van de computer kunnen bedreigen. Het programma verkrijgt informatie over dergelijke processen met antivirusdatabases.

Instellingen van het onderdeel Gedragsdetectie

Parameter	Beschrijving
Actie bij detectie van malwareactiviteit	**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. **Blokkeren**. Als deze optie wordt geselecteerd wanneer schadelijke activiteit wordt gedetecteerd, beëindigt Kaspersky Endpoint Security dit programma. **Melden**. 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.

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 (bijvoorbeeld bestanden en programma's)

De netwerkactiviteit van programma's wordt door het onderdeel firewall beheerd 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. Plaatst het programma in een van de vertrouwensgroepen: *Vertrouwd*, *Deels beperkt*, *Zeer beperkt*, *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 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
Programmarechten	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. 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. Toegangsrechten voor programma's worden weergegeven in de volgende tabellen: • **Bestanden en systeemregister**. Tabel met toegangsrechten voor bronnen van het besturingssysteem en persoonlijke gegevens voor programma's die behoren tot de vertrouwensgroep. • **Rechten**. Tabel met toegangsrechten voor processen en bronnen van het besturingssysteem voor programma's die behoren tot de vertrouwensgroep. • **Netwerkregels**. Een tabel met netwerkregels voor programma's die in een vertrouwensgroep zijn geplaatst. Firewall 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.
Beschermde bronnen	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.
Vertrouwensgroep voor programma's gestart vóór opstart van Kaspersky Endpoint Security	Een vertrouwensgroep waarin Kaspersky Endpoint Security programma's plaatst die eerder worden gestart dan Kaspersky Endpoint Security.
Werk regels voor eerder onbekende programma's bij vanaf KSN	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.
Vertrouw digitaal ondertekende programma's	Als dit selectievakje is ingeschakeld, plaatst het onderdeel Host Intrusion Prevention de digitale handtekening van vertrouwde leveranciers in de *Vertrouwd* groep. *Vertrouwde leveranciers* zijn de softwareleveranciers die Kaspersky vertrouwt. U kunt het leverancierscertificaat ook handmatig aan het vertrouwde certificaatarchief toevoegen. 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.

Parameter	Beschrijving
Verwijder regels voor programma's die niet zijn gestart de laatste N dagen (van 1 tot 90)	Als het selectievakje is ingeschakeld, verwijdert Kaspersky Endpoint Security automatisch informatie over het programma (vertrouwensgroep en toegangsrechten) indien aan de volgende voorwaarden wordt voldaan: • U hebt het programma handmatig in een vertrouwensgroep geplaatst of hebt de toegangsrechten ervan handmatig geconfigureerd. • Het programma is niet binnen de opgegeven periode gestart. 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. De volgende keer dat u dit programma start, analyseert Kaspersky Endpoint Security het programma alsof het voor de eerste keer wordt gestart.
Vertrouwensgroep voor programma's die niet in andere groepen zijn opgenomen	De opties in deze vervolgkeuzelijst bepalen aan welke vertrouwensgroep een onbekend programma wordt toegewezen door Kaspersky Endpoint Security. U kunt één van de volgende opties kiezen: • **Deels beperkt**. • **Zeer beperkt**. • **Niet vertrouwd**.

Remediation Engine

Via het onderdeel 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 geïnfiltreerd.
  - 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 malwarescan.

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.

KSN-functionaliteit is mogelijk niet beschikbaar in het programma in de Verenigde Staten.

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 het Kaspersky Security Network, voorzien de KSN-services Kaspersky Endpoint Security van informatie over de reputatie van gescande webadressen, evenals informatie over de categorie en reputatie van gescande bestanden. Voor meer informatie over het configureren van de toegang tot KSN raadpleeg de Help van Kaspersky Security Center.

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.

De infrastructuur van Kaspersky-reputatiedatabases

Kaspersky Endpoint Security ondersteunt de volgende infrastructuuroplossingen voor het werken met Kaspersky-reputatiedatabases:

- *Kaspersky Security Network (KSN)* is de oplossing die door de meeste Kaspersky-programma's wordt gebruikt. Deelnemers aan KSN ontvangen informatie van Kaspersky 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-databases die reputatie-informatie en statistische gegevens bevatten.

- *Kaspersky Private Security Network (KPSN)* is een oplossing waarmee gebruikers van computers waarop Kaspersky Endpoint Security of andere Kaspersky-programma's worden gehost toegang krijgen tot reputatiedatabases van Kaspersky en tot andere statistische gegevens zonder gegevens naar Kaspersky te versturen vanaf hun eigen computers. KPSN 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.

Instellingen van Kaspersky Security Network

Parameter	Beschrijving
Uitgebreide KSN-modus inschakelen	De *uitgebreide KSN-modus* is een modus waarin Kaspersky Endpoint Security aanvullende gegevens naar Kaspersky verstuurt. Kaspersky Endpoint Security gebruikt KSN om dreigingen te detecteren, ongeacht de schakelpositie.
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. 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. Kaspersky Endpoint Security downloadt de beperkte versie van de antivirusdatabases tijdens de volgende update nadat u het selectievakje hebt ingeschakeld. Als de schakelaar is uitgeschakeld, gebruikt Kaspersky Endpoint Security de complete versie van de antivirusdatabases. Kaspersky Endpoint Security downloadt de complete versie van de antivirusdatabases tijdens de volgende update nadat u het selectievakje hebt uitgeschakeld.
Computerstatus wanneer KSN-servers niet beschikbaar zijn *(alleen beschikbaar in de Kaspersky Security Center-console)*	De opties in deze vervolgkeuzelijst bepalen de status van een computer in Kaspersky Security Center wanneer de KSN-servers niet beschikbaar zijn.

Parameter	Beschrijving
Gebruik Administration Server als een KSN-proxyserver *(alleen beschikbaar in de Kaspersky Security Center-console)*	Als het selectievakje is ingeschakeld, gebruikt Kaspersky Endpoint Security de service KSN-proxy. U kunt de instellingen van de KSN-proxyservice configureren in de eigenschappen van Administration Server.
Gebruik Kaspersky Security Network-servers als de KSN-proxyserver niet beschikbaar is *(alleen beschikbaar in de Kaspersky Security Center-console)*	Als het selectievakje is ingeschakeld, gebruikt Kaspersky Endpoint Security KSN-servers wanneer de KSN Proxy service niet beschikbaar is. KSN-servers kunnen zowel van Kaspersky als van derden (wanneer privaat KSN wordt gebruikt) zijn.

Log Inspectie

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

Vanaf versie 11.11.0 omvat Kaspersky Endpoint Security voor Windows het onderdeel Log Inspectie. Log Inspectie bewaakt de integriteit van de beschermde omgeving op basis van de inspectiere van het Windows-gebeurtenislogboek. Wanneer het programma tekenen van atypisch gedrag in het systeem detecteert, informeert het de beheerder, omdat dit gedrag kan wijzen op een poging tot cyberaanval.

Kaspersky Endpoint Security analyseert Windows-gebeurtenislogboeken en detecteert overtreding van de regels. De component bevat voorgedefinieerde regels. Voorgedefinieerde regels worden aangedreven door heuristische analyse. U kunt ook uw eigen regels toevoegen (aangepaste regels). Wanneer een regel wordt geactiveerd, maakt hete programma een gebeurtenis met de status *Critical* (zie onderstaande afbeelding).

Als u log inspectie wilt gebruiken, zorg er dan voor dat de beveiligingsinstellingen van het auditbeleid zijn geconfigureerd en dat het systeem de relevante gebeurtenissen vastlegt (raadpleeg de technische ondersteuningswebsite van Microsoft voor details).



Melding log inspectie

Parameter	Beschrijving
Voorgedefinieerde regels	Lijst van regels voor log inspectie Voorgedefinieerde regels bevatten sjablonen van abnormale activiteit op de beveiligde computer. Abnormale activiteit kan een poging tot aanval omvatten.
Aangepaste regels	Lijst van regels voor log inspectie toegevoegd door de gebruiker. U kunt uw eigen activeringscriteria voor Log inspectie regels instellen. Hiervoor moet je een gebeurtenis-ID invoeren en een gebeurtenisbron selecteren. U kunt een gebeurtenisbron selecteren uit de standaardlogboeken: *Application*, *Security* or *System*. U kunt ook het logboek van een programma van derden specificeren.

Anti-Cryptor

Het onderdeel Anti-Cryptor 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.

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.

Parameter	Beschrijving
Uitzonderingen op naam of IP-adres	**Uitzonderingen op naam of IP-adres**. 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. **Uitzonderingen door masker**. Uitzonderingen voor beschermd bereik. Het uitsluiten van een map van het beschermd bereik 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. 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:\Folder\**\*.txt` omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen bevinden genest in de `Folder`, uitgezonderd de `Folder` 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:\Folder\???.txt` omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam `Folder` bevinden, die een TXT-extensie hebben en die een naam met drie tekens hebben.
Actie bij detectie van een dreiging	• **Melden**. Als deze optie is geselecteerd, voegt Kaspersky Endpoint Security bij het detecteren van een poging om bestanden in gedeelde mappen te wijzigen, informatie over deze poging toe aan de lijst met actieve bedreigingen, voegt een item toe aan lokale programma-interface rapporten en stuurt informatie over de gedetecteerde kwaadaardige activiteit naar Kaspersky Security Center. • **Verbinding blokkeren voor (min) N min**. Als Kaspersky Endpoint Security een poging tot wijziging van bestanden in gedeelde mappen detecteert wanneer deze optie is geselecteerd, blokkeert het toegang tot bestandswijziging voor de sessie die de kwaadaardige activiteit heeft gestart en maakt back-ups van de gewijzigde bestanden. Als het onderdeel Remediation Engine is ingeschakeld en de optie **Verbinding blokkeren voor (min) N min** is geselecteerd, worden gewijzigde bestanden teruggezet vanuit back-ups.
Beschermd bereik	Het *beschermd bereik* is een lijst met paden naar gedeelde mappen waarin Kaspersky Endpoint Security de bestandsactiviteit controleert. Kaspersky Endpoint Security ondersteunt omgevingsvariabelen en de `*` en `?`-tekens bij het invoeren van een masker. Standaard identificeert het programma automatisch gedeelde mappen en controleert de bestandsactiviteit in alle mappen.

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).

Om Webcontrole te kunnen gebruiken, moet u de initiële configuratie van het programma voltooien:

- Voor de bewaking van HTTPS-verkeer, schakel het scannen van versleutelde verbindingen in (standaard ingeschakeld).
- Selecteer de poorten die: Kaspersky Endpoint Security moet monitoren (standaard bewaakt het programma alle poorten).

- Selecteer het programma waarvan u wilt dat Kaspersky Endpoint Security het verkeer bewaakt. De meeste browsers staan al in de lijst met door Kaspersky aanbevolen programma's. Als uw browser niet in de lijst staat, kunt u deze handmatig toevoegen.

- Wij adviseren om een script voor webpagina-interactie in het webverkeer te injecteren (scriptinjectie is standaard uitgeschakeld). Met dit script kunnen Webcontrole-gebeurtenissen voor het programmagebeurtenislogboek, het OS-gebeurtenislogboek en rapporten worden geregistreerd.

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 *Afbeeldingen*.

- **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-programmabestanden* 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.



Berichten van Webcontrole

Parameter	Beschrijving
Toegangsregels voor webbronnen	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.
Standaardregel	De *Standaardregel* is een regel voor toegang tot webbronnen die niet in andere regels is vastgelegd. De volgende opties zijn beschikbaar: • **Alles toestaan behalve de regellijst**, ook wel als de denylist-modus voor verboden websites genoemd. • **Alles weigeren behalve de regellijst**, ook wel de allowlist-modus voor toegestane websites genoemd.
Beëindig actieve browsersessies van gebruikers nadat de regel is toegepast	Als het selectievakje is ingeschakeld, beëindigt Webcontrole de verbinding met geblokkeerde webbronnen onmiddellijk nadat het beleid is toegepast. De browser stopt onmiddellijk met het downloaden van gegevens van de webpagina. Wanneer u de webpagina vernieuwt of naar een andere verboden webpagina gaat, toont het programma een waarschuwing. Met Webcontrole kunt u alleen in webbrowsers de verbinding met webbronnen onmiddellijk verbreken. Voor andere programma's beperkt Webcontrole alleen nieuwe verbindingen. Als het selectievakje is uitgeschakeld, beperkt Webcontrole alleen nieuwe verbindingen met verboden webbronnen. Webcontrole beëindigt geen actieve verbindingen.
Sjablonen	**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. Er zijn speciale variabelen voorzien voor het beheer van de berichtsjablonen (bijvoorbeeld `%USER_NAME%`). Met variabelen kan één berichtsjabloon voor verschillende computers worden gebruikt.
Registreer het openen van toegestane pagina's	Kaspersky Endpoint Security registreert gegevens over bezoeken aan websites, waaronder toegestane websites. Kaspersky Endpoint Security verstuurt gebeurtenissen naar Kaspersky Security Center, naar het lokale logboek van Kaspersky Endpoint Security en naar het Windows-gebeurtenislogboek. Als u de activiteit van gebruikers op het internet wilt bewaken, moet u de instellingen voor het opslaan van gebeurtenissen configureren. 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. De bewaking van de activiteit van gebruikers op het internet vereist meer computerbronnen bij de decryptie van HTTPS-verkeer.

Apparaatcontrole

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

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 **Advanced** → **Repositories** → **Hardware**.

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 – .
  - Volgens regels (alleen printers en draagbare apparaten) – .
  - Afhankelijk van verbindingsbus (behalve wifi) – .
  - Blokkeren met uitzonderingen (alleen wifi) – .

- **Verbindingsbus**. Een *verbindingsbus* is een interface voor de aansluiting van apparaten op de computer (bijvoorbeeld USB of FireWire). Als **Afhankelijk van verbindingsbus** modus is geselecteerd voor het apparaattype, staat het programma de toegang tot het apparaat toe of weigert afhankelijk van de verbindings-interface (bijv. 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.

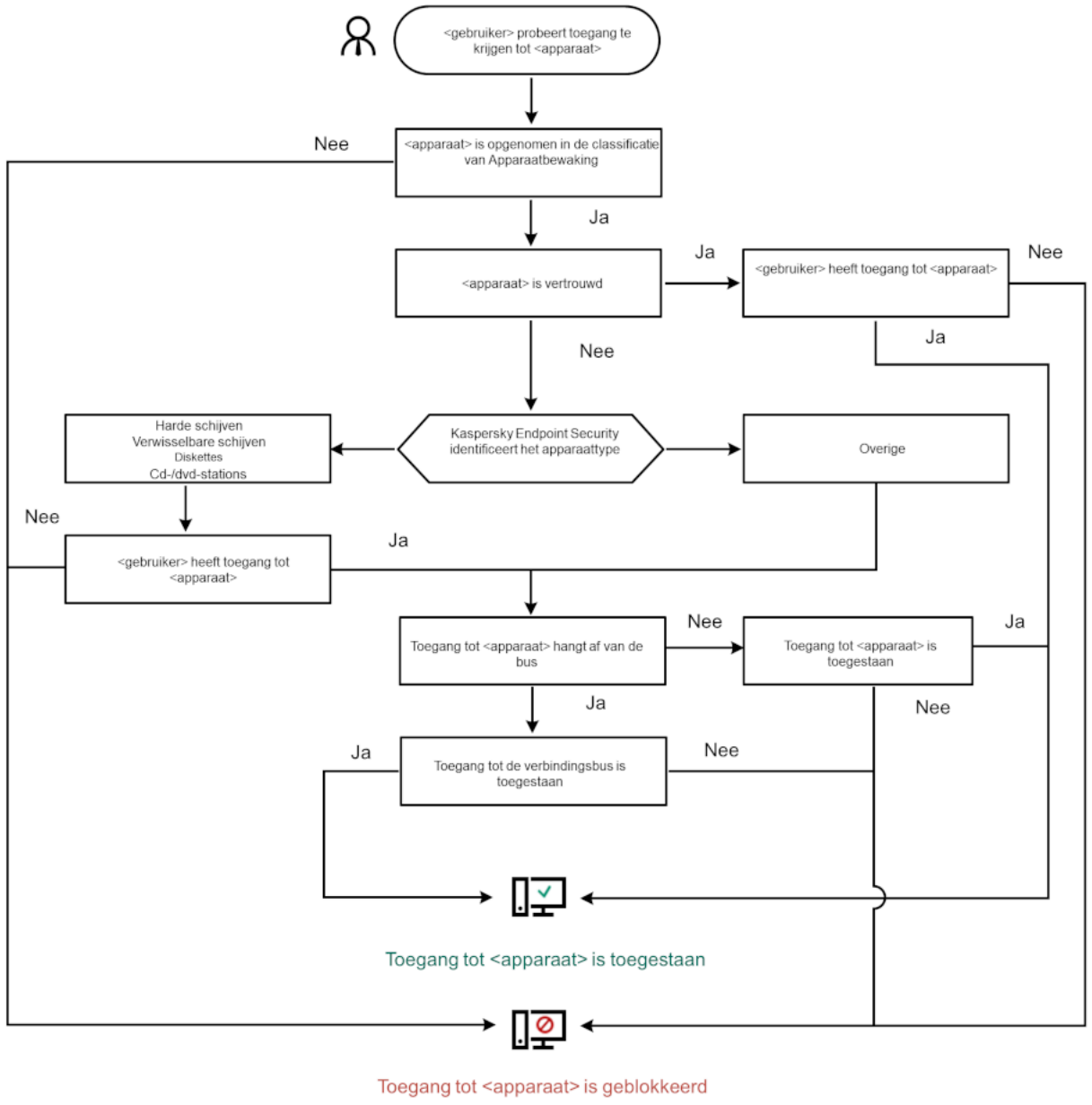
Wanneer een apparaat dat wordt geblokkeerd door Apparaatcontrole wordt aangesloten op de computer, blokkeert Kaspersky Endpoint Security de toegang en toont het een melding (zie onderstaande afbeelding).



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.

Parameter	Beschrijving
Aanvragen voor tijdelijke toegang toestaan *(alleen beschikbaar in de Kaspersky Security Center-console)*	Als het selectievakje is ingeschakeld, wordt de knop **Toegang vragen** in de lokale interface van Kaspersky Endpoint Security weergegeven. Met deze knop kan de gebruiker tijdelijke toegang tot een geblokkeerd apparaat aanvragen.
Apparaten en wifinetwerken	In deze tabel ziet u alle mogelijke soorten apparaten volgens de classificatie van het onderdeel Apparaatcontrole, inclusief de respectieve toegangsstatus.
Verbindingsbussen	Een lijst met alle beschikbare verbindingsbussen volgens de classificatie van Apparaatcontrole, inclusief de respectieve toegangsstatus. Kaspersky Endpoint Security staat wel of geen toegang tot apparaten toe, afhankelijk van het type verbindingsbus als: **Afhankelijk van verbindingsbus** modus is geselecteerd.
Vertrouwde apparaten	Lijst met vertrouwde apparaten en gebruikers die toegang hebben tot deze apparaten.
Waarden samenvoegen bij overname *(alleen beschikbaar in de Kaspersky Security Center-console)*	Hiermee wordt de lijst met vertrouwde apparaten 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. 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 apparaten voor de hele organisatie maken. Overgenomen lijstitems in een onderliggend beleid kunnen niet worden verwijderd of bewerkt. Items op de lijst met vertrouwde apparaten 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. Als items op lijsten van het onderliggende beleid en het bovenliggende beleid overeenkomen, worden deze items weergegeven als hetzelfde item van het bovenliggende beleid. Als het selectievakje is uitgeschakeld, worden items van lijsten niet samengevoegd wanneer de instellingen van het Kaspersky Security Center-beleid worden overgenomen. Met deze functie kunt u ook lijsten in beleidsprofielen samenvoegen. Als u lijsten wilt samenvoegen, schakelt u in het profiel met de hoogste prioriteit de overname van instellingen van een profiel met een lagere prioriteit in. Voor meer informatie over beleidsprofiel-prioriteiten, raadpleegt u de Help van Kaspersky Security Center.
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 blokkeert het maken van meerdere verbindingen volgens de prioriteiten van apparaten. Hoe hoger een apparaat in de lijst staat, hoe hoger de prioriteit ervan. 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. 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. Anti-Bridging ondersteunt de volgende soorten apparaten: netwerkadapter, wifi en modem.
Berichtsjablonen	**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.

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* of een andere categorie), 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. De beheerder kan veel regels maken. Eén programma kan voldoen aan de criteria van meerdere regels. De prioriteit van een Blokkeren-regel is hoger dan die van een Toestaan-regel. Telkens wanneer het programma wordt gestart, controleert Kaspersky Endpoint Security of een programma overeenkomt met een regel. Kaspersky Endpoint Security vergelijkt het programma achtereenvolgens met alle regels van Programmacontrole.

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.

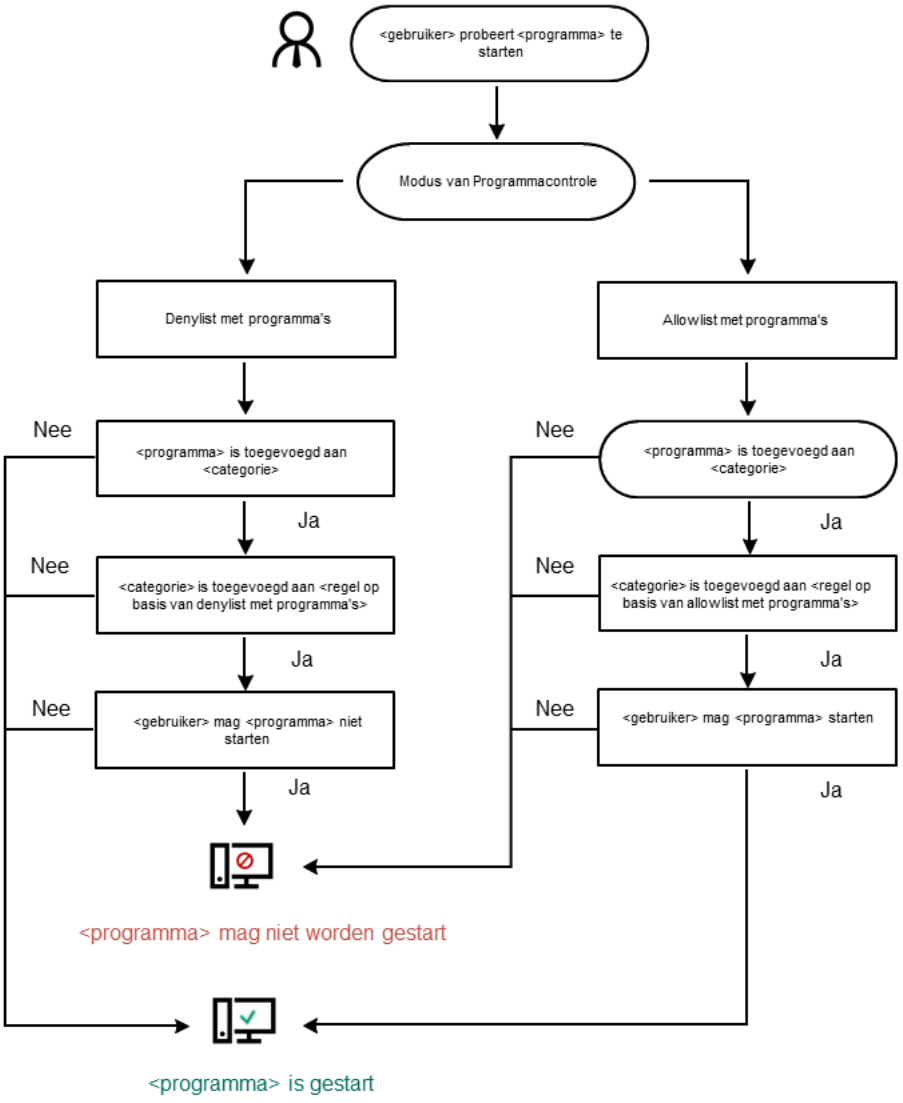
  De regels van Programmacontrole die worden aangemaakt in de Beheerconsole van Kaspersky Security Center zijn gebaseerd op aangepaste categorieën van programma's en niet op uitvoerings- of uitzonderingsvoorwaarden zoals in de lokale interface van Kaspersky Endpoint Security.

- 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

Parameter	Beschrijving
Actie op startende aanvragen geblokkeerd door regels	**Regels toepassen**. Kaspersky Endpoint Security beheert het opstarten van programma's volgens de geselecteerde modus. **Regels testen**. Kaspersky Endpoint Security staat toe dat een programma dat wordt geblokkeerd in de huidige modus van Programmacontrole wordt gestart, maar registreert het informatie over de opstart van dat programma in het rapport.
Modus van Controle van programma-opstart	U kunt één van de volgende opties kiezen: • **Denylist**. Als deze optie is geselecteerd, staat Programmacontrole toe dat alle gebruikers programma's kunnen starten, behalve in gevallen die voldoen aan de voorwaarden van de blokkeringsregels van Programmacontrole. • **Allowlist**. Als deze optie is geselecteerd, staat Programmacontrole niet toe dat gebruikers een programma starten, behalve in gevallen waarbij aan de voorwaarden van de uitvoeringsregels van Programmacontrole is voldaan. Wanneer de modus **Allowlist** is geselecteerd, worden twee regels van Programmacontrole automatisch aangemaakt: • **Golden Image**. • **Vertrouwde updaters**. U kunt de instellingen van automatisch aangemaakte regels niet bewerken, noch kunt u die regels verwijderen. U kunt deze regels inschakelen of uitschakelen.
Controleer het laden van DLL-modules	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. 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 "**Golden Image\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. 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 degene die zijn geladen voordat Kaspersky Endpoint Security opstart.
Strikte digitale-handtekeningsverificatie gebruiken	U kunt een certificaat selecteren als activerende voorwaarden voor een programmacontrole-regel. Als dit selectievakje is ingeschakeld, past Kaspersky Endpoint Security regels toe op programma's die alleen zijn ondertekend met certificaten uit het vertrouwde certificaatarchief van het systeem. Programma's die met een dergelijk certificaat zijn ondertekend, worden ook door de beschermingsonderdelen, bijvoorbeeld de *Malware-scan*-taak, als vertrouwd beschouwd. Als u echter een certificaat uit een ander archief opgeeft in een programmacontrole-regel, past Kaspersky Endpoint Security een dergelijke regel niet toe. Als het selectievakje is uitgeschakeld, past Kaspersky Endpoint Security regels toe op programma's die zijn ondertekend door een certificaat uit het Windows Trusted Root Certificate Store. Dergelijke programma's maken geen deel uit van de vertrouwde zone. Beschermingsonderdelen bewaken de activiteit van dergelijke programma's.
Sjablonen van berichten over programmablokkering	**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. **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.

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 **Rule triggers in Smart Training state**.

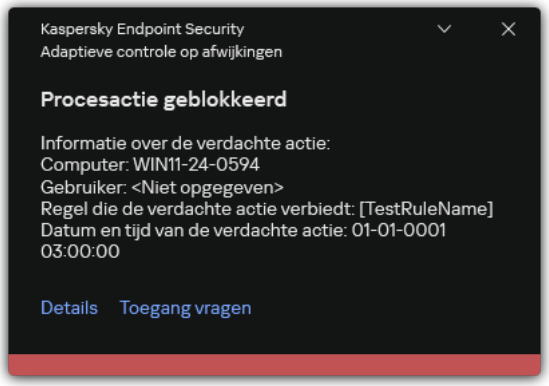
2. Rapport over activering van regels analyseren.

   De beheerder analyseert het rapport over de activering van regels of de inhoud van de opslagplaats **Rule triggers 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 via de volgende kanalen geconfigureerd:

- Adaptieve controle op afwijkingen begint automatisch 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 **Rule triggers in Smart Training state**. We raden aan dat u het rapport over het activeren van regels en de inhoud van de **Rule triggers in Smart Training state** opslag controleert.

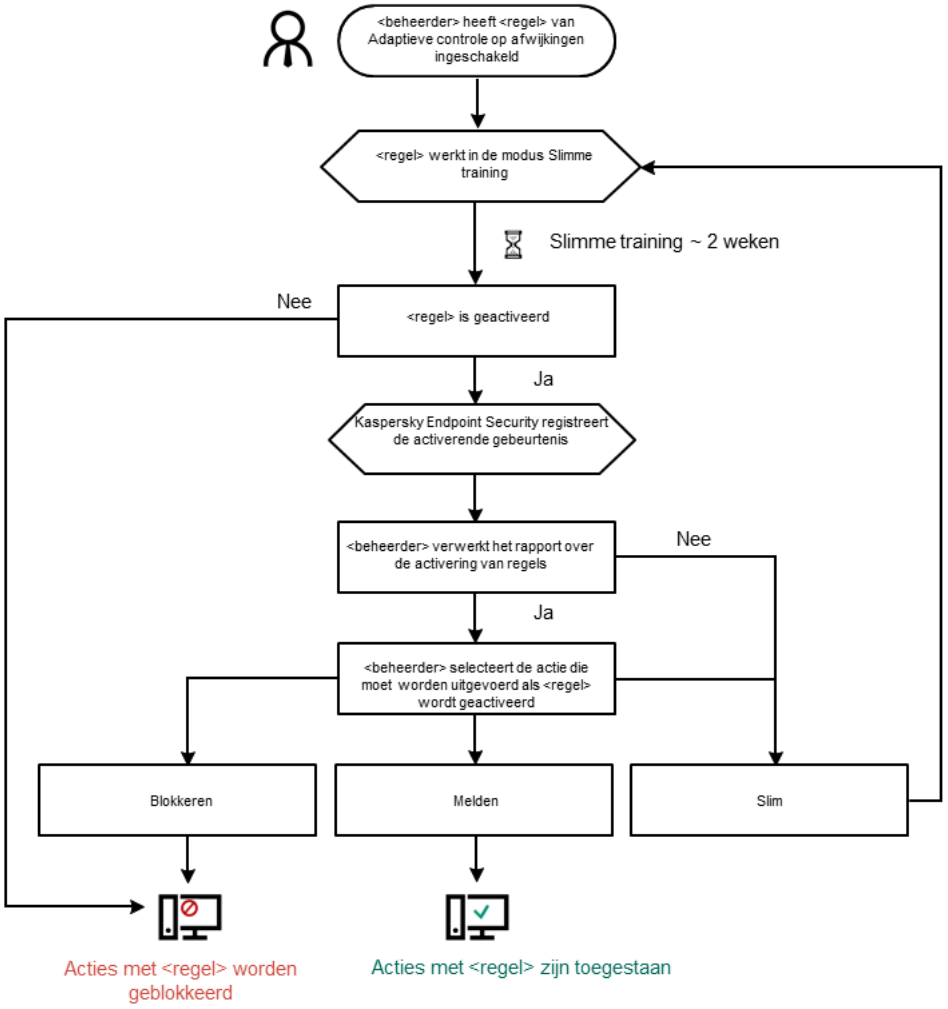
Wanneer een schadelijk programma een actie probeert uit te voeren, blokkeert Kaspersky Endpoint Security de actie en toont het een melding (zie onderstaande afbeelding).



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

Parameter	Beschrijving
Rapport over de status van de regels van Adaptieve controle op afwijkingen *(alleen beschikbaar in de Kaspersky Security Center-console)*	Dit rapport bevat informatie over de status van de detectieregels van Adaptieve controle op afwijkingen (bijvoorbeeld *Uitgeschakeld* of *Blokkeren*). Het rapport wordt voor alle beheergroepen gegenereerd.
Rapport over geactiveerde regels van Adaptieve controle op afwijkingen *(alleen beschikbaar in de Kaspersky Security Center-console)*	Dit rapport bevat informatie over afwijkende acties die door Adaptieve controle op afwijkingen zijn gedetecteerd. Het rapport wordt voor alle beheergroepen gegenereerd.
Regels	Tabel met regels voor Adaptieve controle op afwijkingen. Regels worden door Kaspersky-experts gemaakt op basis van kenmerkende scenario's van malware-activiteit.
Sjablonen	**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.

Systeemintegriteitscontrole

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

Vanaf versie 12.6, omvat Kaspersky Endpoint Security voor Windows het onderdeel Systeemintegriteitscontrole in plaats van de Bestandsintegriteitsmonitor onderdeel. Het onderdeel Systeemintegriteitscontrole omvat alle functionaliteit van Bestandsintegriteitsmonitor en maakt het bovendien mogelijk om registerwijzigingen en de aansluiting van externe apparaten te monitoren.

Het onderdeel Systeemintegriteitscontrole bewaakt veranderingen in het besturingssysteem die kunnen wijzen op inbreuken op de beveiliging van de computer. Wanneer dergelijke wijzigingen worden gedetecteerd, genereert Kaspersky Endpoint Security overeenkomstige gebeurtenissen en waarschuwt de beheerder. Systeemintegriteitscontrole kan in realtime werken en kan op verzoek ook Systeemintegriteitscheck uitvoeren.

Realtime systeemintegriteitscontrole

In realtime-modus, Systeemintegriteitscontrole houdt wijzigingen bij in objecten die u hebt opgenomen in het bereik van de onderdelen (de *bewakingsbereik*). Met Systeemintegriteitscontrole kan ook ongeautoriseerde toegang tot dergelijke objecten in realtime worden geblokkeerd.

On-demand systeemintegriteitscontrole

On-demand systeemintegriteitscontrole is een taak die u handmatig of volgens een schema kunt uitvoeren. Om de uit te voeren *Systeemintegriteitscheck* taak, moet u het bereik van het onderdeel configureren (de *bewakingsbereik*) en maak een basislijn. Een *basislijn* is een geregistreerde staat van objecten in het systeem, die het programma als referentie gebruikt bij het vergelijken met de huidige staat.

Systeemintegriteitscontrole instellingen

Parameter	Beschrijving
Uitvoermodus voor het blokkeren van regels	• **Blokkeren**. In deze modus blokkeert Systeemintegriteitscontrole acties met bestanden en registersleutels uit het bewakingsbereik en genereert het een overeenkomstige gebeurtenis. • **Melden**. In deze modus staat Systeemintegriteitscontrole acties toe met bestanden en registersleutels uit het bewakingsbereik en genereert het een overeenkomstige gebeurtenis.
Realtime Systeemintegriteitscontrole	In realtime-modus, Systeemintegriteitscontrole houdt wijzigingen bij in objecten die u hebt opgenomen in het bereik van de onderdelen (de *bewakingsbereik*). Met Systeemintegriteitscontrole kan ook ongeautoriseerde toegang tot dergelijke objecten in realtime worden geblokkeerd.
Bewaak apparaten	Systeemintegriteitscontrole bewaakt het aansluiten en loskoppelen van externe apparaten.
Bewaak bestanden en het register	Systeemintegriteitscontrole controleert wijzigingen in bestanden, mappen en register.
Systeemintegriteitscheck	On-demand systeemintegriteitscontrole is een taak die u handmatig of volgens een schema kunt uitvoeren. Om de uit te voeren *Systeemintegriteitscheck* taak, moet u het bereik van het onderdeel configureren (de *bewakingsbereik*) en maak een basislijn. Een *basislijn* is een geregistreerde staat van objecten in het systeem, die het programma als referentie gebruikt bij het vergelijken met de huidige staat.

Endpoint Sensor

Endpoint Sensor is geen onderdeel van Kaspersky Endpoint Security 11.4.0.

U kunt de Endpoint Sensor beheren 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 beheren.

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 drie functionele eenheden:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

U kunt alle functionele eenheden of afzonderlijke functionele eenheden afzonderlijk kopen. 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 8.1.1 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.

Sandbox

Kaspersky Endpoint Security for Windows heeft een ingebouwde agent voor integratie met de Kaspersky Sandbox-oplossing. Het *Sandbox*-onderdeel detecteert en blokkeert automatisch geavanceerde dreigingen op computers. Sandbox analyseert het gedrag van objecten om schadelijke activiteit en activiteit kenmerkend voor doelgerichte aanvallen op de IT-infrastructuur van het bedrijf te detecteren. Sandbox analyseert en scant objecten op speciale servers met geïmplementeerde virtuele kopieën van Microsoft Windows-besturingssystemen (Sandbox-servers). Voor informatie over de oplossing raadpleeg de Help van Kaspersky Sandbox en Help van Kaspersky Anti Targeted Attack Platform.

Vanaf versie 12.7 ondersteunt Kaspersky Endpoint Security for Windows het onderdeel Sandbox die deel uitmaakt van de Kaspersky Anti Targeted Attack Platform-oplossing. In tegenstelling tot de Kaspersky Sandbox-oplossing, staat het KATA Sandbox-onderdeel het scannen van bestanden niet alleen automatisch toe, maar ook handmatig vanuit het bestandscontextmenu.

Voor de implementatie van KATA Sandbox is Kaspersky Anti Targeted Attack Platform 7.0 of hoger vereist.

Het onderdeel kan alleen worden beheerd met behulp van de Kaspersky Security Center-webconsole. U kunt dit onderdeel niet beheren met de Beheerconsole (MMC).

Sandbox-componentinstellingen

Parameter	Beschrijving
Integration mode	**Kaspersky Sandbox**. Integratie met Kaspersky Sandbox-oplossing. Het programma verstuurt bestanden die moeten worden gescand in Kaspersky Sandbox alleen in de automatische modus. **KATA Sandbox**. Integratie met het onderdeel Sandbox van de Kaspersky Anti Targeted Attack Platform-oplossing. U kunt de modus insturen van bestanden om te scannen selecteren: • **Manually**. De gebruiker stuurt het bestand handmatig in voor scannen vanuit het contextmenu (**Verzenden naar Sandbox**). • **Automatically**. Het programma detecteert automatisch objecten en stuurt ze in naar Sandbox om ze te scannen. • **Combined**.
Server connection settings	**Timeout (msec)**. Time-out van verbinding voor de Sandbox-server (voor Kaspersky Sandbox) of Central Node-server (voor KATA). Nadat de geconfigureerde time-out is verstreken, stuurt Kaspersky Endpoint Security een verzoek naar de volgende server. U kunt de verbindingstime-out voor de server verlengen als uw verbindingssnelheid laag is of als de verbinding onstabiel is. De aanbevolen timeout voor een aanvraag is 0,5 seconden of minder. **Request queue**. Grootte van de verzoekwachtrijmap. Bij het verzenden van meerdere objecten om te scannen in Sandbox, maakt Kaspersky Endpoint Security een wachtrij voor aanvragen. Standaard is de grootte van de verzoekwachtrijmap beperkt tot 100 MB. Nadat de maximale grootte is bereikt, stopt 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. **Server TLS certificate**. Als u een vertrouwde verbinding met de Sandbox-server (voor Kaspersky Sandbox) of Central Node server (voor KATA) wilt configureren, moet u een TLS-certificaat voorbereiden. Vervolgens moet u het certificaat met behulp van een beleid aan de computer toevoegen. U moet het certificaat ook toevoegen aan de Sandbox-server (voor Kaspersky Sandbox) of Central Node server (voor KATA). **Use two-way authentication** (alleen voor KATA Sandbox). Tweerichtingsverificatie bij het tot stand brengen van een beveiligde verbinding tussen Kaspersky Endpoint Security en de Central Node-server. Om tweerichtingsverificatie te gebruiken, moet u tweerichtingsverificatie inschakelen in de Central Node-server instellingen, vervolgens een crypto-container ophalen en een wachtwoord instellen om de crypto-container te beschermen. Een *crypto-container* is een PFX-archief met een certificaat en een privésleutel. U kunt een crypto-container verkrijgen in de Kaspersky Anti Targeted Attack Platform-console (zie de instructies in de Help van Kaspersky Anti Targeted Attack Platform). Na het configureren van de Central Node-instellingen, moet u ook tweerichtingsverificatie inschakelen in de instellingen van Kaspersky Endpoint Security en een met een wachtwoord beveiligde crypto-container laden.
Connection to Sandbox servers	**Kaspersky Sandbox**. Sandbox server-verbindingsinstellingen. 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. **KATA Sandbox**. Verbindingsinstellingen voor de Central Node-server. Central Node kiest optimale instellingen voor het scannen en verdeelt de belasting tussen Sandbox-servers.
Action on threat detection	**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 Critical Areas Scan**. Als deze optie is geselecteerd, start Kaspersky Endpoint Security de taak *Critical Areas Scan*. Standaard scant Kaspersky Endpoint Security het kernelgeheugen, actieve processen en de opstartsectoren van de schijf. **Create IOC Scan task**. Als deze optie geselecteerd is, maakt Kaspersky Endpoint Security automatisch de *IOC Scan (autonomen IOC-scantaak)*. Voor deze taak kunt u de uitvoermodus, het scanbereik en de actie voor IOC-detectie configureren (*Move copy to Quarantine, delete object* of *Run Critical Areas Scan*). Om andere instellingen van de *IOC Scan* taak te wijzigen, gaat u naar de taakinstellingen.
IOC Scan scope	**Critical file areas**. Als deze optie geselecteerd is, voert Kaspersky Endpoint Security alleen een IOC-scan uit in kritieke bestandsgebieden van de computer: kernelgeheugen en opstartsectoren. **File areas on system drive of the computer**. Als deze optie geselecteerd is, voert Kaspersky Endpoint Security een IOC-scan uit op het systeemstation van de computer.

Parameter	Beschrijving
Run IOC Scan task	**Manually**. Uitvoeringsmodus waarin u de *IOC Scan* handmatig kunt starten op een moment dat u uitkomt. **Automatically**. Uitvoermodus waarin Kaspersky Endpoint Security de *IOC Scan* taak automatisch wordt uitgevoerd nadat een dreiging wordt gedetecteerd. **Run only when the computer is idle**. Uitvoermodus waarin Kaspersky Endpoint Security de *IOC-scan* taak uitvoert als de screensaver actief is of het scherm wordt vergrendeld. Als de gebruiker de computer ontgrendelt, pauzeert Kaspersky Endpoint Security de scantaak. Dit betekent dat de taak enkele dagen in beslag kan nemen.

Managed Detection and Response

Kaspersky Endpoint Security voor Windows ondersteunt integratie met 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.

Instellingen Managed Detection and Response

Parameter	Beschrijving
MDR-configuratiebestand	Het BLOB-bestand bevat de client-ID en informatie over de licentie voor Kaspersky Managed Detection and Response. Het BLOB-bestand bevindt zich in het ZIP-archief van het MDR-configuratiebestand. U kunt het Ziparchief verkrijgen in de Kaspersky Managed Detection and Response-console. Raadpleeg de Help van Kaspersky Managed Detection and Response voor gedetailleerde informatie over een BLOB-bestand.

Endpoint Detection and Response

Kaspersky Endpoint Security for Windows heeft een ingebouwde agent voor de Kaspersky Endpoint Detection and Response Optimum-oplossing (hierna ook "EDR Optimum"). Vanaf versie 11.8.0 bevat Kaspersky Endpoint Security for Windows 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. Een *Waarschuwing* is een gebeurtenis in de IT-infrastructuur van het bedrijf die door het programma is geïdentificeerd als ongebruikelijk of verdacht en die een beveiligingsrisico kan vormen voor de IT-infrastructuur van het bedrijf. *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 Endpoint Detection and Response Optimum component configureren in Webconsole en Cloud Console. De instellingen voor de onderdelen Endpoint Detection and Response Expert (cloud) izijn alleen beschikbaar in Cloudconsole.

Instellingen Endpoint Detection and Response

Parameter	Beschrijving
Enable advanced system activity logging	Uitgebreide telemetrie verbetert de nauwkeurigheid van IOC-detectie, maar gebruikt meer bronnen van de computer. We raden aan om uitgebreide telemetrie op de computer in te schakelen voor retrospectieve IOC-scans. *Retrospectieve IOC-scan* is een modus van de *IOC Scan* taak waarbij Kaspersky Endpoint Security gedurende een bepaalde periode scant op indicatoren van besmetting met behulp van gegevens. Deze modus is bedoeld voor het zoeken naar indicatoren van besmetting door de telemetrie van de beschermde computer, zoals netwerkactiviteit, processen, bestanden en andere telemetriegegevens. Als uitgebreide telemetrie is uitgeschakeld, kan Kaspersky Endpoint Security de informatie over gedetecteerde indicatoren van een besmetting rouleren.
Network Isolation	Automatische isolatie van de computer van het netwerk als reactie op gedetecteerde bedreigingen. 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: • Verbindingen die worden vermeld in uitzonderingen voor netwerkisolatie. • Verbindingen gestart door Kaspersky Endpoint Security-services. • Verbindingen gestart door de Kaspersky Security Center Netwerkagent.
Automatically unlock isolated device in (hours)	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.
Network isolation exclusions	Lijst van regels voor uitzonderingen van netwerkisolatie. Netwerkverbindingen die overeenkomen met de regels, worden niet geblokkeerd op computers 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. 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.
Execution Prevention	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 een reeks office-bestandsextensies en een reeks scriptinterpreters. Als u de component Preventie van uitvoering wilt gebruiken, moet u regels voor preventie van uitvoering toevoegen. *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.

Parameter	Beschrijving
Action on execution or opening of forbidden object	**Block and add to event log**. 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. **Add to event log**. 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.
Execution prevention rules	*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.
Cloud Sandbox	*Cloud Sandbox* is een technologie waarmee u geavanceerde bedreigingen op een computer kunt detecteren. Kaspersky Endpoint Security stuurt gedetecteerde bestanden automatisch door naar Cloud Sandbox voor analyse. Cloud Sandbox voert deze bestanden uit in een geïsoleerde omgeving om kwaadaardige activiteiten te identificeren en over hun reputatie te beslissen. Gegevens over deze bestanden worden vervolgens naar Kaspersky Security Network verzonden. Als Cloud Sandbox daarom een kwaadaardig bestand heeft gedetecteerd, zal Kaspersky Endpoint Security de juiste actie ondernemen om deze bedreiging te elimineren op alle computers waarop dit bestand wordt gedetecteerd. Cloud Sandbox-technologie is permanent ingeschakeld en is beschikbaar voor alle gebruikers van Kaspersky Security Network, ongeacht het type licentie dat ze gebruiken. Als dit selectievakje is ingeschakeld, zal Kaspersky Endpoint Security de teller inschakelen voor gedetecteerde dreigingen met Cloud Sandbox in het hoofdvenster van het programma onder **Technologieën voor detectie van dreigingen**. Kaspersky Endpoint Security zal ook Cloud Sandbox-technologie aangeven in programmagebeurtenissen en in het *Report on threats* in de Kaspersky Security Center-console.

Endpoint Detection and Response Expert (on-premises)

Endpoint Detection and Response Expert (on-premises)

Kaspersky Endpoint Security voor Windows ondersteunt integratie met de Kaspersky Endpoint Detection and Response Expert (on-premises)-oplossing. *Kaspersky Endpoint Detection and Response Expert (on-premises)* is een enterprise-cyberbeveiligingsoplossing die Kaspersky-programma's bevat waarmee een organisatie zich kan verdedigen tegen de meeste soorten cyberrisico's en die de belangrijkste scenario's voor de verspreiding van dreigingen dekt. Onderdelen van EDR Expert (on-premises) worden geïmplementeerd op het Open Single Management Platform (OSMP). Dit platform voert cross-platformscenario's uit in één enkele interface en maakt het mogelijk om Kaspersky-programma's te integreren met programma's van derden in een uitgebreid beveiligingssysteem.

Een van de centrale elementen van de oplossing is: *SIEM*. SIEM houdt gebeurtenissen bij die afkomstig zijn van alle onderdelen en correleert deze gebeurtenissen met elkaar met behulp van door de leverancier en door de gebruiker gedefinieerde regels. EDR Expert (on-premises) bekijkt logboeken en telemetriegegevens die worden ontvangen van de bedrijfsinfrastructuur om aanvallen automatisch te detecteren en maakt het onderzoek van incidenten mogelijk met behulp van een uniforme onderzoeksgrafiek die alle gebeurtenissen combineert die in EDR Expert (on-premises) zijn verzameld, inclusief gebeurtenissen van Kaspersky-programma's en informatiebeveiligingsproducten van derden.

Voor de reactie op geavanceerde incidenten gebruikt EDR Expert (on-premises) vooraf ingestelde en door de gebruiker gedefinieerde scenario's. U kunt ook responsacties van programma's van derden en responsscenario's waarbij meerdere programma's zijn betrokken, gebruiken.

Endpoint Detection and Response (KATA)

Kaspersky Endpoint Security voor Windows ondersteund het werken met de Kaspersky Endpoint Detection and Response als onderdeel van de Kaspersky Anti Targeted Attack Platform (EDR (KATA))-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 drie functionele eenheden:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

U kunt alle functionele eenheden of afzonderlijke functionele eenheden afzonderlijk kopen. Voor informatie over de oplossing raadpleegt u de Help van Kaspersky Anti Targeted Attack Platform.

Het programma Kaspersky Endpoint Security 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 (telemetriegegevens) wordt verzonden naar de Kaspersky Anti Targeted Attack Platform-server. In dit geval verzendt Kaspersky Endpoint Security ook informatie naar de Kaspersky Anti Targeted Attack Platform-server over dreigingen gevonden door het programma, evenals informatie over verwerkingsresultaten voor deze dreigingen.

De EDR (KATA) en NDR (KATA)-integratie wordt geconfigureerd op de Kaspersky Security Center-console. De ingebouwde agent wordt vervolgens beheerd met behulp van de Kaspersky Anti Targeted Attack Platform-console, inclusief het uitvoeren van taken, het beheren van in quarantaine geplaatste objecten, het bekijken van rapporten en andere acties.

Instellingen Endpoint Detection and Response Expert (on-premises)

Parameter	Beschrijving
Connection to telemetry collection servers	Een *telemetrieverzamelingsserver* is een server die deel uitmaakt van een SIEM oplossing die informatie over gebeurtenissen op de computer verzamelt, normaliseert, correleert, analyseert en opslaat. Configureer het volgende om verbinding te maken met de servers voor het verzamelen van telemetriegegevens (KUMA): • **Timeout (sec)**. Maximale time-out voor de serverrespons. Wanneer de time-out is verstreken, probeert Kaspersky Endpoint Security verbinding te maken met een andere server. • **Server certificate**. TLS-certificaat voor het tot stand brengen van een vertrouwde verbinding met de server. U kunt een TLS-certificaat verkrijgen via het Open Single Management Platform (zie de instructies in de Help van Kaspersky Endpoint Detection and Response Expert (on-premises)). • **Use two-way authentication**. Tweerichtingsverificatie bij het tot stand brengen van een beveiligde verbinding tussen Kaspersky Endpoint Security en de server. Om tweerichtingsverificatie te gebruiken, moet u tweerichtingsverificatie inschakelen in de server instellingen, vervolgens een crypto-container ophalen en een wachtwoord instellen om de crypto-container te beschermen. Een *crypto-container* is een PFX-archief met een certificaat en een privésleutel. U kunt een cryptocontainer verkrijgen op het Open Single Management Platform (zie de instructies in de Help van Kaspersky Endpoint Detection and Response Expert (on-premises)). Na het configureren van de server instellingen, moet u ook tweerichtingsverificatie inschakelen in de instellingen van Kaspersky Endpoint Security en een met een wachtwoord beveiligde crypto-container laden. De crypto-container moet met een wachtwoord worden beveiligd. Het is niet mogelijk om een crypto-container toe te voegen met een leeg wachtwoord.
Address en **Port** (servers voor het verzamelen van telemetriegegevens)	Instellingen voor verbinding met telemetrieverzamelingsservers. U kunt een IP-adres (IPv4 of IPv6) invoeren. U kunt meerdere adressen van telemetrie-verzamelingsservers toevoegen. Kaspersky Endpoint Security probeert verbinding te maken met de server op het eerste IP-adres. Als er geen verbinding tot stand kan worden gebracht, probeert Kaspersky Endpoint Security verbinding te maken via het tweede IP-adres in de lijst, enzovoort.

Parameter	Beschrijving
Send telemetry to telemetry collection servers	Met deze functionaliteit kunt u het verzenden van telemetrie naar de KATA-server volledig uitschakelen. Als u bijvoorbeeld Kaspersky Anti Targeted Attack Platform gebruikt in combinatie met een andere oplossing die ook telemetrie gebruikt, kunt u het versturen van telemetrie voor KATA (EDR) uitschakelen. Hiermee kunt u de serverbelasting voor deze oplossingen optimaliseren. Als u de Managed Detection and Response-oplossing en KATA (EDR) hebt geïmplementeerd, kunt u MDR-telemetrie gebruiken en Threat Response-taken maken in KATA (EDR). • **Send telemetry with IOA only**. Dit maakt het mogelijk om telemetrie te optimaliseren en alleen telemetrie verzenden met IOA. *Indicator van aanval (IOA)* is een regel die een beschrijving bevat van verdacht gedrag in het systeem dat kan wijzen op een gerichte aanval. Het programma vergelijkt het gedrag in het systeem met deze regels en registreert gebeurtenissen die wijzen op een gerichte aanval. Het programma gebruikt de *streaming scan*technologie die het mogelijk maakt om dergelijke gebeurtenissen in realtime bij te houden. • **Maximum event transmission delay (sec)**. Het programma synchroniseert met de server om gebeurtenissen te verzenden nadat het synchronisatie-interval is verlopen. De standaardinstelling is 30 seconden. • **Limit the number of event packets per transmission**. Het programma synchroniseert met de server wanneer de buffer gevuld is met gebeurtenissen. De standaardinstelling is 1024 gebeurtenissen. Met deze functie kunt u het bufferen van gebeurtenissen vóór synchronisatie met de server uitschakelen.
Enable request throttling	Dit helpt de belasting op de server te optimaliseren. Als deze functionaliteit is ingeschakeld, beperkt het programma de verzending van gebeurtenissen. Als het aantal gebeurtenissen de ingestelde limieten overschrijdt, stopt Kaspersky Endpoint Security met het verzenden van gebeurtenissen. Telemetrie-instellingen configureren: • **Maximum number of events per hour**. Het programma analyseert de telemetriegegevensstroom en beperkt het verzenden van gebeurtenissen als de gebeurtenisstroom de geconfigureerde limiet voor gebeurtenissen per uur overschrijdt. Kaspersky Endpoint Security hervat het verzenden van gebeurtenissen na een uur. De standaardinstelling is 3000 gebeurtenissen per uur. Als het programma op een server is geïnstalleerd, is de telemetrie gegevensstroom hoger. Voor servers wordt aanbevolen om de waarde te verhogen tot 60 000 gebeurtenissen per uur. • **Percentage of event limit excess**. Het programma sorteert gebeurtenissen op type (bijvoorbeeld 'wijzigingen in het register'-gebeurtenissen) en beperkt de overdracht van gebeurtenissen als de verhouding tussen gebeurtenissen van hetzelfde type en het totale aantal gebeurtenissen de geconfigureerde limiet overschrijdt. Kaspersky Endpoint Security hervat het verzenden van gebeurtenissen wanneer de verhouding tussen andere gebeurtenissen en het totale aantal gebeurtenissen opnieuw groot genoeg is. De standaardinstelling is 15 %.
Send sync request to server every (min)	Frequentie van synchronisatieverzoeken die naar de server worden verzonden. Tijdens de synchronisatie verzendt Kaspersky Endpoint Security informatie over gewijzigde programma-instellingen en -taken.
Connection to response servers	Een *responsservers* is een server voor het ontvangen en scannen van gegevens, het bestuderen van het gedrag van objecten en het publiceren van de resultaten van dergelijke onderzoeken. Configureer de volgende instellingen voor de verbinding met de responsservers: • **Timeout (sec)**. Maximale time-out voor de serverrespons. Wanneer de time-out is verstreken, probeert Kaspersky Endpoint Security verbinding te maken met een andere server. • **Server certificate**. TLS-certificaat voor het tot stand brengen van een vertrouwde verbinding met de server. U kunt een TLS-certificaat verkrijgen via het Open Single Management Platform (zie de instructies in de Help van Kaspersky Endpoint Detection and Response Expert (on-premises)). • **Use two-way authentication**. Tweerichtingsverificatie bij het tot stand brengen van een beveiligde verbinding tussen Kaspersky Endpoint Security en de server. Om tweerichtingsverificatie te gebruiken, moet u tweerichtingsverificatie inschakelen in de server instellingen, vervolgens een crypto-container ophalen en een wachtwoord instellen om de crypto-container te beschermen. Een *crypto-container* is een PFX-archief met een certificaat en een privésleutel. U kunt een cryptocontainer verkrijgen op het Open Single Management Platform (zie de instructies in de Help van Kaspersky Endpoint Detection and Response Expert (on-premises)). Na het configureren van de server instellingen, moet u ook tweerichtingsverificatie inschakelen in de instellingen van Kaspersky Endpoint Security en een met een wachtwoord beveiligde crypto-container laden.
Address en **Port** (responsservers)	Instellingen voor verbinding met responsservers. U kunt een IP-adres (IPv4 of IPv6) invoeren. U kunt meerdere adressen van telemetrie-verzamelingsservers toevoegen. Kaspersky Endpoint Security probeert verbinding te maken met de server op het eerste IP-adres. Als er geen verbinding tot stand kan worden gebracht, probeert Kaspersky Endpoint Security verbinding te maken via het tweede IP-adres in de lijst, enzovoort.

Parameter	Beschrijving
Send sync request to server every (min)	Frequentie van synchronisatieverzoeken die naar de server worden verzonden. Tijdens de synchronisatie verzendt Kaspersky Endpoint Security informatie over gewijzigde programma-instellingen en -taken.
Connection to KATA servers	Configureer het volgende voor de verbinding met de Central Node-server: • **Timeout (sec)**. Maximale time-out voor de serverrespons van Central Node. Wanneer de time-out is verstreken, probeert Kaspersky Endpoint Security verbinding te maken met een andere Central Node-server. • **Server certificate**. TLS-certificaat voor het tot stand brengen van een vertrouwde verbinding met de Central Node-server. U kunt een TLS-certificaat verkrijgen in de Kaspersky Anti Targeted Attack Platform-console (zie de instructies in de Help van Kaspersky Anti Targeted Attack Platform). • **Use two-way authentication**. Tweerichtingsverificatie bij het tot stand brengen van een beveiligde verbinding tussen Kaspersky Endpoint Security en de Central Node-server. Om tweerichtingsverificatie te gebruiken, moet u tweerichtingsverificatie inschakelen in de Central Node-server instellingen, vervolgens een crypto-container ophalen en een wachtwoord instellen om de crypto-container te beschermen. Een *crypto-container* is een PFX-archief met een certificaat en een privésleutel. U kunt een crypto-container verkrijgen in de Kaspersky Anti Targeted Attack Platform-console (zie de instructies in de Help van Kaspersky Anti Targeted Attack Platform). Na het configureren van de Central Node-instellingen, moet u ook tweerichtingsverificatie inschakelen in de instellingen van Kaspersky Endpoint Security en een met een wachtwoord beveiligde crypto-container laden. De crypto-container moet met een wachtwoord worden beveiligd. Het is niet mogelijk om een crypto-container toe te voegen met een leeg wachtwoord.
Address en **Port** (KATA-servers)	Instellingen voor verbinding met Kaspersky Anti Targeted Attack Platform-servers. Voer het IP-adres (IPv4 of IPv6) en de poort van de Central Node-server in om verbinding te maken. U kunt meerdere Central Node-serveradressen toevoegen. Kaspersky Endpoint Security probeert verbinding te maken met de server op het eerste IP-adres. Als er geen verbinding tot stand kan worden gebracht, probeert Kaspersky Endpoint Security verbinding te maken via het tweede IP-adres in de lijst, enzovoort.
Send telemetry to KATA	Met deze functionaliteit kunt u het verzenden van telemetrie naar de KATA-server volledig uitschakelen. Als u bijvoorbeeld Kaspersky Anti Targeted Attack Platform gebruikt in combinatie met een andere oplossing die ook telemetrie gebruikt, kunt u het versturen van telemetrie voor KATA (EDR) uitschakelen. Hiermee kunt u de serverbelasting voor deze oplossingen optimaliseren. Als u de Managed Detection and Response-oplossing en KATA (EDR) hebt geïmplementeerd, kunt u MDR-telemetrie gebruiken en Threat Response-taken maken in KATA (EDR). Telemetrie-instellingen configureren: • **Maximum event transmission delay (sec)**. Het programma synchroniseert met de server om gebeurtenissen te verzenden nadat het synchronisatie-interval is verlopen. De standaardinstelling is 30 seconden. • **Maximum number of event packages**. Het programma synchroniseert met de server wanneer de buffer gevuld is met gebeurtenissen. De standaardinstelling is 1024 gebeurtenissen.
Enable request throttling	Dit helpt de belasting op de server te optimaliseren. Als deze functionaliteit is ingeschakeld, beperkt het programma de verzending van gebeurtenissen. Als het aantal gebeurtenissen de ingestelde limieten overschrijdt, stopt Kaspersky Endpoint Security met het verzenden van gebeurtenissen. Telemetrie-instellingen configureren: • **Maximum number of events per hour**. Het programma analyseert de telemetriegegevensstroom en beperkt het verzenden van gebeurtenissen als de gebeurtenisstroom de geconfigureerde limiet voor gebeurtenissen per uur overschrijdt. Kaspersky Endpoint Security hervat het verzenden van gebeurtenissen na een uur. De standaardinstelling is 3000 gebeurtenissen per uur. Als het programma op een server is geïnstalleerd, is de telemetrie gegevensstroom hoger. Voor servers wordt aanbevolen om de waarde te verhogen tot 60 000 gebeurtenissen per uur. • **Percentage of event limit excess**. Het programma sorteert gebeurtenissen op type (bijvoorbeeld 'wijzigingen in het register'-gebeurtenissen) en beperkt de overdracht van gebeurtenissen als de verhouding tussen gebeurtenissen van hetzelfde type en het totale aantal gebeurtenissen de geconfigureerde limiet overschrijdt. Kaspersky Endpoint Security hervat het verzenden van gebeurtenissen wanneer de verhouding tussen andere gebeurtenissen en het totale aantal gebeurtenissen opnieuw groot genoeg is. De standaardinstelling is 15 %.

Network Detection and Response (KATA)

Kaspersky Endpoint Security voor Windows ondersteund het werken met de Kaspersky Network Detection and Response als onderdeel van de Kaspersky Anti Targeted Attack Platform (EDR (KATA))-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 drie functionele eenheden:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

U kunt alle functionele eenheden of afzonderlijke functionele eenheden afzonderlijk kopen. Voor informatie over de oplossing raadpleegt u de Help van Kaspersky Anti Targeted Attack Platform.

Het programma Kaspersky Endpoint Security 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 (telemetriegegevens) wordt verzonden naar de Kaspersky Anti Targeted Attack Platform-server. In dit geval verzendt Kaspersky Endpoint Security ook informatie naar de Kaspersky Anti Targeted Attack Platform-server over dreigingen gevonden door het programma, evenals informatie over verwerkingsresultaten voor deze dreigingen.

De EDR (KATA) en NDR (KATA)-integratie wordt geconfigureerd op de Kaspersky Security Center-console. De ingebouwde agent wordt vervolgens beheerd met behulp van de Kaspersky Anti Targeted Attack Platform-console, inclusief het uitvoeren van taken, het beheren van in quarantaine geplaatste objecten, het bekijken van rapporten en andere acties.

Network Detection and Response (KATA) parameters

Parameter	Beschrijving
Serververbindingsinstellingen	**Time-out (sec.)**. Maximale time-out voor de serverrespons van Central Node. Wanneer de time-out is verstreken, probeert Kaspersky Endpoint Security verbinding te maken met een andere Central Node-server. **Server TLS certificaat**. TLS-certificaat voor het tot stand brengen van een vertrouwde verbinding met de Central Node-server. U kunt een TLS-certificaat verkrijgen in de Kaspersky Anti Targeted Attack Platform-console (zie de instructies in de Help van Kaspersky Anti Targeted Attack Platform). **Gebruik twee-weg verificatie**. Tweerichtingsverificatie bij het tot stand brengen van een beveiligde verbinding tussen Kaspersky Endpoint Security en de Central Node-server. Om tweerichtingsverificatie te gebruiken, moet u tweerichtingsverificatie inschakelen in de Central Node-server instellingen, vervolgens een crypto-container ophalen en een wachtwoord instellen om de crypto-container te beschermen. Een *crypto-container* is een PFX-archief met een certificaat en een privésleutel. U kunt een crypto-container verkrijgen in de Kaspersky Anti Targeted Attack Platform-console (zie de instructies in de Help van Kaspersky Anti Targeted Attack Platform). Na het configureren van de Central Node-instellingen, moet u ook tweerichtingsverificatie inschakelen in de instellingen van Kaspersky Endpoint Security en een met een wachtwoord beveiligde crypto-container laden. De crypto-container moet met een wachtwoord worden beveiligd. Het is niet mogelijk om een crypto-container toe te voegen met een leeg wachtwoord.
Adres en **Poort**	Instellingen voor verbinding met Kaspersky Anti Targeted Attack Platform-servers. Voer het IP-adres (IPv4 of IPv6) en de poort van de Central Node-server in om verbinding te maken. U kunt meerdere Central Node-serveradressen toevoegen. Kaspersky Endpoint Security probeert verbinding te maken met de server op het eerste IP-adres. Als er geen verbinding tot stand kan worden gebracht, probeert Kaspersky Endpoint Security verbinding te maken via het tweede IP-adres in de lijst, enzovoort.
Stuur sync-verzoek naar NDR-server elke (min)	Frequentie van synchronisatieverzoeken die naar de server worden verzonden. Tijdens de synchronisatie verzendt Kaspersky Endpoint Security informatie over gewijzigde programma-instellingen en -taken.

Parameter	Beschrijving
Maximale vertraging gebeurtenisoverdracht (sec)	Het programma synchroniseert met de server om gebeurtenissen te verzenden nadat het synchronisatie-interval is verlopen. De standaardinstelling is 30 seconden.
Afremmen van verzoeken inschakelen	Dit helpt de belasting op de server te optimaliseren. Als deze functionaliteit is ingeschakeld, beperkt het programma de verzending van gebeurtenissen. Als het aantal gebeurtenissen de ingestelde limieten overschrijdt, stopt Kaspersky Endpoint Security met het verzenden van gebeurtenissen.
Maximum aantal gebeurtenissen per uur	Het programma analyseert de telemetriegegevensstroom en beperkt het verzenden van gebeurtenissen als de gebeurtenisstroom de geconfigureerde limiet voor gebeurtenissen per uur overschrijdt. Kaspersky Endpoint Security hervat het verzenden van gebeurtenissen na een uur. De standaardinstelling is 3000 gebeurtenissen per uur. Als het programma op een server is geïnstalleerd, is de telemetrie gegevensstroom hoger. Voor servers wordt aanbevolen om de waarde te verhogen tot 60 000 gebeurtenissen per uur.
Percentage van de limietoverschrijding	Het programma sorteert gebeurtenissen op type (bijvoorbeeld 'wijzigingen in het register'-gebeurtenissen) en beperkt de overdracht van gebeurtenissen als de verhouding tussen gebeurtenissen van hetzelfde type en het totale aantal gebeurtenissen de geconfigureerde limiet overschrijdt. Kaspersky Endpoint Security hervat het verzenden van gebeurtenissen wanneer de verhouding tussen andere gebeurtenissen en het totale aantal gebeurtenissen opnieuw groot genoeg is. De standaardinstelling is 15 %.

Integratie met KUMA

Kaspersky Endpoint Security voor Windows ondersteunt de Kaspersky Unified Monitoring and Analysis Platform-oplossing. *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* is een security information and event management (SIEM) oplossing voor de IT-infrastructuur van organisaties. Met KUMA kunnen beveiligingsbedreigingen worden gedetecteerd, geanalyseerd en beperkt voordat ze schade kunnen veroorzaken.

Instellingen voor KUMA-integratie

Parameter	Beschrijving
Maximum delay when sending events (sec)	Het programma synchroniseert met de server om gebeurtenissen te verzenden nadat het synchronisatie-interval is verlopen. De standaardinstelling is 30 seconden.
Connection to KUMA servers	**Timeout (sec)**. Maximale time-out voor de serverrespons van KUMA. Wanneer de time-out is verstreken, probeert Kaspersky Endpoint Security verbinding te maken met een andere KUMA-server. **Server certificate**. TLS-certificaat voor het tot stand brengen van een vertrouwde verbinding met de KUMA-server. U kunt een TLS-certificaat verkrijgen in de console van Kaspersky Unified Monitoring and Analysis Platform (zie de instructies in Kaspersky Unified Monitoring and Analysis Platform). Om een vertrouwde verbinding tot stand te brengen, moet u in de KUMA-console, in de instellingen van de tcp-connector, de **With verification** TLS-modus (zie de instellingen voor de tcp-type connector in de Hulp bij Kaspersky Unified Monitoring and Analysis Platform). **Use two-way authentication**. Tweerichtingsverificatie bij het tot stand brengen van een beveiligde verbinding tussen Kaspersky Endpoint Security en KUMA. Om tweerichtingsverificatie te gebruiken, moet u in de KUMA-console, in de instellingen van de tcp-connector, de **Custom PFX** TLS-modus (zie de instellingen voor de tcp-type connector in de Hulp bij Kaspersky Unified Monitoring and Analysis Platform). Dan moet u een cryptocontainer aanschaffen en een wachtwoord instellen om de cryptocontainer te beschermen. Een *crypto-container* is een PFX-archief met een certificaat en een privésleutel. Na het configureren van de KUMA-instellingen, moet u ook tweerichtingsverificatie inschakelen in de instellingen van Kaspersky Endpoint Security en een met een wachtwoord beveiligde crypto-container laden. De crypto-container moet met een wachtwoord worden beveiligd. Het is niet mogelijk om een crypto-container toe te voegen met een leeg wachtwoord.
KUMA-servers	Verbinding met de instellingen van de servers van het Kaspersky Unified Monitoring and Analysis Platform. U kunt een IP-adres (IPv4 of IPv6) invoeren. U kunt meerdere adressen van KUMA-servers toevoegen. Kaspersky Endpoint Security probeert verbinding te maken met de server op het eerste IP-adres. Als er geen verbinding tot stand kan worden gebracht, probeert Kaspersky Endpoint Security verbinding te maken via het tweede IP-adres in de lijst, enzovoort.

Full Disk Encryption

U kunt een encryptietechnologie selecteren: Kaspersky Disk Encryption of BitLocker-stationsversleuteling (hierna ook gewoon "BitLocker" genoemd).

Kaspersky Disk Encryption

Kaspersky Disk Encryption wordt niet ondersteund op Arm-computers.

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 de taak *Accounts voor Authenticatie-agent beheren*. Dit account is gebaseerd op een Microsoft Windows-account waarmee een gebruiker zich bij het besturingssysteem aanmeldt. U kunt ook gebruikmaken van Single Sign-On (SSO)-technologie, 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 beheren en controleren via de Kaspersky Next-infrastructuur. 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.

Bij het encrypten van de schijf plaatst BitLocker de bootloader en andere hulpbestanden in de system partition. Deze partitie is niet geëncrypt. Het besturingssysteem maakt de systeempartitie automatisch aan tijdens de installatie van Windows. Als de schijf volledig is gepartitioneerd voordat Windows wordt geïnstalleerd, kan het besturingssysteem geen systeempartitie maken. In dit geval wordt u door het besturingssysteem gevraagd de schijf opnieuw te partitioneren en een systeempartitie te maken wanneer u

BitLocker schijfversleuteling start. Na het maken van een systeempartitie start het besturingssysteem de BitLocker encryptie.

BitLocker biedt veilige opslag van toegangssleutels met behulp van een vertrouwde platformmodule. Een *Trusted Platform Module* (TPM) is een men 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 de harde schijf van het systeem, moet de gebruiker BitLocker-verificatie doorlopen om het besturingssysteem op te starten. Na de authenticatie staat BitLocker de gebruiker toe zich aan te melden. BitLocker ondersteunt geen technologie voor eenmalige aanmelding (SSO).

Na het encrypten van een schijf, maakt BitLocker een herstelsleutel aan. Kaspersky Endpoint Security stuurt de herstelsleutel naar Kaspersky Security Center zodat u de toegang tot de schijf kunt herstellen, bijvoorbeeld als een gebruiker zijn wachtwoord is vergeten.

Als een gebruiker een schijf van encryptie voorziet met BitLocker, stuurt Kaspersky Endpoint Security de herstelsleutel en informatie over schijfencryptie naar Kaspersky Security Center.

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.

Onderdeelinstellingen van Kaspersky Disk Encryption

Parameter	Beschrijving
Encryptiemodus	**Alle harde schijven encrypten**. Als deze optie is geselecteerd wanneer het beleid is toegepast, worden alle harde schijven geëncrypt door het programma. 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. **Alle harde schijven decrypten**. Als deze optie is geselecteerd wanneer het beleid is toegepast, worden alle eerder geëncrypte harde schijven gedecrypt door het programma. **Ongewijzigd laten**. 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.
Accounts in Authenticatie-agent automatisch voor Windows-gebruikers aanmaken tijdens encryptie	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.

Parameter	Beschrijving
Instellingen voor aanmaak van account voor Authenticatie-agent	**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.
Accounts in Authenticatie-agent automatisch aanmaken voor alle gebruikers van deze computer bij aanmelding	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 handmatig Authenticatie-agent-accounts toe te voegen met de taak *Accounts voor Authenticatie-agent beheren* voor computers met reeds versleutelde stations.
Ingevoerde gebruikersnaam in Authenticatie-agent opslaan	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.
Alleen gebruikte schijfruimte encrypten (snellere encryptie)	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. De in- of uitschakeling van de functie **Alleen gebruikte schijfruimte encrypten (snellere encryptie)** 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. Het selectievakje is standaard uitgeschakeld.
Ondersteuning voor verouderde USB-apparaten gebruiken (niet aanbevolen)	Dit selectievakje schakelt de Legacy USB Support functionaliteit in of uit. *Ondersteuning voor verouderde USB-apparaten* **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). Legacy USB Support is niet van invloed op de ondersteuning voor USB-apparaten nadat het besturingssysteem is gestart. Als het selectievakje is ingeschakeld, wordt de ondersteuning voor USB-apparaten tijdens de initiële opstart van de computer ingeschakeld. Wanneer de functie Legacy USB Support 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.

Parameter	Beschrijving
Wachtwoordinstellingen	Instellingen voor wachtwoordsterkte voor Authenticatie-agent-accounts. 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.
Eenmalige aanmelding (SSO) gebruiken	Met SSO-technologie kunt u dezelfde accountgegevens gebruiken om toegang tot geëncrypte harde schijven te krijgen en u bij het besturingssysteem aan te melden. 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. 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.
Wrap gebruikersgegevens van andere leveranciers	Kaspersky Endpoint Security ondersteunt de externe referentieprovider ADSelfService Plus. Bij het werken met externe referentieproviders onderschept de authenticatie-agent het wachtwoord voordat het besturingssysteem wordt geladen. Dit betekent dat een gebruiker slechts één keer een wachtwoord hoeft in te voeren wanneer hij zich aanmeldt bij Windows. Na aanmelding bij Windows, kan de gebruiker gebruikmaken van een externe referentieprovider voor authenticatie in bijvoorbeeld bedrijfsservices. Externe referentieproviders stellen gebruikers ook in staat om onafhankelijk hun eigen wachtwoord opnieuw in te stellen. In dit geval werkt Kaspersky Endpoint Security het wachtwoord voor Authenticatie-agent automatisch bij. Als u een externe referentieprovider gebruikt die niet door het programma wordt ondersteund, kunt u enkele beperkingen tegenkomen bij de werking van Single Sign-On-technologie.
Help	**Authenticatie**. Helptekst die wordt weergegeven in het venster Authenticatie-agent bij het invoeren van aanmeldingsgegevens voor een account. **Wachtwoord wijzigen**. Helptekst die wordt weergegeven in het venster Authenticatie-agent wanneer het wachtwoord voor het Authenticatie-agent-account wordt gewijzigd. **Wachtwoord herstellen**. Helptekst die wordt weergegeven in het venster Authenticatie-agent wanneer het wachtwoord voor het Authenticatie-agent-account wordt hersteld.

Instellingen component BitLocker-stationsversleuteling

Parameter	Beschrijving
Encryptiemodus	**Alle harde schijven encrypten**. Als deze optie is geselecteerd wanneer het beleid is toegepast, worden alle harde schijven geëncrypt door het programma. 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. **Alle harde schijven decrypten**. Als deze optie is geselecteerd wanneer het beleid is toegepast, worden alle eerder geëncrypte harde schijven gedecrypt door het programma. **Ongewijzigd laten**. 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.
Gebruik van BitLocker-authenticatie inschakelen die preboot-toetsenbordinvoer op tablets vereist	Verificatie gebruiken die gegevensinvoer vereist in een preboot-omgeving, zelfs als het platform geen mogelijkheid heeft voor preboot-invoer (bijvoorbeeld met toetsenborden op aanraakschermen van tablets). 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. Als het selectievakje is ingeschakeld, is het gebruik van een authenticatie met invoer vóór de opstart toegestaan. We raden aan deze instelling alleen te gebruiken voor apparaten die beschikken over alternatieve middelen voor gegevensinvoer vóór de opstart, zoals een USB-toetsenbord naast schermtoetsenborden. Als het selectievakje is uitgeschakeld, is BitLocker-stationsversleuteling niet mogelijk op tablets.
Hardware-encryptie gebruiken (Windows 8 en nieuwer)	Als het selectievakje is ingeschakeld, past het programma een hardware-encryptie toe. Hiermee kunt u sneller encrypten en gebruikt u minder computerbronnen.

Parameter	Beschrijving
Alleen gebruikte schijfruimte encrypten (Windows 8 en nieuwer)	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. De in- of uitschakeling van de functie **Alleen gebruikte schijfruimte encrypten (snellere encryptie)** 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. Het selectievakje is standaard uitgeschakeld.
Authenticatiemethode	**Alleen wachtwoord (Windows 8 en nieuwer)** 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. **Trusted Platform Module (TPM)** Als deze optie is geselecteerd, gebruikt BitLocker een Trusted Platform Module (TPM). Een *Trusted Platform Module* (TPM) is een men 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: • **Pincode gebruiken voor 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. • **Trusted Platform Module (TPM), of wachtwoord als TPM niet beschikbaar is**. Als deze optie 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. De geselecteerde authenticatiemethode moet worden geconfigureerd door wachtwoord- of pincodevereisten op te geven: • **Minimale lengte van pincode (tekens)**. • **Minimale lengte van wachtwoord (tekens)**. • **Geldigheidsduur van wachtwoord / pincode voor TPM beperken (dagen)**. • **Geavanceerde pincode gebruiken (letters en cijfers)**. Met *Geavanceerde pincode* kunt u naast cijfers ook andere tekens gebruiken: hoofdletters en kleine letters, speciale tekens en spaties.
Herstelsleutel automatisch opnieuw maken (dagen)	Werk het wachtwoord automatisch bij om de toegang tot een schijf die wordt beschermd door BitLocker te herstellen. Als het selectievakje is ingeschakeld, geef de geldigheidsperiode van het wachtwoord voor de herstelsleutel op. Dit helpt hergebruik van het wachtwoord voor de herstelsleutel te voorkomen.

File Level Encryption

Bestandsencryptie wordt niet ondersteund op Arm-computers.

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.

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.

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	**Ongewijzigd laten**. Als deze optie is geselecteerd, laat Kaspersky Endpoint Security bestanden en mappen ongewijzigd door ze niet te encrypten of te decrypten. **Volgens regels**. 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. **Alles decrypten**. Als deze optie is geselecteerd, worden alle geëncrypte bestanden en mappen gedecrypt door Kaspersky Endpoint Security.

Parameter	Beschrijving
Encryptie	Op dit tabblad ziet u encryptieregels voor bestanden die op lokale schijven zijn opgeslagen. U kunt als volgt bestanden toevoegen: • **Vooraf gedefinieerde mappen**. In Kaspersky Endpoint Security kunt u de volgende gebieden toevoegen: **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). • **Aangepaste map**. U kunt het pad naar de map typen. 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. • **Bestanden op extensie**. U kunt extensiegroepen in de lijst selecteren, zoals de extensiegroep *Archieven*. U kunt de bestandsextensie ook handmatig toevoegen.
Decryptie	Op dit tabblad ziet u decryptieregels voor bestanden die op lokale schijven zijn opgeslagen.
Regels voor programma's	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.
Geëncrypte pakketten	Wachtwoordsterkte-eisen waaraan moet worden voldaan bij het maken van geëncrypte pakketten.

Encryptie van verwisselbare schijven

Versleuteling van verwisselbare schijven wordt niet ondersteund op Arm-gebaseerde computers.

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

Onderdeelinstellingen voor encryptie van verwisselbare schijven

Parameter	Beschrijving
Encryptiemodus	**Gehele verwisselbare schijf encrypten**. 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). **Alle bestanden encrypten**. 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. **Alleen nieuwe bestanden encrypten**. 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 encryptiefunctionaliteit is ingeschakeld. Hierdoor is de toegang tot persoonlijke bestanden altijd beschikbaar, ongeacht of Kaspersky Endpoint Security met ingeschakelde encryptiefunctionaliteit is geïnstalleerd op de computer. **Gehele verwisselbare schijf decrypten**. 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. **Ongewijzigd laten**. 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.
Portable modus	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. 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. De portable modus is beschikbaar voor de modi **Alle bestanden encrypten** of **Alleen nieuwe bestanden encrypten**.
Alleen gebruikte schijfruimte encrypten	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. 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. Als het selectievakje is uitgeschakeld, wordt de gehele schijf geëncrypt, inclusief achtergebleven fragmenten van eerder verwijderde en gewijzigde bestanden. De mogelijkheid om alleen gebruikte ruimte te encrypten is alleen beschikbaar voor de modus **Gehele verwisselbare schijf encrypten**. Na de start van de encryptie wordt deze instelling niet gewijzigd door de inschakeling of uitschakeling van de functie **Alleen gebruikte schijfruimte encrypten**. U moet het selectievakje inschakelen of uitschakelen alvorens de encryptie te starten.

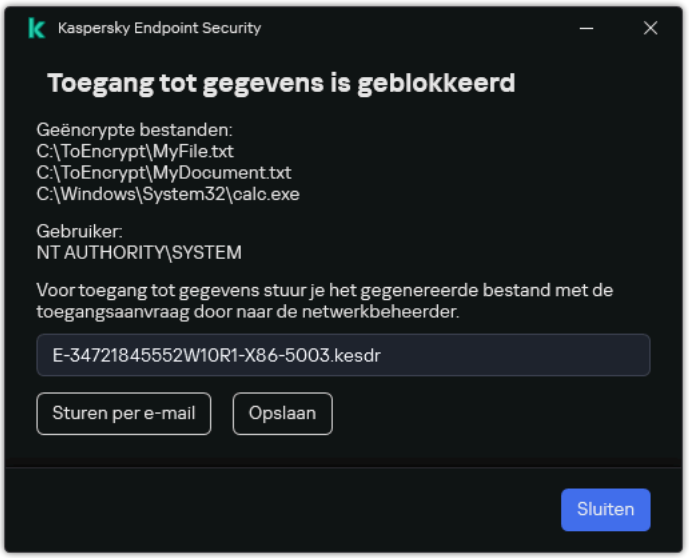
Parameter	Beschrijving

Aangepaste regels	In deze tabel ziet u de apparaten waarvoor aangepaste encryptieregels zijn gedefinieerd. U kunt op de volgende manieren encryptieregels maken voor afzonderlijke verwisselbare schijven:
	• Een verwisselbare schijf toevoegen uit de lijst met vertrouwde apparaten voor apparaatbeheer.
	• Handmatig een verwisselbare schijf toevoegen:
	  • Op apparaat-ID (Hardware ID of HWID)
	  • Op apparaatmodel: Vendor ID (VID) en Product ID (PID)

Encryptie van verwisselbare schijven in offline modus toestaan	Als dit selectievakje is ingeschakeld, worden verwisselbare schijven door Kaspersky Endpoint Security geëncrypt zelfs 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. Als het selectievakje is uitgeschakeld, worden verwisselbare schijven niet geëncrypt door Kaspersky Endpoint Security als er geen verbinding met Kaspersky Security Center is.
Instellingen van encryptiewachtwoord / Portable bestandsbeheer	Wachtwoordsterkte-instellingen voor Portable bestandsbeheer.

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:

- **Aan**. Voer het e-mailadres in van de beheerdersgroep met rechten voor de functies voor gegevensencryptie.
- **Onderwerp**. 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 van gebruiker**. 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 uitzonderingen en vertrouwde programma's maken naast de algemene vertrouwde zone in een beleid.

Vanaf Kaspersky Endpoint Security 12.5 voor Windows kunt u EDR-telemetrie toevoegen aan de vertrouwde zone. Hierdoor kunnen de gegevens worden geoptimaliseerd die het programma naar de Telemetrieverzamelingsserver verzendt voor de Kaspersky Anti Targeted Attack Platform (EDR)-oplossing.

Beginnend met Kaspersky Endpoint Security 12.6 voor Windows, uitzonderingen scannen en vertrouwde programma's worden toegevoegd aan de vertrouwde zone. Vooraf gedefinieerde scanuitzonderingen en vertrouwde programma's helpen bij het snel configureren van Kaspersky Endpoint Security op SQL-servers, Microsoft Exchange-servers en System Center Configuration Manager. Dit betekent dat u niet handmatig een vertrouwde zone voor het programma op servers hoeft in te stellen.

Vanaf Kaspersky Endpoint Security 12.8 voor Windows kun je het programma in Light Agent-modus installeren om virtuele omgevingen te beschermen. Met voorgedefinieerde uitzonderingen van scans en vertrouwde programma's kunt u Kaspersky Endpoint Security snel configureren in Citrix- en VMware-virtuele omgevingen.

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 een 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 inbrekers kunnen gebruiken om uw 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
- *Malware-scan*-taak

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 bewaakt 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. Nadat een programma is toegevoegd aan de lijst met vertrouwde programma's, stopt Kaspersky Endpoint Security met het monitoren van de activiteit van het programma.

Het verschil tussen scanuitzonderingen en vertrouwde programma's is dat Kaspersky Endpoint Security voor uitzonderingen geen bestanden scant, terwijl het voor vertrouwde programma's geen controle heeft over de gestarte processen. Als een vertrouwd programma een kwaadaardig bestand maakt in een map die niet is opgenomen in scanuitzonderingen, zal Kaspersky Endpoint Security het bestand detecteren en de dreiging elimineren. Als de map wordt toegevoegd aan uitzonderingen, slaat Kaspersky Endpoint Security dit bestand over.

Als u bijvoorbeeld objecten die door het standaard Microsoft Windows-programma Kladblok worden gebruikt als veilig beschouwt, omdat u dit programma vertrouwt, kunt u Microsoft Windows-programma Kladblok toevoegen aan de lijst met vertrouwde programma's, zodat de objecten die door dit programma worden gebruikt, niet bewaakt. Dit zal de computerprestaties verbeteren, wat vooral belangrijk is bij het gebruik van servertoepassingen.

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.

Vertrouwde programma's helpen compatibiliteitsproblemen tussen Kaspersky Endpoint Security en andere programma's te voorkomen (bijvoorbeeld het probleem van het dubbel scannen van het netwerkverkeer van een computer van derden door Kaspersky Endpoint Security en door een ander antivirusprogramma).

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.

Parameter	Beschrijving

Soorten gedetecteerde objecten

Kaspersky Endpoint Security detecteert en blokkeert altijd virussen, wormen en Trojans, ongeacht de geconfigureerde programma-instellingen. Ze kunnen een computer immers grote schade toebrengen.

- **Virussen en wormen**

  Subcategorie: Virussen en wormen (Viruses_and_Worms)

  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. *Overwriting* 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. *Parasitic* virussen wijzigen bestanden waardoor ze volledig of deels functioneel blijven. *Companion* 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: *Link virussen*, *OBJ-virussen*, *LIB-virussen*, *broncode* virussen 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. 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.
IRC-Worm	Online chat wormen	Deze verspreiden zich via Internet Relay Chats, servicesystemen waarmee mensen met elkaar kunnen communiceren in real time via het internet. 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.
Net-worm	Netwerkwormen	Deze wormen verspreiden zich via computernetwerken. 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.
P2P-worm	Netwerkwormen voor bestandsdeling	Deze verspreiden zich via peer-to-peernetwerken voor bestandsdeling. 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. 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.
Worm	Andere soorten wormen	Enkele andere soorten wormen zijn: • 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. • 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.

  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
Trojan-ArcBomb	Trojans – "archiefbommen"	Tijdens het uitpakken worden deze archieven zo groot dat de werking van de computer wordt beïnvloed. 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.
Backdoor	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.
Trojan	Trojans	Deze omvatten de volgende schadelijke programma's: • **Klassieke Trojans**. 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. • **Veelzijdige Trojans**. Deze programma's hebben geavanceerde functies die kenmerken zijn voor diverse soorten Trojans.
Trojan-Ransom	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.
Trojan-Clicker	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.
Trojan-Downloader	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.
Trojan-Dropper	Trojan droppers	Deze bevatten andere Trojans die ze op de harde schijf plaatsen en vervolgens installeren. Indringers kunnen programma's van het type Trojan Dropper gebruiken voor het volgende: • 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. • De detectie van een ander schadelijk programma voorkomen: niet alle antivirussoftware kan een schadelijk programma in een programma van het type Trojan Dropper detecteren.
Trojan-Notifier	Trojan notifiers	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. 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.
Trojan-Proxy	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.
Trojan-PSW	Software voor het stelen van wachtwoorden	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. 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).
Trojan-Spy	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.

Trojan-DDoS	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. 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.
Trojan-IM	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.
Rootkit	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.
Trojan-SMS	Trojans in de vorm van sms-berichten	Deze infecteren mobiele telefoons door sms-berichten naar betalende telefoonnummers te versturen.
Trojan-GameThief	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.
Trojan-Banker	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.
Trojan-Mailfinder	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
Constructeur	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.
Dos	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).
Exploit	Exploits	Een *exploit* 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. 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. Net-Worms verspreiden zich via netwerken door middel van exploits. Nuker exploits zijn netwerkpakketten die computers uitschakelen.
FileCryptor	Encryptors	Deze encrypten andere schadelijke programma's om ze te verbergen voor het antivirusprogramma.
Flooder	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).
HackTool	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.
Hoax	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.
Spoofer	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.

VirTool	Tools die schadelijke programma's aanpassen	Deze kunnen worden gebruikt om malware aan te passen en ze te verbergen voor antivirusprogramma's.
Email-Flooder	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.
IM-Flooder	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.
SMS-Flooder	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 inbrekers 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 internetservers 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
Client-IRC	Online chatprogramma's	Gebruikers installeren deze programma's om met personen in Internet Relay Chats te spreken. Indringers gebruiken ze om malware te verspreiden.
Downloader	Programma's voor downloads	Deze kunnen bestanden vanaf webpagina's downloaden in een verborgen modus.
Monitor	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).
PSWTool	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.
RemoteAdmin	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. 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.
Server-FTP	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.
Server-Proxy	Proxyservers	Deze werken als proxyservers. Indringers plaatsen ze op de computer van de gebruiker om spam onder de naam van de gebruiker te versturen.
Server-Telnet	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.
Server-Web	Webservers	Deze werken als webservers. Indringers plaatsen ze op de computer van de gebruiker om er op afstand toegang tot te krijgen via HTTP.
RiskTool	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.
NetTool	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.
Client-P2P	P2P-netwerkprogramma's	Deze hebben functies voor peer-to-peernetwerken. Ze kunnen door indringers worden gebruikt om malware te verspreiden.

Client-SMTP	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.
WebToolbar	Online werkbalken	Deze voegen werkbalken aan de interface van andere programma's toe om zoekmachines te gebruiken.
FraudTool	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.

- **Legitieme software die hackers kunnen gebruiken om de computer of persoonlijke gegevens te beschadigen**

  Subcategorie: Legitieme software die inbrekers 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 internetservers 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
Client-IRC	Online chatprogramma's	Gebruikers installeren deze programma's om met personen in Internet Relay Chats te spreken. Indringers gebruiken ze om malware te verspreiden.
Downloader	Programma's voor downloads	Deze kunnen bestanden vanaf webpagina's downloaden in een verborgen modus.
Monitor	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).
PSWTool	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.
RemoteAdmin	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. 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.
Server-FTP	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.
Server-Proxy	Proxyservers	Deze werken als proxyservers. Indringers plaatsen ze op de computer van de gebruiker om spam onder de naam van de gebruiker te versturen.
Server-Telnet	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.
Server-Web	Webservers	Deze werken als webservers. Indringers plaatsen ze op de computer van de gebruiker om er op afstand toegang tot te krijgen via HTTP.
RiskTool	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.
NetTool	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.
Client-P2P	P2P-netwerkprogramma's	Deze hebben functies voor peer-to-peernetwerken. Ze kunnen door indringers worden gebruikt om malware te verspreiden.
Client-SMTP	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.
WebToolbar	Online werkbalken	Deze voegen werkbalken aan de interface van andere programma's toe om zoekmachines te gebruiken.
FraudTool	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**

  subcategorie: Ingepakte bestanden die schade kunnen veroorzaken.

  Veiligheidsrisico: Gemiddeld.

	Het bestand wordt ingepakt met een speciale packer die wordt gebruikt voor het verpakken van malware: virussen, wormen, Trojans. Kaspersky Endpoint Security scant de decompressiemodule in SFX-archieven (zelfuitpakkende archieven). Om malware te verbergen voor detectie door een antivirusprogramma, pakken hackers het in met speciale packers. Kaspersky-experts hebben de compressieprogramma's geïdentificeerd die hackers het meest gebruiken. • **Meermaals ingepakte objecten** **subcategorie**: Ingepakte bestanden die schade kunnen veroorzaken. **Veiligheidsrisico**: Gemiddeld. Het bestand wordt ingepakt met een speciale packer die wordt gebruikt voor het verpakken van malware: virussen, wormen, Trojans. Kaspersky Endpoint Security scant de decompressiemodule in SFX-archieven (zelfuitpakkende archieven). Om malware te verbergen voor detectie door een antivirusprogramma, pakken hackers het in met speciale packers. Kaspersky-experts hebben de compressieprogramma's geïdentificeerd die hackers het meest gebruiken.
Uitzonderingen	Deze tabel bevat informatie over scanuitzonderingen. We raden aan dat u relatieve paden opgeeft in plaats van absolute paden. Hierdoor kunt u niet alleen bestandssysteemobjecten uitsluiten, maar ook objecten zonder bestanden. Bijvoorbeeld `*\Program Files (x86)\Folder\Subfolder`.

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:\Folder\**\*.txt` omvat bijvoorbeeld alle paden naar bestanden met de TXT-extensie die zich in mappen bevinden genest in de `Folder`, uitgezonderd de `Folder` 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:\Folder\???.txt` omvat bijvoorbeeld paden naar alle bestanden die zich in de map met de naam `Folder` bevinden, die een TXT-extensie hebben en die een naam met drie tekens hebben.

    U kunt maskers overal in een bestands- of mappad gebruiken. Als u bijvoorbeeld wilt dat het scanbereik de map Downloads bevat voor alle gebruikersaccounts op de computer, voert u het masker `C:\Users\*\Downloads\` uit.

    Kaspersky Endpoint Security ondersteunt omgevingsvariabelen

    > Kaspersky Endpoint Security ondersteunt de omgevingsvariabele `%userprofile%` niet bij het genereren van een lijst met uitzonderingen 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.

- Voer de naam van het object 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 het programma `Client-IRC`, `Client-P2P` en `Client-SMTP`-objecten uit van scans.

> Kaspersky Endpoint Security verbergt de lijst met scanuitzonderingen in de gebruikersinterface van het programma als het instellen van scanuitzonderingen geblokkeerd is door de beheerder in de console ("gesloten slot"-symbool) en lokale scanuitzonderingen zijn verboden (het selectievakje **Gebruik van lokale uitzonderingen toestaan** is uitgeschakeld).

Vertrouwde programma's	In deze tabel ziet u vertrouwde programma's waarvan de activiteit niet wordt gemonitord door Kaspersky Endpoint Security tijdens de werking ervan. 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. Het onderdeel Programmacontrole controleert de opstart van elk programma, ongeacht of het programma voorkomt in de tabel met vertrouwde programma's. Kaspersky Endpoint Security verbergt de geconsolideerde lijst met vertrouwde programma's in de gebruikersinterface van het programma als het instellen van vertrouwde programma's geblokkeerd is door de beheerder in de console ("gesloten slot"-symbool) en lokale vertrouwde programma's zijn verboden (het selectievakje **Gebruik van lokale vertrouwde programma's toestaan** is uitgeschakeld).
Waarden samenvoegen bij overname *(alleen beschikbaar in de Kaspersky Security Center-console)*	Hiermee wordt de lijst met scanuitzonderingen 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. 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. Overgenomen lijstitems in een onderliggend beleid kunnen niet worden verwijderd of bewerkt. Items op de lijst met scanuitzonderingen 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. Als items op lijsten van het onderliggende beleid en het bovenliggende beleid overeenkomen, worden deze items weergegeven als hetzelfde item van het bovenliggende beleid. Als het selectievakje is uitgeschakeld, worden items van lijsten niet samengevoegd wanneer de instellingen van het Kaspersky Security Center-beleid worden overgenomen. Met deze functie kunt u ook lijsten in beleidsprofielen samenvoegen. Als u lijsten wilt samenvoegen, schakelt u in het profiel met de hoogste prioriteit de overname van instellingen van een profiel met een lagere prioriteit in. Voor meer informatie over beleidsprofiel-prioriteiten, raadpleegt u de Help van Kaspersky Security Center.
Gebruik van lokale uitzonderingen toestaan / **Gebruik van lokale vertrouwde programma's toestaan** *(alleen beschikbaar in de Kaspersky Security Center-console)*	*Lokale uitzonderingen en lokale vertrouwde programma's (lokale vertrouwde zone)* - 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 hun eigen lokale lijsten met uitzonderingen en vertrouwde programma's maken naast de algemene vertrouwde zone in een beleid. Als het selectievakje is ingeschakeld, kan een gebruiker een lokale lijst met scanuitzonderingen 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. Als het selectievakje is uitgeschakeld, heeft een gebruiker alleen toegang tot de algemene lijsten met scanuitzonderingen en vertrouwde programma's die in het beleid zijn gegenereerd.
EDR (KATA) / NDR (KATA) telemetrie *(alleen beschikbaar in de Kaspersky Security Center-console)*	Deze tabel bevat informatie over EDR-telemetrie uitzonderingen.
KUMA-telemetrie *(alleen beschikbaar in de Kaspersky Security Center-console)*	Lijst met gebeurtenissen die naar Kaspersky Unified Monitoring and Analysis Platform (KUMA) moet worden verzonden. Kaspersky Endpoint Security werkt in de volgende modussen: • **Alle evenementen versturen**. In deze modus verstuurt het programma alle gebeurtenissen uit het Windows-logboek, behalve gebeurtenissen die zijn toegevoegd aan uitzonderingsregels. • **Alleen geselecteerde evenementen versturen**. In deze modus verstuurt het programma alleen gebeurtenissen die zijn toegevoegd aan inclusieregels.
Vertrouwde systeemcertificatenopslag	Als een van de vertrouwde systeemcertificaatopslagplaatsen 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 **Vertrouwd**. Als **Niet gebruiken** 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.

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
Programma starten wanneer computer wordt opgestart (aanbevolen)	Wanneer deze optie is geselecteerd, wordt Kaspersky Endpoint Security gestart nadat het besturingssysteem is geladen, om de computer tijdens de gehele sessie te beschermen. Als deze optie is uitgeschakeld, wordt Kaspersky Endpoint Security niet na de opstart van het besturingssysteem gestart, totdat de gebruiker dit handmatig doet. Computerbescherming is uitgeschakeld en de gegevens van de gebruiker lopen mogelijk gevaar.
Gebruik Geavanceerde desinfectietechnologie (vereist heel wat computerbronnen)	Doorgaans beëindigt Kaspersky Endpoint Security gedetecteerde malware voordat de computer geïnfecteerd raakt. De geavanceerde desinfectietechnologie beschermt de computer tegen reeds actieve malware (actieve infectie), waardoor het risico op gegevensverlies en de verspreiding van dreigingen tot een minimum wordt beperkt. Als deze technologie is ingeschakeld, toont Kaspersky Endpoint Security een pop-upmelding wanneer kwaadaardige activiteit wordt gedetecteerd. In de melding wordt de gebruiker door Kaspersky Endpoint Security de optie aangeboden om een geavanceerde desinfectie op de computer uit te voeren. Nadat de gebruiker deze procedure heeft goedgekeurd, neutraliseert Kaspersky Endpoint Security de dreiging en herstart vervolgens de computer. De geavanceerde desinfectietechnologie gebruikt heel wat computerbronnen waardoor andere programma's mogelijk trager gaan werken. 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. Als Kaspersky Endpoint Security is geïnstalleerd op een computer met Windows for Servers, toont Kaspersky Endpoint Security de melding niet. Daarom kan u 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 *Malware-scan*. Vervolgens moet u de *Malware-scan* starten.
Kaspersky Security Center gebruiken als proxyserver voor activering *(alleen beschikbaar in de Kaspersky Security Center-console)*	Als dit selectievakje is ingeschakeld, gebruikt het programma de Kaspersky Security Center Administration Server als een proxyserver om verbinding te maken met de activeringsserver. Dit is vereist indien je een activeringscode gebruikt om het programma te activeren in een geïsoleerd netwerksegment zonder internettoegang. Als je het programma met een sleutelbestand activeert, is internettoegang niet nodig.
Zelfbescherming inschakelen	Als deze functionaliteit is ingeschakeld, voorkomt Kaspersky Endpoint Security dat programmabestanden op de harde schijf, geheugenprocessen en vermeldingen in het systeemregister worden gewijzigd of verwijderd.

Parameter	Beschrijving
Extern beheer van programmadiensten blokkeren	Als deze functionaliteit is ingeschakeld, staat Kaspersky Endpoint Security het beheer van programmaservices via programma's van derden (zoals CMD) niet toe. Wanneer er een poging wordt gedaan om programmaservices te beheren met behulp van programma's van derden wordt een melding boven het pictogram van het programma in de Microsoft Windows-taakbalk weergegeven (tenzij de meldingen zijn uitgeschakeld door de gebruiker). U kunt extern beheer van programmaservices alleen toestaan op computers die de AM-PPL-technologie niet ondersteunen of op computers waarop de technologie is uitgeschakeld.
Geplande taken uitstellen bij werking op accustroom	Als dit selectievakje is ingeschakeld, wordt de energiebesparende modus ingeschakeld wanneer de computer op de batterijspanning werkt. Kaspersky Endpoint Security stelt geplande taken uit. U kunt indien nodig een scan- en updatetaken handmatig starten. Wanneer de energiebesparingsmodus is ingeschakeld en een computer op batterijspanning werkt, worden de volgende taken niet gestart zelfs als ze zijn gepland: • *Volledige Scan* • *Kritieke Gebiedenscan* • *Aangepaste Scan* • *Programma Integriteitscontrole* • *IOC-scan* • *Update van databases en programmamodules* (alleen patches) Het programma slaat geplande database-updates alleen over wanneer de laptop werkt op de batterij en het batterijniveau lager is dan 30%. In alle andere gevallen werkt Kaspersky Endpoint Security de databases bij volgens schema, ongeacht of de laptop is aangesloten op een stopcontact of werkt op de batterij, of dat het programma zich in de energiebesparingsmodus bevindt.
Bronnen aan andere programma's geven	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.
Beperk CPU-gebruik voor scantaken	Om de prestaties van Kaspersky Endpoint Security te optimaliseren, kunt u het CPU-gebruik beperken via: *Malware-scan* taak. Als het selectievakje is ingeschakeld, wordt de gemiddelde belasting van alle CPU-kernen van de *Malware-scan* taak de opgegeven waarde. Het selectievakje is standaard uitgeschakeld.
Schrijven naar dump inschakelen	Als het selectievakje is ingeschakeld, schrijft Kaspersky Endpoint Security dumps wanneer het crasht. Als het selectievakje is uitgeschakeld, schrijft Kaspersky Endpoint Security geen dumps. Het programma verwijdert ook bestaande dumpbestanden op de harde schijf van de computer.
Bescherming voor dump- en tracebestanden inschakelen	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. Als het selectievakje is uitgeschakeld, hebben alle gebruikers toegang tot dump- en tracebestanden.
Computerstatus wanneer instellingen worden toegepast *(alleen beschikbaar in de Kaspersky Security Center-console)*	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 volgende statussen zijn beschikbaar *OK*, *Waarschuwing* en *Kritiek*.

Parameter	Beschrijving
Updates installeren zonder computer opnieuw te starten	Door het programma te upgraden zonder de computer opnieuw op te starten, bent u verzekerd van een ononderbroken werking van servers. U kunt het programma upgraden zonder opnieuw te starten vanaf versie 11.10.0. Als u een eerdere versie van het programma wilt upgraden, moet u de computer opnieuw opstarten. Vanaf versie 11.11.0 kunt u de volgende acties uitvoeren zonder een computer opnieuw op te starten: • patches installeren • verander de set van programma-onderdelen • installeer Kaspersky Endpoint Security over Kaspersky Security for Windows Server De standaardwaarde van de parameter varieert afhankelijk van het type besturingssysteem. Als het programma geïnstalleerd is op een werkstation, is het upgraden van het programma zonder herstartoptie uitgeschakeld. Als het programma geïnstalleerd is op een server, is het upgraden van het programma zonder herstartoptie ingeschakeld.
Compatibiliteit met externe beheersoftware *(alleen beschikbaar in de Kaspersky Security Center-console)*	Als het gebruik van Kaspersky Endpoint Security naast Remote Administration Tools (RAT) problemen veroorzaakt, kunt u de compatibiliteitsmodus inschakelen. De problemen kunnen te maken hebben met de incompatibiliteit van RAT's met de functie Secure Desktop van het programma. Het doel van deze functionaliteit is het bevestigen van acties die mogelijk het beveiligingsniveau van de computer kunnen verlagen. Met deze functionaliteit kan een programma een bevestigingsvenster weergeven dat is geïsoleerd van andere processen. Deze functionaliteit gebruikt verhoogde rechten om het verzoek te beveiligen. Op deze manier kan alleen de gebruiker de actie bevestigen en niet de malware. Als deze optie is ingeschakeld, is de RAT-compatibiliteitsmodus ingeschakeld. Het programma geeft een bevestigingsvenster weer zonder deze functionaliteit. Dit kan het beveiligingsniveau van de computer verminderen. We raden niet aan om de compatibiliteitsmodus in te schakelen als Kaspersky Endpoint Security geen problemen veroorzaakt met uw RAT. Als deze optie is uitgeschakeld, is de RAT-compatibiliteitsmodus uitgeschakeld. Het selectievakje is standaard uitgeschakeld. Voorbeeld: Wanneer u de browser in de RemoteApp-modus gebruikt, geeft Kaspersky Endpoint Security mogelijk geen bevestigingsvenster weer wanneer u een website bezoekt met een niet-vertrouwd certificaat, omdat RemoteApp de Secure Desktop-functionaliteit van het programma niet ondersteunt. Dit kan ervoor zorgen dat de browser niet meer reageert. Om de browser correct te laten werken in de RemoteApp-modus, moet u de compatibiliteitsmodus inschakelen. U kunt ook proberen de compatibiliteitsmodus in te schakelen als u problemen ondervindt met de Secure Desktop-functionaliteit bij het gebruik van andere software van derden.

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.14.1\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.14.1\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 wanneer het is geïntegreerd met Kaspersky Detection and Response-oplossingen. 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, Kaspersky Endpoint Detection and Response Expert Help, Kaspersky Anti Targeted Attack Platform Help, en Kaspersky Endpoint Detection and Response Expert (on-premises) 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
Delete reports after (days)	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.
Limit the size of report file to (MB)	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.
Delete objects after (days)	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.
Limit the size of Backup to (MB)	Als het selectievakje is ingeschakeld, is de maximale opslaggrootte beperkt tot de opgegeven waarde. De maximale grootte is standaard 1024 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.
Limit the size of Quarantine	Als het selectievakje is ingeschakeld, is de maximale Quarantainegrootte beperkt tot de opgegeven waarde. De maximale grootte is standaard 1024 MB. Wanneer Quarantaine de maximale grootte bereikt, stuurt Kaspersky Endpoint Security de gebeurtenis *Onvoldoende ruimte in Quarantaine* 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 (%)	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.

Parameter	Beschrijving
Gegevensoverdracht naar Administration Server *(alleen beschikbaar in Kaspersky Security Center)*	Categorieën van gebeurtenissen op clientcomputers waarvan de informatie moet worden verstuurd naar de Administration Server. U kunt de overdracht van bepaalde gegevens uitschakelen om de schijfruimte op de Beheerserver te optimaliseren. Het programma verstuurt gebeurtenissen van de volgende categorieën: • **About Quarantine files**. U kunt de lijst met bestanden in quarantaine bekijken in de Kaspersky Security Center-console in de map **Advanced** → **Repositories** → **Quarantine**. Kaspersky Endpoint Security gebruikt Quarantaine alleen wanneer het is geïntegreerd met Kaspersky Detection and Response-oplossingen. • **About files in Backup**. U kunt de lijst met bestanden in de back-up bekijken in de Kaspersky Security Center-console in de map **Advanced** → **Repositories** → **Backup**. • **About unprocessed files**. U kunt de lijst met onverwerkte bestanden bekijken in Kaspersky Security Center-console in de map **Advanced** → **Repositories** → **Active threats**. • **About installed devices**. U kunt de lijst met aangesloten apparaten bekijken in Kaspersky Security Center-console in de map **Advanced** → **Repositories** → **Hardware**. De lijst met apparaten is ook beschikbaar in de eigenschappen van de computer en in het beleid van Kaspersky Endpoint Security for Windows (**Apparaatcontrole** gedeelte). • **About started applications**. U kunt de lijst met uitvoerbare bestanden bekijken in Kaspersky Security Center-console in de map **Advanced** → **Application management** → **Executable files**. De lijst met uitvoerbare bestanden is ook beschikbaar in de eigenschappen van de computer. • **About file encryption errors**. U kunt de lijst met fouten die tijdens de bestandsencryptie bekijken in Kaspersky Security Center-console in de map **Advanced** → **Data encryption and protection** → **Encryption events**. De lijst met fouten is ook beschikbaar in de eigenschappen van de computer. • **Report on Adaptive Anomaly Control rules state**. U kunt bekijk het rapport in Kaspersky Security Center console in de **Administration Server** knoop op de **Reports** tabblad. Dit rapport is ook beschikbaar in de Beleidseigenschappen van Kaspersky Endpoint Security for Windows (**Adaptieve controle op afwijkingen** gedeelte). • **Report on triggered Adaptive Anomaly Control rules**. U kunt bekijk het rapport in Kaspersky Security Center console in de **Administration Server** knoop op de **Reports** tabblad. Dit rapport is ook beschikbaar in de Beleidseigenschappen van Kaspersky Endpoint Security for Windows (**Adaptieve controle op afwijkingen** gedeelte). • **About a threat development chain**. U kunt de details van de detectie bekijken in de Webconsole van Kaspersky Security Center in het **Monitoring** → **Alerts** gedeelte. De informatie over de ontwikkelingsketen voor bedreigingen wordt gebruikt door: Kaspersky Endpoint Detection and Response-oplossingen.

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 opzetten.

Netwerkopties

Parameter	Beschrijving
Beperk verkeer bij verbindingen met datalimiet	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. Kostenbewuste netwerkverbinding werkt op computers met Windows 8 of hoger.
Injecteer script in internetverkeer voor interactie met webpagina's	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 de bewaking van de internetactiviteit van gebruikers niet inschakelen. Kaspersky-experts raden aan om dit interactiescript voor webpagina's in het verkeer te injecteren om een correcte werking van Webcontrole te garanderen.
Proxyserverinstellingen	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. 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 het programma het adres van de proxyserver dat in de instellingen van Microsoft Internet Explorer is opgegeven.

Parameter	Beschrijving
Geen proxyserver gebruiken voor lokale adressen	Als het selectievakje is ingeschakeld, gebruikt Kaspersky Endpoint Security geen proxyserver wanneer een update vanuit een gedeelde map wordt uitgevoerd.
Instellingen voor authenticatie van de proxyserver	Om het programma op de proxyserver voor internettoegang te verifiëren, moet u de inloggegevens van de gebruiker invoeren. Kaspersky Endpoint Security ondersteunt automatische authenticatie op de proxyserver. Als de automatische verificatie mislukt, wordt u door het programma gevraagd de inloggegevens in te voeren. **Gebruik geen authenticatie**. **NTLM-authenticatie**. NTLM-authenticatie met het huidige gebruikersaccount (standaard). **NTLM-authenticatie met gebruikersnaam en wachtwoord**. NTLM-authenticatie met handmatig opgegeven referenties. **Gebruikersnaam en wachtwoord**. Authenticatie met handmatig opgegeven referenties. **Automatische authenticatie**. **Kerberos-authenticatie**. Kerberos-authenticatie met het huidige gebruikersaccount. Om ervoor te zorgen dat de Kerberos-authenticatie correct werkt wanneer u CNAME-records gebruikt voor het adres van de proxyserver, moet u een Service-Principal Name (SPN) registreren voor elke CNAME-record. **Kerberos-authenticatie met gebruikersnaam en wachtwoord**. Kerberos-authenticatie met handmatig opgegeven referenties. Als Kerberos-authenticatie geselecteerd is, kan Kaspersky Endpoint Security, afhankelijk van de proxyserverinstellingen, authenticatie uitvoeren dppr gebruik van het Kerberos- of NTLM-protocol.
Bewaakte poorten	**Alle netwerkpoorten bewaken**. In deze bewakingsmodus voor netwerkpoorten bewaken de beschermingsonderdelen (File Threat Protection, Web Threat Protection en Mail Threat Protection) gegevensstromen die via alle open netwerkpoorten van de computer worden verstuurd. **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 Web 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.

Parameter	Beschrijving
Vertrouwde basiscertificaten	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 verbindingsfout krijgen vanwege een certificaatprobleem. Als u wilt toevoegen aan het systeemcertificaatarchief, kunt u het groepsbeleid van Active Directory gebruiken.
Een domein bezoeken met een niet-vertrouwd certificaat	• **Toestaan**. 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 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 *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. • **Blokkeren**. 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.
Een domein bezoeken met een scanfout met geëncrypte verbindingen	• **Blokkeren**. Als een fout tijdens het scannen van een beveiligde verbinding optreedt, blokkeert Kaspersky Endpoint Security de netwerkverbinding. • **Toestaan en domein toevoegen aan uitzonderingen**. Als 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 **Blokkeren** selecteren. Kaspersky Endpoint Security genereert ook een gebeurtenis voor de fout bij het scannen van de versleutelde verbinding.
Blokkeer SSL 2.0-verbindingen	Als het selectievakje is ingeschakeld, bewaakt en blokkeert het programma netwerkverbindingen die via het SSL 2.0-protocol tot stand zijn gebracht. Als het selectievakje is uitgeschakeld, bewaakt of blokkeert het programma netwerkverbindingen die via het SSL 2.0-protocol tot stand zijn gebracht. Het programma bewaakt echter geen netwerkverkeer via dit protocol.
Blokkeer SSL 3.0-verbindingen	Als het selectievakje is ingeschakeld, blokkeert het programma netwerkverbindingen die via het SSL 3.0-protocol tot stand zijn gebracht. Als het selectievakje is uitgeschakeld, bewaakt of blokkeert het programma netwerkverbindingen die via het SSL 3.0-protocol tot stand zijn gebracht. Het programma bewaakt het netwerkverkeer via dit protocol. Alle onderdelen van het programma werken zonder beperkingen.
Blokkeer TLS 1.0-verbindingen	Als het selectievakje is ingeschakeld, blokkeert het programma netwerkverbindingen die via het TLS 1.0-protocol tot stand zijn gebracht. Als het selectievakje is uitgeschakeld, bewaakt of blokkeert het programma netwerkverbindingen die via het TLS 1.0-protocol tot stand zijn gebracht. Het programma bewaakt het netwerkverkeer via dit protocol. Alle onderdelen van het programma werken zonder beperkingen.
Ontsleutel een versleutelde verbinding met de website die een EV-certificaat gebruikt	EV-certificaten (Extended Validation Certificate) 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. Als het selectievakje is ingeschakeld, decrypt en bewaakt het programma geëncrypte verbindingen met websites die een EV-certificaat gebruiken. Als het selectievakje is uitgeschakeld, heeft het programma geen toegang tot de inhoud van HTTPS-verkeer. Om deze reden bewaakt het programma HTTPS-verkeer alleen op basis van het webadres, zoals `https://bing.com`. Als u een website met een EV-certificaat voor het eerst opent, wordt de beveiligde verbinding gedecrypt ongeacht of het selectievakje is ingeschakeld.

Parameter	Beschrijving
Configureer vertrouwde adressen	Dit gebruikt een lijst met webadressen waarvoor Kaspersky Endpoint Security geen netwerkverbindingen scant. In dit geval scant Kaspersky Endpoint Security geen HTTPS-verkeer van vertrouwde webadressen wanneer de onderdelen Web Threat Protection, Mail Threat Protection en Webcontrole hun werk doen. U kunt een domeinnaam of een IP-adres invoeren. Kaspersky Endpoint Security ondersteunt het teken `*` voor de invoer van een masker in de domeinnaam. Kaspersky Endpoint Security ondersteunt niet het symbool `*` voor IP-adressen. U kunt een bereik van IP-adressen selecteren door een subnet masker te gebruiken (bijvoorbeeld 198.51.100.0/24). Voorbeelden: • `domain.com` – de record bevat de volgende adressen: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. De record bevat geen subdomeinen (bijvoorbeeld `subdomain.domain.com`). • `subdomain.domain.com` – de record bevat de volgende adressen: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. De record bevat niet het domein `domain.com`. • `*.domain.com` – de record bevat de volgende adressen: `https://movies.domain.com`, `https://images.domain.com/page123`. De record bevat niet het domein `domain.com`.
Configureer vertrouwde programma's	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.
Om geëncrypte verbindingen te scannen in programma's met hun eigen certificaatopslag, gebruik *(alleen beschikbaar in de Kaspersky Endpoint Security-interface)*	Als dit selectievakje is ingeschakeld, scant het programma geëncrypt verkeer in de Mozilla Firefox-browser en Thunderbird-mailclient. Het openen van bepaalde websites via het HTTPS-protocol wordt mogelijk geblokkeerd. 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 het programma geen versleuteld verkeer in de Mozilla Firefox-browser en Thunderbird-mailclient. Het programma gebruikt het Kaspersky-rootcertificaat om geëncrypt verkeer te decrypten en te analyseren. U kunt de certificaatopslag voor het Kaspersky-rootcertificaat selecteren. • **Windows-certificaatarchief (aanbevolen)**. Het Kaspersky-rootcertificaat wordt aan deze opslag toegevoegd tijdens de installatie van Kaspersky Endpoint Security. • **Eigen certificaatopslag**. 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.

Interface

U kunt de instellingen van de programma-interface configureren.

Interface-instellingen

Parameter	Beschrijving
Interactie met gebruiker *(alleen beschikbaar in de Kaspersky Security Center-console)*	**Vereenvoudigde interface weergeven**. 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 alleen meldingen die een actie van de gebruiker vereisen boven het programmapictogram. **Gebruikersinterface weergeven**. 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. **Bewaking van programma-activiteit verbergen**. Op de clientcomputer is de knop **Bewaking van programma-activiteit** niet beschikbaar in het hoofdvenster van Kaspersky Endpoint Security. *Bewaking van programma-activiteit* is een tool ontworpen voor de realtime weergave van informatie over de activiteit van de computer van een gebruiker. **Gebruikersinterface niet weergeven**. Op een clientcomputer wordt de werking van Kaspersky Endpoint Security niet aangegeven. Het pictogram in het Windows-systeemvak en de meldingen zijn niet beschikbaar.

Parameter	Beschrijving
Meldingen configureren	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.
E-mailmeldingen configureren	De SMTP-serverinstellingen voor de levering van meldingen over gebeurtenissen die zich tijdens de werking van het programma voordoen. Kaspersky Endpoint Security gebruikt standaard instellingen voor e-mailmeldingen van Kaspersky Security Center. Voor meer informatie over de instellingen voor e-mailmeldingen raadpleegt u de Help van Kaspersky Security Center. Als u individuele e-mailmeldingen moet configureren, kunt u de volgende instellingen bewerken: • **Adres van afzender**. E-mailadres van de afzender. Het is aangeraden een niet bestaand adres te gebruiken. • **SMTP-server**. Een of meer adressen van e-mailservers van uw organisatie (bijvoorbeeld `mail.company.com`). U kunt een IP-adres (IPv4 of IPv6) invoeren. Om de gebruiker op de SMTP-server te authenticeren, voert u de gegevens van de afzender in de overeenkomstige velden in. Om e-mailmeldingen te testen, kunt u een testbericht verzenden. • **Adres van ontvanger**. E-mailadressen van ontvangers naar wie het programma meldingen zal sturen. • **Verzendmodus**. Verzendmodus van e-mailmeldingen. Kaspersky Endpoint Security kan onmiddellijk berichten verzenden wanneer er een gebeurtenis plaatsvindt; als alternatief kan het een vooraf geconfigureerd schema volgen.
Toon status van het programma in het systeemvak	Categorieën van programmagebeurtenissen die ervoor zorgen dat het Kaspersky Endpoint Security-pictogram in het systeemvak van de Microsoft Windows-taakbalk wijzigt (of) en leiden tot een pop-upmelding.
Statusmeldingen van lokale anti-malwaredatabase	Instellingen van meldingen over verouderde antivirusdatabases die door het programma worden gebruikt.
Wachtwoordbeveiliging	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. Na de inschakeling van Wachtwoordbeveiliging wordt u door Kaspersky Endpoint Security gevraagd om een wachtwoord voor de KLAdmin-account in te stellen.
Gebruikersondersteuning / Koppelingen naar webbronnen *(alleen beschikbaar in de Kaspersky Security Center-console)*	Lijst met koppelingen naar webbronnen met informatie over technische ondersteuning voor Kaspersky Endpoint Security. Toegevoegde koppelingen worden in plaats van de standaardkoppelingen weergegeven in het venster **Support** van de lokale Kaspersky Endpoint Security-interface.
Gebruikersondersteuning / Beschrijving *(alleen beschikbaar in de Kaspersky Security Center-console)*	Bericht dat wordt weergegeven in het venster **Support** 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.

Instellingen	Beschrijving
Importeren	Pak de programma-instellingen uit een bestand met CFG-indeling uit en pas ze toe.
Exporteren	Sla de huidige programma-instellingen in een bestand met CFG-indeling op.
Terugzetten	U kunt de door Kaspersky aanbevolen programma-instellingen op elk moment herstellen. Wanneer de instellingen zijn hersteld, wordt het **Aanbevolen** 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.

Update-functionaliteit (inclusief het leveren van updates van antivirussignaturen en codebase-updates) is mogelijk niet beschikbaar in het programma in de Verenigde Staten.

Voor periodieke updates hebt u een actieve licentie nodig. Zonder actieve licentie kunt u maar één keer een update uitvoeren.

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.

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.

Als het programma in de Light Agent-modus werkt, zijn er speciale overwegingen bij het bijwerken van programmadatabases en modules.

Instellingen voor programmamodule en database-update

Parameter	Beschrijving
Planning van database-updates	**Automatisch**. In deze modus controleert het programma 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. **Manually**. Met deze uitvoermodus voor updatetaken kunt u een updatetaak handmatig starten. **By schedule**. 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.
Run missed tasks	Als het selectievakje is ingeschakeld, wordt de overgeslagen taak door Kaspersky Endpoint Security gestart zodra dit mogelijk is. De taak kan bijvoorbeeld worden overgeslagen als de computer uitgeschakeld was op de starttijd van de taak. Als het programma een kans krijgt om gemiste taken uit te voeren, start het de taken willekeurig binnen een bepaalde tijdsinterval om de lading voor de computer te spreiden. Als het selectievakje is uitgeschakeld, worden overgeslagen taken niet gestart door Kaspersky Endpoint Security. In plaats daarvan voert het de volgende taak uit volgens het huidige schema.

Parameter	Beschrijving
Updatebronnen	Een *updatebron* is een bron die updates voor de databases en de programmamodules van Kaspersky Endpoint Security bevat. Updatebronnen zijn onder andere de server van Kaspersky Security Center, Kaspersky-updateservers en netwerk- of lokale mappen. Als de Kaspersky updateservers niet beschikbaar zijn, kan Kaspersky Endpoint Security alternatieve domeinen gebruiken om de databases en softwaremodules van het programma bij te werken. Raadpleeg de Knowledge Base van de Technische Support voor gedetailleerde informatie. 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. Kaspersky Endpoint Security gebruikt standaard de Kaspersky Security Center-server als eerste updatebron. Dit helpt verkeer te besparen tijdens het updaten. Als een beleid niet op de computer wordt toegepast, worden Kaspersky-servers geselecteerd als de eerste updatebron in de instellingen van de lokale taak *Update van databases en programmamodules* omdat het programma mogelijk geen toegang heeft tot de Kaspersky Security Center-server. Als het programma in Light Agent-modus draait, wordt een map op de SVM geselecteerd als updatebron.
Start database-updates als	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 programma-instellingen 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. Het selectievakje is standaard ingeschakeld.
Updates naar map kopiëren	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.14.1\Update distribution\`.

Parameter	Beschrijving
Proxyserver voor updates *(alleen beschikbaar in de Kaspersky Endpoint Security-interface)*	Proxyserverinstellingen voor internettoegang van gebruikers van clientcomputers om programmamodules en databases bij te werken. 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.
Gebruik geen proxyserver voor lokale adressen *(alleen beschikbaar in de Kaspersky Endpoint Security-interface)*	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-welkomstscherm

cpl – module van Microsoft Windows-configuratiescherm

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 – hypertekstdocument

htt – Microsoft Windows-hypertekstkop

hta – hypertekstprogramma voor Microsoft Internet Explorer®

asp – Active Server Pages-script

chm – gecompileerd HTML-bestand

pht – HTML-bestand met geïntegreerde PHP-scripts

php – script dat in HTML-bestanden is geïntegreerd

wsh – Microsoft Windows Script Host-bestand

wsf – Microsoft Windows-script

the – Microsoft Windows 95-bureaubladbestand

hlp – Win Help-bestand

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

fpm – databaseprogramma, Microsoft Visual FoxPro-opstartbestand

rtf – Rich Text Format-document

shs – Windows Shell Scrap Object Handler-fragment

dwg – AutoCAD®-tekeningdatabase

msi – Microsoft Windows Installer-pakket

otm – VBA-project voor Microsoft Office Outlook

pdf – Adobe Acrobat-document

swf – Shockwave® Flash-pakketobject

jpg, jpeg – indeling van gecomprimeerde afbeeldingen

emf – Enhanced Metafile-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, xlsm voor Microsoft Office Excel 2007-sjablonen met macro-ondersteuning en xlam voor Microsoft Office Excel 2007-invoegtoepassingen met macro-ondersteuning

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

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

sldx – een Microsoft PowerPoint 2007-dia

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

thmx – een Microsoft Office 2007-thema

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-welkomstscherm

cpl – module van Microsoft Windows-configuratiescherm

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 – hypertekstdocument

htt – Microsoft Windows-hypertekstkop

hta – hypertekstprogramma voor Microsoft Internet Explorer®

asp – Active Server Pages-script

chm – gecompileerd HTML-bestand

pht – HTML-bestand met geïntegreerde PHP-scripts

php – script dat in HTML-bestanden is geïntegreerd

wsh – Microsoft Windows Script Host-bestand

wsf – Microsoft Windows-script

the – Microsoft Windows 95-bureaubladbestand

hlp – Win Help-bestand

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

fpm – databaseprogramma, Microsoft Visual FoxPro-opstartbestand

rtf – Rich Text Format-document

shs – Windows Shell Scrap Object Handler-fragment

dwg – AutoCAD®-tekeningdatabase

msi – Microsoft Windows Installer-pakket

otm – VBA-project voor Microsoft Office Outlook

pdf – Adobe Acrobat-document

swf – Shockwave® Flash-pakketobject

jpg, jpeg – indeling van gecomprimeerde afbeeldingen

emf – Enhanced Metafile-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, xlsm voor Microsoft Office Excel 2007-sjablonen met macro-ondersteuning en xlam voor Microsoft Office Excel 2007-invoegtoepassingen met macro-ondersteuning

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

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

sldx – een Microsoft PowerPoint 2007-dia

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

thmx – een Microsoft Office 2007-thema

Appendix 5. Netwerkinstellingen 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 de volgende netwerkinstellingen voor interactie met externe services.

Netwerkinstellingen

Adres	Beschrijving
`activation-v2.kaspersky.com/activationservice/activationservice.svc` Protocol: `HTTPS` Poort: `443`	Programma activeren.

Adres	Beschrijving

`s00.upd.kaspersky.com`
`s01.upd.kaspersky.com`
`s02.upd.kaspersky.com`
`s03.upd.kaspersky.com`
`s04.upd.kaspersky.com`
`s05.upd.kaspersky.com`
`s06.upd.kaspersky.com`
`s07.upd.kaspersky.com`
`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`
	Databases en softwaremodules van het programma bijwerken.

`downloads.upd.kaspersky.com` Protocol: `HTTPS` Poort: `443`	• Databases en softwaremodules van het programma bijwerken. • Toegang tot Kaspersky-servers verifiëren. 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). 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.
`touch.kaspersky.com` Protocol: `HTTP`	• Het ontvangen van de vertrouwde tijd voor het controleren van de geldigheidsperiode van het certificaat (TLS-verbinding). • Waarschuwing over geweigerde toegang tot een webbron in de browser wanneer Web Threat Protection actief is.

Adres	Beschrijving

`p00.upd.kaspersky.com`
`p01.upd.kaspersky.com`
`p02.upd.kaspersky.com`
`p03.upd.kaspersky.com`
`p04.upd.kaspersky.com`
`p05.upd.kaspersky.com`
`p06.upd.kaspersky.com`
`p07.upd.kaspersky.com`
`p08.upd.kaspersky.com`
`p09.upd.kaspersky.com`
`p10.upd.kaspersky.com`
`p11.upd.kaspersky.com`
`p12.upd.kaspersky.com`
`p13.upd.kaspersky.com`
`p14.upd.kaspersky.com`
`p15.upd.kaspersky.com`
`p16.upd.kaspersky.com`
`p17.upd.kaspersky.com`
`p18.upd.kaspersky.com`
`p19.upd.kaspersky.com`
`downloads.kaspersky-labs.com`
`cm.k.kaspersky-labs.com`
Protocol: `HTTP`
Poort: `80`
	Databases en softwaremodules van het programma bijwerken.

`ds.kaspersky.com`
`dc1.ksn.kaspersky-labs.com`
`dc1-file.ksn.kaspersky-labs.com`
`dc1-pp.ksn.kaspersky-labs.com`
`dc1-st.ksn.kaspersky-labs.com`
Protocol: `HTTPS`
Poort: `443`
	Bij het gebruik van Kaspersky Security Network.

`ksn-a-stat-geo.kaspersky-labs.com`
`ksn-file-geo.kaspersky-labs.com`
`ksn-verdict-geo.kaspersky-labs.com`
`ksn-url-geo.kaspersky-labs.com`
`ksn-a-p2p-geo.kaspersky-labs.com`
`ksn-info-geo.kaspersky-labs.com`
`ksn-cinfo-geo.kaspersky-labs.com`
Protocol: `KSN`
Poort: `443`, `1443`
	Bij het gebruik van Kaspersky Security Network.

`click.kaspersky.com`
`redirect.kaspersky.com`
Protocol: `HTTPS`
Poort: `443`
	Volg links vanuit de interface.

Instellingen, gebruikt voor encryptie.

Adres	Beschrijving

`crl.kaspersky.com`
`ocsp.kaspersky.com`
Protocol: `HTTP`
Poort: `80`
	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 malwarescantaak, 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` – *Info*, `2` – *Warning*, `3` – *Functional failure*, `4` – *Critical*.
- `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.

Hoe lang gebeurtenissen worden opgeslagen op de server

Kritiek

License expired

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)	✓

The application established a connection to a website with an untrusted certificate

Status	ⓘ
Onderdeel	Systeemaudit
Windows-gebeurtenissen ID	57
Kaspersky Security Center gebeurtenis ID	00000039

Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Failed to verify an encrypted connection. The domain is added to the list of exclusions

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 Web Threat Protection Mail Threat Protection AMSI-bescherming Host Intrusion Prevention Gedragsdetectie Anti-Cryptor Exploit-preventie Malware-scan
Windows-gebeurtenissen ID	`302`
Kaspersky Security Center gebeurtenis ID	`GNRL_EV_VIRUS_FOUND`
Gebeurtenisparameters	• `GNRL_EA_PARAM_1` is de hash van het object (SHA256). • `GNRL_EA_PARAM_2` is de naam van het object. Wanneer externe encryptie van gedeelde mappen wordt gedetecteerd, toont het programma het pad naar het doelbestand. • `GNRL_EA_PARAM_5` is de naam van de dreiging in overeenstemming met de Kaspersky-classificatie, bijvoorbeeld `EICAR-Test-File`. • `GNRL_EA_PARAM_7` is de naam van de sessiegebruiker. • `GNRL_EA_PARAM_8` is het type dreiging (`type`). • `GNRL_EA_PARAM_9` is bijkomende informatie over het gedetecteerde object: Programmacomponent (`engine`). Threat detection technology (`method`). Dreiging gedetecteerd door Kaspersky Private Security Network (`blacklist`): `true` of `false`. EDR-versie. Identificatie van dreiging in EDR. MD5 hash van het object.
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Malicious object detected (KSN)

Status	ⓘ
Onderdeel	File Threat Protection Web Threat Protection Mail Threat Protection AMSI-bescherming Host Intrusion Prevention Gedragsdetectie Anti-Cryptor Exploit-preventie Malware-scan
Windows-gebeurtenissen ID	`302`
Kaspersky Security Center gebeurtenis ID	`GNRL_EV_VIRUS_FOUND_BY_KSN`
Gebeurtenisparameters	• `GNRL_EA_PARAM_1` is de hash van het object (SHA256). • `GNRL_EA_PARAM_2` is de naam van het object. • `GNRL_EA_PARAM_5` is de naam van de dreiging in overeenstemming met de Kaspersky-classificatie, bijvoorbeeld `EICAR-Test-File`. • `GNRL_EA_PARAM_7` is de naam van de sessiegebruiker. • `GNRL_EA_PARAM_8` is het type dreiging (`type`). • `GNRL_EA_PARAM_9` is bijkomende informatie over het gedetecteerde object: Programmacomponent (`engine`). Threat detection technology (`method`). Dreiging gedetecteerd door Kaspersky Private Security Network (`blacklist`): `true` of `false`. EDR-versie. Identificatie van dreiging in EDR. MD5 hash van het object.
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Disinfection impossible

Status	ⓘ
Onderdeel	File Threat Protection Mail Threat Protection Host Intrusion Prevention Gedragsdetectie Anti-Cryptor Malware-scan
Windows-gebeurtenissen ID	`312`
Kaspersky Security Center gebeurtenis ID	`GNRL_EV_OBJECT_NOTCURED`
Gebeurtenisparameters	• `GNRL_EA_PARAM_1` is de hash van het object (SHA256). • `GNRL_EA_PARAM_2` is de naam van het object. • `GNRL_EA_PARAM_5` is de naam van de dreiging in overeenstemming met de Kaspersky-classificatie, bijvoorbeeld `EICAR-Test-File`. • `GNRL_EA_PARAM_7` is de naam van de sessiegebruiker. • `GNRL_EA_PARAM_8` is het type dreiging (`type`). • `GNRL_EA_PARAM_9` is bijkomende informatie over het gedetecteerde object: Programmacomponent (`engine`). Threat detection technology (`method`). Dreiging gedetecteerd door Kaspersky Private Security Network (`blacklist`): `true` of `false`. EDR-versie. Identificatie van dreiging in EDR. MD5 hash van het object.
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Cannot be deleted

Status	⚠
Onderdeel	File Threat Protection Host Intrusion Prevention Gedragsdetectie Anti-Cryptor Malware-scan
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 Web Threat Protection Mail Threat Protection Host Intrusion Prevention AMSI-bescherming Malware-scan
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 Host Intrusion Prevention Gedragsdetectie Malware-scan
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 Host Intrusion Prevention Gedragsdetectie Malware-scan
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	• GNRL_EA_PARAM_2 is het pad naar het object. • GNRL_EA_PARAM_5 is de naam van het object volgens de Kaspersky-classificatie. • GNRL_EA_PARAM_7 is de naam van de sessiegebruiker. • GNRL_EA_PARAM_8 is het type dreiging (type). • GNRL_EA_PARAM_9 is bijkomende informatie over het gedetecteerde object: Programmacomponent (engine). Threat detection technology (method). Dreiging gedetecteerd door Privaat KSN (blacklist): true of false.
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	• GNRL_EA_PARAM_2 is het pad naar het object. • GNRL_EA_PARAM_5 is de naam van het object volgens de Kaspersky-classificatie. • GNRL_EA_PARAM_7 is de naam van de sessiegebruiker. • GNRL_EA_PARAM_8 is het type dreiging (type). • GNRL_EA_PARAM_9 is bijkomende informatie over het gedetecteerde object: Programmacomponent (engine). Threat detection technology (method). Dreiging gedetecteerd door Privaat KSN (blacklist): true of false.
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	• GNRL_EA_PARAM_2 is het pad naar het object. • GNRL_EA_PARAM_5 is de naam van het object volgens de Kaspersky-classificatie. • GNRL_EA_PARAM_7 is de naam van de sessiegebruiker. • GNRL_EA_PARAM_8 is het type dreiging (type). • GNRL_EA_PARAM_9 is bijkomende informatie over het gedetecteerde object: Programmacomponent (engine). Threat detection technology (method). Dreiging gedetecteerd door Privaat KSN (blacklist): true of false.

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	• `GNRL_EA_PARAM_1` is de naam van de regel voor Adaptieve controle op afwijkingen. • `GNRL_EA_PARAM_2` is de ID van de heuristische regel. • `GNRL_EA_PARAM_3` is de naam van de sessiegebruiker. • `GNRL_EA_PARAM_4` is het bronproces. • `GNRL_EA_PARAM_5` is het bronobject. • `GNRL_EA_PARAM_6` is het doelproces. • `GNRL_EA_PARAM_7` is het doelobject. • `GNRL_EA_PARAM_8` is bijkomende informatie over het gedetecteerde object: Controlesommen van het bronproces/object en het doelproces/object. Proces geblokkeerd (`verdict_type`): `true` of `false`. User security ID (SID).
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	• `GNRL_EA_PARAM_1` is de naam van de aanval. • `GNRL_EA_PARAM_2` is het protocol. • `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`. • `GNRL_EA_PARAM_4` is het poortnummer. • `GNRL_EA_PARAM_5` is een IPv6-adres, bijvoorbeeld `12B012B012B012B012B012B012B012B0`. • `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`.
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	• `GNRL_EA_PARAM_2` is de naam van de sessiegebruiker. • `GNRL_EA_PARAM_3` is de handmatig aangemaakte categorie-ID. • `GNRL_EA_PARAM_4` is de programmacategorie-ID. • `GNRL_EA_PARAM_5` is informatie over de digitale handtekening van het programma. • `GNRL_EA_PARAM_6` is de naam van het uitvoerbare bestand van het programma (bijvoorbeeld chrome.exe). • `GNRL_EA_PARAM_7` is het pad naar het uitvoerbare bestand. • `GNRL_EA_PARAM_8` is de hash van het object (SHA256). • `GNRL_EA_PARAM_9` is de versie van het programma die de gebruiker probeert uit te voeren.
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	• GNRL_EA_PARAM_1 is de URL. • GNRL_EA_PARAM_2 is de naam van de sessiegebruiker. • GNRL_EA_PARAM_3 is de naam van de Webcontrole-regel.
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	• GNRL_EA_PARAM_1 is de URL. • GNRL_EA_PARAM_2 is de naam van de sessiegebruiker. • GNRL_EA_PARAM_3 is de naam van de Webcontrole-regel.
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	• GNRL_EA_PARAM_1 is de Hardware-ID (HWID). • GNRL_EA_PARAM_2 is de naam van de sessiegebruiker.
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	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	Update
Windows-gebeurtenissen ID	1012
Kaspersky Security Center gebeurtenis ID	000003f4
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Local update error

Status	⚠
Onderdeel	Update
Windows-gebeurtenissen ID	1014
Kaspersky Security Center gebeurtenis ID	000003f6
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Network update error

Status	⚠
Onderdeel	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	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	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	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	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	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	Update
Windows-gebeurtenissen ID	2153
Kaspersky Security Center gebeurtenis ID	00000869
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Patch rollback failed

Status	!
Onderdeel	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	• GNRL_EA_PARAM_1 is het pad naar het bestand. • GNRL_EA_PARAM_2 is de oorzaak van de fout. • GNRL_EA_PARAM_3 is het type apparaat.
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	• GNRL_EA_PARAM_1 is het doelobject. • GNRL_EA_PARAM_2 is de naam van de sessiegebruiker. • 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.
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

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

Status	ⓘ
Onderdeel	Systeemaudit
Windows-gebeurtenissen ID	1312
Kaspersky Security Center gebeurtenis ID	00000520
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

FDE upgrade failed

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)

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	Sandbox
Windows-gebeurtenissen ID	2252
Kaspersky Security Center gebeurtenis ID	000008cc
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Object not quarantined (Sandbox)

Status	ⓘ
Onderdeel	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	Sandbox
Windows-gebeurtenissen ID	2607
Kaspersky Security Center gebeurtenis ID	00000a2f
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Invalid Sandbox server certificate

Status	ⓘ
Onderdeel	Sandbox
Windows-gebeurtenissen ID	2613
Kaspersky Security Center gebeurtenis ID	00000a35
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

The Sandbox node is unavailable

Status	ⓘ
Onderdeel	Sandbox
Windows-gebeurtenissen ID	2614
Kaspersky Security Center gebeurtenis ID	00000a36
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Failed to process the object in Sandbox

Status	ⓘ
Onderdeel	Sandbox
Windows-gebeurtenissen ID	2617
Kaspersky Security Center gebeurtenis ID	00000a39
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Maximum load to Sandbox is exceeded

Status	ⓘ
Onderdeel	Sandbox
Windows-gebeurtenissen ID	2618
Kaspersky Security Center gebeurtenis ID	00000a3a
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

IOC found

Status	ⓘ
Onderdeel	Endpoint Detection and Response
Windows-gebeurtenissen ID	2651
Kaspersky Security Center gebeurtenis ID	00000a5b
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Sandbox license verification failed

Status	ⓘ
Onderdeel	Sandbox
Windows-gebeurtenissen ID	2620
Kaspersky Security Center gebeurtenis ID	00000a3c
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Het verzenden van de scantaak naar Sandbox door een gebruiker is mislukt

Status	ⓘ
Onderdeel	Sandbox
Windows-gebeurtenissen ID	2623
Kaspersky Security Center gebeurtenis ID	00000a3e
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Fout bij het maken van Sandbox-taak

Status	ⓘ
Onderdeel	Sandbox
Windows-gebeurtenissen ID	2621
Kaspersky Security Center gebeurtenis ID	00000a3d
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)	✓

Process startup blocked

Status	ⓘ
Onderdeel	Endpoint Detection and Response
Windows-gebeurtenissen ID	2551
Kaspersky Security Center gebeurtenis ID	000009f7
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Script execution blocked

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)	✓

Process startup is not blocked

Status	ⓘ
Onderdeel	Endpoint Detection and Response
Windows-gebeurtenissen ID	2561
Kaspersky Security Center gebeurtenis ID	00000a01
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Object is not blocked

Status	ⓘ
Onderdeel	Endpoint Detection and Response
Windows-gebeurtenissen ID	2562
Kaspersky Security Center gebeurtenis ID	00000a02
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Script execution is not blocked

Status	ⓘ
Onderdeel	Endpoint Detection and Response
Windows-gebeurtenissen ID	2563
Kaspersky Security Center gebeurtenis ID	00000a03
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)	✓

There are patterns of a possible brute-force attack in the system

Status	!
Onderdeel	Log Inspectie
Windows-gebeurtenissen ID	2800
Kaspersky Security Center gebeurtenis ID	00000af0
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

There are patterns of a possible Windows Event Log abuse

Status	!
Onderdeel	Log Inspectie
Windows-gebeurtenissen ID	2801
Kaspersky Security Center gebeurtenis ID	00000af1
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Atypical actions detected on behalf of a new service installed

Status	!
Onderdeel	Log Inspectie
Windows-gebeurtenissen ID	2802
Kaspersky Security Center gebeurtenis ID	00000af2
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Atypical logon that uses explicit credentials detected

Status	!
Onderdeel	Log Inspectie
Windows-gebeurtenissen ID	2803
Kaspersky Security Center gebeurtenis ID	00000af3
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

There are patterns of a possible Kerberos forged PAC (MS14-068) attack in the system

Status	!
Onderdeel	Log Inspectie
Windows-gebeurtenissen ID	2804
Kaspersky Security Center gebeurtenis ID	00000af4
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Suspicious changes detected in the privileged built-in Administrators group

Status	!
Onderdeel	Log Inspectie
Windows-gebeurtenissen ID	2805
Kaspersky Security Center gebeurtenis ID	00000af5
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

There is an atypical activity detected during a network logon session

Status	!
Onderdeel	Log Inspectie
Windows-gebeurtenissen ID	2806
Kaspersky Security Center gebeurtenis ID	00000af6
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Log Inspection rule triggered

Status	!
Onderdeel	Log Inspectie
Windows-gebeurtenissen ID	2807
Kaspersky Security Center gebeurtenis ID	00000af7
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Atypical event occurs too often. Event aggregation started

Status	!
Onderdeel	Log Inspectie
Windows-gebeurtenissen ID	2808
Kaspersky Security Center gebeurtenis ID	00000af8
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Report on an atypical event for the aggregation period

Status	!
Onderdeel	Log Inspectie
Windows-gebeurtenissen ID	2809
Kaspersky Security Center gebeurtenis ID	00000af9
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Error connecting to the EDR Expert server

Status	ⓘ
Onderdeel	Endpoint Detection and Response Expert (on-premises)
Windows-gebeurtenissen ID	2850
Kaspersky Security Center gebeurtenis ID	00000b22
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Invalid certificate of the EDR Expert server

Status	ⓘ
Onderdeel	Endpoint Detection and Response Expert (on-premises)
Windows-gebeurtenissen ID	2851
Kaspersky Security Center gebeurtenis ID	00000b23
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Invalid certificate of the agent on the EDR Expert server

Status	ⓘ
Onderdeel	Endpoint Detection and Response Expert (on-premises)
Windows-gebeurtenissen ID	2852
Kaspersky Security Center gebeurtenis ID	00000b24
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Fout bij verbinden met de EDR Expert Responses-server

Status	ⓘ
Onderdeel	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows-gebeurtenissen ID	2858
Kaspersky Security Center gebeurtenis ID	00000b22
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Ongeldig certificaat van de EDR Expert reactieserver

Status	ⓘ
Onderdeel	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows-gebeurtenissen ID	2859
Kaspersky Security Center gebeurtenis ID	00000b23
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Ongeldig certificaat van de agent op de EDR Expert reactieserver

Status	ⓘ
Onderdeel	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows-gebeurtenissen ID	2860
Kaspersky Security Center gebeurtenis ID	00000b24
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

EDR Expert Telemetrieverzamelingsserver-verbindingsfout

Status	ⓘ
Onderdeel	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows-gebeurtenissen ID	2854
Kaspersky Security Center gebeurtenis ID	00000b22
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Ongeldig certificaat van de EDR Expert telemetrieverzamelingsserver

Status	ⓘ
Onderdeel	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows-gebeurtenissen ID	2855
Kaspersky Security Center gebeurtenis ID	00000b23
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Ongeldig certificaat van de agent op de EDR Expert telemetrieverzamelingsserver

Status	ⓘ
Onderdeel	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows-gebeurtenissen ID	2856
Kaspersky Security Center gebeurtenis ID	00000b24
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Fout bij verbinden met de NDR-server

Status	ⓘ
Onderdeel	Network Detection and Response (KATA)
Windows-gebeurtenissen ID	3080
Kaspersky Security Center gebeurtenis ID	00000c08

Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Ongeldig certificaat van de NDR-server

Status	ⓘ
Onderdeel	Network Detection and Response (KATA)
Windows-gebeurtenissen ID	3081
Kaspersky Security Center gebeurtenis ID	00000c09
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Ongeldig certificaat van de agent op de NDR-server

Status	ⓘ
Onderdeel	Network Detection and Response (KATA)
Windows-gebeurtenissen ID	3082
Kaspersky Security Center gebeurtenis ID	00000c0a
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Uw apparaat is verbonden met de niet-vertrouwde Administration Server. Neem contact op met de beheerder

Status	ⓘ
Onderdeel	Administration Server verbindingsbescherming
Windows-gebeurtenissen ID	3301
Kaspersky Security Center gebeurtenis ID	00000ce5
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

File or folder change was detected

Status	ⓘ / ⚠ / ⓘ
Onderdeel	Systeemintegriteitscontrole
Windows-gebeurtenissen ID	2950
Kaspersky Security Center gebeurtenis ID	00000b86
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Om de bewaarperiode voor deze gebeurtenis te configureren, ga naar de **Event configuration** van het beleid en stel de bewaarperiode in voor de algemene gebeurtenis Systeemintegriteitscontrole: *File or folder change was detected*.

Object changes too often. Event aggregation started

Status	/ /
Onderdeel	Systeemintegriteitscontrole
Windows-gebeurtenissen ID	2955
Kaspersky Security Center gebeurtenis ID	00000b8b
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Report on object modification for the aggregation period

Status	/ /
Onderdeel	Systeemintegriteitscontrole
Windows-gebeurtenissen ID	2956
Kaspersky Security Center gebeurtenis ID	00000b8c
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Om de bewaarperiode voor deze gebeurtenis te configureren, ga naar de **Event configuration** van het beleid en stel de bewaarperiode in voor de algemene gebeurtenis Systeemintegriteitscontrole: *File or folder change was detected*.

Monitoring scope includes incorrect objects

Status	
Onderdeel	Systeemintegriteitscontrole
Windows-gebeurtenissen ID	2953
Kaspersky Security Center gebeurtenis ID	00000b89
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Registry change was detected

Status	/ /
Onderdeel	Systeemintegriteitscontrole
Windows-gebeurtenissen ID	2951
Kaspersky Security Center gebeurtenis ID	00000b87
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Om de bewaarperiode voor deze gebeurtenis te configureren, ga naar de **Event configuration** van het beleid en stel de bewaarperiode in voor de algemene gebeurtenis Systeemintegriteitscontrole: *File or folder change was detected*.

Device connection / disconnection is detected

Status	/ /
Onderdeel	Systeemintegriteitscontrole

Windows-gebeurtenissen ID	2952
Kaspersky Security Center gebeurtenis ID	00000b88
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Om de bewaarperiode voor deze gebeurtenis te configureren, ga naar de **Event configuration** van het beleid en stel de bewaarperiode in voor de algemene gebeurtenis Systeemintegriteitscontrole: *File or folder change was detected*.

Bereik van bewaking bevat onjuiste objecten

Status	ⓘ / ⚠ / ⓘ
Onderdeel	Systeemintegriteitscontrole
Windows-gebeurtenissen ID	2903
Kaspersky Security Center gebeurtenis ID	00000b89
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Om de bewaarperiode voor deze gebeurtenis te configureren, ga naar de **Event configuration** van het beleid en stel de bewaarperiode in voor de algemene gebeurtenis Systeemintegriteitscontrole: *File or folder change was detected*.

Attempts to perform the restricted operations with the object is too many. Event aggregation started

Status	ⓘ
Onderdeel	Systeemintegriteitscontrole
Windows-gebeurtenissen ID	2963
Kaspersky Security Center gebeurtenis ID	00000b93
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

An operation with the files of the monitoring scope was blocked

Status	ⓘ
Onderdeel	Systeemintegriteitscontrole
Windows-gebeurtenissen ID	2959
Kaspersky Security Center gebeurtenis ID	00000b8f
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Om de bewaarperiode voor deze gebeurtenis te configureren, ga naar de **Event configuration** van het beleid en stel de bewaarperiode in voor de algemene gebeurtenis Systeemintegriteitscontrole: *File or folder change was detected*.

Registry modification blocked

Status	⚠
Onderdeel	Systeemintegriteitscontrole
Windows-gebeurtenissen ID	2960
Kaspersky Security Center gebeurtenis ID	00000b90
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Om de bewaarperiode voor deze gebeurtenis te configureren, ga naar de **Event configuration** van het beleid en stel de bewaarperiode in voor de algemene gebeurtenis Systeemintegriteitscontrole: *File or folder change was detected*.

Processing error

Status	⚠
Onderdeel	Systeemintegriteitscontrole
Windows-gebeurtenissen ID	2954
Kaspersky Security Center gebeurtenis ID	00000b8a
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

System Integrity Monitoring: rule triggering disabled for user accounts without matching security identifier (SID)

Status	⚠
Onderdeel	Systeemintegriteitscontrole
Windows-gebeurtenissen ID	2964
Kaspersky Security Center gebeurtenis ID	00000b94
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Application Control: rule triggering disabled for user accounts without matching security identifier (SID)

Status	⚠
Onderdeel	Programmacontrole
Windows-gebeurtenissen ID	711
Kaspersky Security Center gebeurtenis ID	000002c7
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Device Control: rule triggering disabled for user accounts without matching security identifier (SID)

Status	⚠
Onderdeel	Apparaatcontrole
Windows-gebeurtenissen ID	810
Kaspersky Security Center gebeurtenis ID	0000032a

Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Web Control: rule triggering disabled for user accounts without matching security identifier (SID)

Status	⚠
Onderdeel	Webcontrole
Windows-gebeurtenissen ID	757
Kaspersky Security Center gebeurtenis ID	000002f5
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Adaptive Anomaly Control: rule triggering disabled for user accounts without matching security identifier (SID)

Status	⚠
Onderdeel	Adaptieve controle op afwijkingen
Windows-gebeurtenissen ID	504
Kaspersky Security Center gebeurtenis ID	000001f8
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Log Inspection: rule triggering disabled for user accounts without matching security identifier (SID)

Status	⚠
Onderdeel	Log Inspectie
Windows-gebeurtenissen ID	2810
Kaspersky Security Center gebeurtenis ID	00000afa
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Unable to connect to the Integration Server for more than 6 hours. Check Integration Server status and network settings

Status	⚠
Onderdeel	Light Agent
Windows-gebeurtenissen ID	3103
Kaspersky Security Center gebeurtenis ID	00000c1f
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

SVM is unavailable

Status	⚠
Onderdeel	Light Agent
Windows-gebeurtenissen ID	3151

Kaspersky Security Center gebeurtenis ID	00000c4f
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Malicious object detected. Advanced Disinfection should be started on a virtual machine template

Status	ⓘ
Onderdeel	Light Agent
Windows-gebeurtenissen ID	3182
Kaspersky Security Center gebeurtenis ID	00000c6e
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

De netwerkverbinding die via het verouderde protocol tot stand is gebracht, is geblokkeerd

Status	ⓘ
Onderdeel	Bescherming
Windows-gebeurtenissen ID	75
Kaspersky Security Center gebeurtenis ID	0000004b
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

KUMA-serververbindingsfout

Status	ⓘ
Onderdeel	KUMA-integratie
Windows-gebeurtenissen ID	2854
Kaspersky Security Center gebeurtenis ID	00000b26
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Ongeldig certificaat van de KUMA-server

Status	ⓘ
Onderdeel	KUMA-integratie
Windows-gebeurtenissen ID	2855
Kaspersky Security Center gebeurtenis ID	00000b27
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Ongeldig certificaat van de agent op de KUMA-server

Status	ⓘ
Onderdeel	KUMA-integratie
Windows-gebeurtenissen ID	2856

Kaspersky Security Center gebeurtenis ID	00000b28
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

Application crashed during previous session

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	Gedragsdetectie Anti-Cryptor Exploit-preventie Web Threat Protection
Windows-gebeurtenissen ID	`331`
Kaspersky Security Center gebeurtenis ID	`GNRL_EV_OBJECT_BLOCKED`
Gebeurtenisparameters	• `GNRL_EA_PARAM_1` is de hash van het object (SHA256). • `GNRL_EA_PARAM_2` is de naam van het object. Wanneer externe encryptie van gedeelde mappen wordt gedetecteerd, toont het programma het pad naar het doelbestand. • `GNRL_EA_PARAM_5` is de naam van de dreiging in overeenstemming met de Kaspersky-classificatie, bijvoorbeeld `EICAR-Test-File`. • `GNRL_EA_PARAM_7` is de naam van de sessiegebruiker. • `GNRL_EA_PARAM_8` is het type dreiging (`type`). • `GNRL_EA_PARAM_9` is bijkomende informatie over het gedetecteerde object: Programmacomponent (`engine`). Threat detection technology (`method`). Dreiging gedetecteerd door Kaspersky Private Security Network (`blacklist`): `true` of `false`. EDR-versie. Identificatie van dreiging in EDR. MD5 hash van het object.
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

The operating system settings do not allow to control access to Wi-Fi networks

Status	⚠
Onderdeel	Apparaatcontrole
Windows-gebeurtenissen ID	`249`
Kaspersky Security Center gebeurtenis ID	`000000f9`
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Object not restored 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)	✓

Network connection blocked

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 Mail Threat Protection Host Intrusion Prevention AMSI-bescherming Malware-scan
Windows-gebeurtenissen ID	314
Kaspersky Security Center gebeurtenis ID	GNRL_EV_OBJECT_REPORTED
Gebeurtenisparameters	• GNRL_EA_PARAM_1 is de hash van het object (SHA256). • GNRL_EA_PARAM_2 is de naam van het object. • GNRL_EA_PARAM_5 is de naam van de dreiging in overeenstemming met de Kaspersky-classificatie, bijvoorbeeld EICAR-Test-File. • GNRL_EA_PARAM_7 is de naam van de sessiegebruiker. • GNRL_EA_PARAM_8 is het type dreiging (type). • GNRL_EA_PARAM_9 is bijkomende informatie over het gedetecteerde object: Programmacomponent (engine). Threat detection technology (method). Dreiging gedetecteerd door Kaspersky Private Security Network (blacklist): true of false. EDR-versie. Identificatie van dreiging in EDR. MD5 hash van het object.
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Status	⚠
Onderdeel	File Threat Protection Gedragsdetectie Anti-Cryptor Host Intrusion Prevention Malware-scan
Windows-gebeurtenissen ID	310
Kaspersky Security Center gebeurtenis ID	00000136
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 Web Threat Protection Mail Threat Protection AMSI-bescherming Host Intrusion Prevention Malware-scan
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)

Status	⚠
Onderdeel	File Threat Protection Web Threat Protection Mail Threat Protection Host Intrusion Prevention AMSI-bescherming Gedragsdetectie Anti-Cryptor Anti-Cryptor Malware-scan
Windows-gebeurtenissen ID	`303`
Kaspersky Security Center gebeurtenis ID	`GNRL_EV_VIRUS_FOUND`
Gebeurtenisparameters	• `GNRL_EA_PARAM_1` is de hash van het object (SHA256). • `GNRL_EA_PARAM_2` is de naam van het object. • `GNRL_EA_PARAM_5` is de naam van de dreiging in overeenstemming met de Kaspersky-classificatie, bijvoorbeeld `EICAR-Test-File`. • `GNRL_EA_PARAM_7` is de naam van de sessiegebruiker. • `GNRL_EA_PARAM_8` is het type dreiging (`type`).
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)

Status	⚠
Onderdeel	File Threat Protection Web Threat Protection Mail Threat Protection Host Intrusion Prevention AMSI-bescherming Gedragsdetectie Anti-Cryptor Anti-Cryptor Malware-scan
Windows-gebeurtenissen ID	`303`

Kaspersky Security Center gebeurtenis ID	GNRL_EV_VIRUS_FOUND_BY_KSN
Gebeurtenisparameters	• GNRL_EA_PARAM_1 is de hash van het object (SHA256). • GNRL_EA_PARAM_2 is de naam van het object. • GNRL_EA_PARAM_5 is de naam van de dreiging in overeenstemming met de Kaspersky-classificatie, bijvoorbeeld EICAR-Test-File. • GNRL_EA_PARAM_7 is de naam van de sessiegebruiker. • GNRL_EA_PARAM_8 is het type dreiging (type).
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Object deleted

Status	⚠
Onderdeel	File Threat Protection Mail Threat Protection Host Intrusion Prevention Exploit-preventie Gedragsdetectie Anti-Cryptor Malware-scan
Windows-gebeurtenissen ID	307
Kaspersky Security Center gebeurtenis ID	GNRL_EV_OBJECT_DELETED
Gebeurtenisparameters	• GNRL_EA_PARAM_1 is de hash van het object (SHA256). • GNRL_EA_PARAM_2 is de naam van het object. • GNRL_EA_PARAM_5 is de naam van de dreiging in overeenstemming met de Kaspersky-classificatie, bijvoorbeeld EICAR-Test-File. • GNRL_EA_PARAM_7 is de naam van de sessiegebruiker. • GNRL_EA_PARAM_8 is het type dreiging (type). • GNRL_EA_PARAM_9 is bijkomende informatie over het gedetecteerde object: Programmacomponent (engine). Threat detection technology (method). Dreiging gedetecteerd door Kaspersky Private Security Network (blacklist): true of false. EDR-versie. Identificatie van dreiging in EDR. MD5 hash van het object.
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Object disinfected

Status	⚠
Onderdeel	File Threat Protection Mail Threat Protection Host Intrusion Prevention Malware-scan
Windows-gebeurtenissen ID	306

Kaspersky Security Center gebeurtenis ID	`GNRL_EV_OBJECT_CURED`
Gebeurtenisparameters	• `GNRL_EA_PARAM_1` is de hash van het object (SHA256). • `GNRL_EA_PARAM_2` is de naam van het object. • `GNRL_EA_PARAM_5` is de naam van de dreiging in overeenstemming met de Kaspersky-classificatie, bijvoorbeeld `EICAR-Test-File`. • `GNRL_EA_PARAM_7` is de naam van de sessiegebruiker. • `GNRL_EA_PARAM_8` is het type dreiging (`type`). • `GNRL_EA_PARAM_9` is bijkomende informatie over het gedetecteerde object: Programmacomponent (`engine`). Threat detection technology (`method`). Dreiging gedetecteerd door Kaspersky Private Security Network (`blacklist`): `true` of `false`. EDR-versie. Identificatie van dreiging in EDR. MD5 hash van het object.
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Object will be disinfected on restart

Status	⚠
Onderdeel	Host Intrusion Prevention File Threat Protection Malware-scan
Windows-gebeurtenissen ID	324
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Object will be deleted on restart

Status	⚠
Onderdeel	Gedragsdetectie Anti-Cryptor Exploit-preventie Host Intrusion Prevention File Threat Protection Malware-scan
Windows-gebeurtenissen ID	323
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Object deleted according to settings

Status	⚠
Onderdeel	Mail Threat Protection
Windows-gebeurtenissen ID	342
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Rollback completed

Status	⚠
Onderdeel	File Threat Protection Gedragsdetectie Anti-Cryptor Exploit-preventie Malware-scan
Windows-gebeurtenissen ID	455
Kaspersky Security Center gebeurtenis ID	000001c7
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Object download was blocked

Status	⚠
Onderdeel	Web Threat Protection
Windows-gebeurtenissen ID	341
Kaspersky Security Center gebeurtenis ID	GNRL_EV_OBJECT_BLOCKED
Gebeurtenisparameters	• GNRL_EA_PARAM_1 is de hash van het object (SHA256). • GNRL_EA_PARAM_2 is de naam van het object. • GNRL_EA_PARAM_5 is de naam van de dreiging in overeenstemming met de Kaspersky-classificatie, bijvoorbeeld EICAR-Test-File. • GNRL_EA_PARAM_7 is de naam van de sessiegebruiker. • GNRL_EA_PARAM_8 is het type dreiging (type). • GNRL_EA_PARAM_9 is bijkomende informatie over het gedetecteerde object: Programmacomponent (engine). Threat detection technology (method). Dreiging gedetecteerd door Kaspersky Private Security Network (blacklist): true of false. EDR-versie. Identificatie van dreiging in EDR. MD5 hash van het object.
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	• GNRL_EA_PARAM_1 is de hash van het object (SHA256). • GNRL_EA_PARAM_2 is de naam van het object. • GNRL_EA_PARAM_5 is de naam van de dreiging in overeenstemming met de Kaspersky-classificatie, bijvoorbeeld EICAR-Test-File. • GNRL_EA_PARAM_7 is de naam van de sessiegebruiker. • GNRL_EA_PARAM_8 is het type dreiging (type). • GNRL_EA_PARAM_9 is bijkomende informatie over het gedetecteerde object: Programmacomponent (engine). Threat detection technology (method). Dreiging gedetecteerd door Kaspersky Private Security Network (blacklist): true of false. EDR-versie. Identificatie van dreiging in EDR. MD5 hash van het object.
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	• GNRL_EA_PARAM_1 is de URL. • GNRL_EA_PARAM_2 is de naam van de sessiegebruiker. • GNRL_EA_PARAM_3 is de naam van de Webcontrole-regel.
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	• GNRL_EA_PARAM_1 is de URL. • GNRL_EA_PARAM_2 is de naam van de sessiegebruiker. • GNRL_EA_PARAM_3 is de naam van de Webcontrole-regel.
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 canceled by the user

Status	⚠
Onderdeel	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)	✓

Interrupted applying file encryption / decryption rules

Status	⚠
Onderdeel	Gegevensencryptie
Windows-gebeurtenissen ID	903
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

File encryption / decryption interrupted

Status	⚠
Onderdeel	Gegevensencryptie
Windows-gebeurtenissen ID	914
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Device encryption / decryption interrupted

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	Systeemintegriteitscheck
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)	✓

Process was terminated by the Kaspersky Anti Targeted Attack Platform server administrator

Status	⚠
Onderdeel	Endpoint Sensor
Windows-gebeurtenissen ID	2112
Kaspersky Security Center gebeurtenis ID	00000840
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

The application was terminated by the Kaspersky Anti Targeted Attack Platform server administrator

Status	⚠
Onderdeel	Endpoint Sensor
Windows-gebeurtenissen ID	2113
Kaspersky Security Center gebeurtenis ID	00000841
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

File or stream was deleted by the Kaspersky Anti Targeted Attack Platform server administrator

Status	⚠
Onderdeel	Endpoint Sensor
Windows-gebeurtenissen ID	2111
Kaspersky Security Center gebeurtenis ID	0000083f
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

File was restored from quarantine on the Kaspersky Anti Targeted Attack Platform server by the administrator

Status	⚠
Onderdeel	Endpoint Sensor
Windows-gebeurtenissen ID	2110
Kaspersky Security Center gebeurtenis ID	0000083e
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

File was quarantined on the Kaspersky Anti Targeted Attack Platform server by the administrator

Status	⚠
Onderdeel	Endpoint Sensor
Windows-gebeurtenissen ID	2109
Kaspersky Security Center gebeurtenis ID	0000083d
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Network activity of all third-party applications is blocked

Status	⚠
Onderdeel	Endpoint Sensor
Windows-gebeurtenissen ID	2107
Kaspersky Security Center gebeurtenis ID	0000083b
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Network activity of all third-party applications is unblocked

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 (Sandbox)

Status	⚠
Onderdeel	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	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	• GNRL_EA_DESCRIPTION is het bericht aan de gebruiker. • GNRL_EA_PARAM_2 is de naam van de sessiegebruiker. • GNRL_EA_PARAM_6 is de naam van het uitvoerbare bestand van het programma (bijvoorbeeld chrome.exe). • GNRL_EA_PARAM_7 is het pad naar het uitvoerbare bestand. • GNRL_EA_PARAM_8 is de hash van het object (SHA256). • GNRL_EA_PARAM_9 is de versie van het programma die de gebruiker probeert uit te voeren.
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	• c_er_descr is het bericht aan de gebruiker. • GNRL_EA_PARAM_1 is de Hardware-ID (HWID). • GNRL_EA_PARAM_2 is de naam van de sessiegebruiker.
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	• GNRL_EA_DESCRIPTION is het bericht aan de gebruiker. • GNRL_EA_PARAM_1 is de URL. • GNRL_EA_PARAM_2 is de naam van de sessiegebruiker.
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	• `GNRL_EA_PARAM_1` is de Hardware-ID (HWID). • `GNRL_EA_PARAM_2` is de naam van de sessiegebruiker.
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Application activity blockage message to administrator

Status	⚠
Onderdeel	Bestandsintegriteitsmonitor
Windows-gebeurtenissen ID	`2901`
Kaspersky Security Center gebeurtenis ID	`00000b55`
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Status	⚠
Onderdeel	Bestandsintegriteitsmonitor
Windows-gebeurtenissen ID	`2900`
Kaspersky Security Center gebeurtenis ID	`00000b54`
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Status	⚠
Onderdeel	Adaptieve controle op afwijkingen
Windows-gebeurtenissen ID	`503`
Kaspersky Security Center gebeurtenis ID	`GNRL_EV_ADSEC_USER_REQUEST`
Gebeurtenisparameters	• `GNRL_EA_DESCRIPTION` is het bericht aan de gebruiker. • `GNRL_EA_PARAM_1` is de naam van de regel voor Adaptieve controle op afwijkingen. • `GNRL_EA_PARAM_2` is de ID van de heuristische regel. • `GNRL_EA_PARAM_3` is de naam van de sessiegebruiker. • `GNRL_EA_PARAM_4` is het bronproces. • `GNRL_EA_PARAM_5` is het bronobject. • `GNRL_EA_PARAM_6` is het doelproces. • `GNRL_EA_PARAM_7` is het doelobject. • `GNRL_EA_PARAM_8` is bijkomende informatie over het gedetecteerde object: Hashes van bronproces / object en doelproces / object. Proces geblokkeerd (`verdict_type`): `true` of `false`. User security ID (SID).
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Starting the cloud service client application is blocked

Status	⚠
Onderdeel	Cloud Discovery
Windows-gebeurtenissen ID	2212
Kaspersky Security Center gebeurtenis ID	000008a4
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Access to the cloud service is blocked

Status	⚠
Onderdeel	Cloud Discovery
Windows-gebeurtenissen ID	2213
Kaspersky Security Center gebeurtenis ID	000008a5
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

File or folder change was detected

Status	ⓘ / ⚠ / ⓘ
Onderdeel	Systeemintegriteitscontrole
Windows-gebeurtenissen ID	2950
Kaspersky Security Center gebeurtenis ID	00000b86
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Om de bewaarperiode voor deze gebeurtenis te configureren, ga naar de **Event configuration** van het beleid en stel de bewaarperiode in voor de algemene gebeurtenis Systeemintegriteitscontrole: *File or folder change was detected*.

Object changes too often. Event aggregation started

Status	ⓘ / ⚠ / ⓘ
Onderdeel	Systeemintegriteitscontrole
Windows-gebeurtenissen ID	2955
Kaspersky Security Center gebeurtenis ID	00000b8b
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Report on object modification for the aggregation period

Status	ⓘ / ⚠ / ⓘ
Onderdeel	Systeemintegriteitscontrole
Windows-gebeurtenissen ID	2956
Kaspersky Security Center gebeurtenis ID	00000b8c
Windows gebeurtenislogboek - EventLogItem.	–

Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Om de bewaarperiode voor deze gebeurtenis te configureren, ga naar de **Event configuration** van het beleid en stel de bewaarperiode in voor de algemene gebeurtenis Systeemintegriteitscontrole: *File or folder change was detected*.

Registry change was detected

Status	ⓘ / ⚠ / !
Onderdeel	Systeemintegriteitscontrole
Windows-gebeurtenissen ID	2951
Kaspersky Security Center gebeurtenis ID	00000b87
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Om de bewaarperiode voor deze gebeurtenis te configureren, ga naar de **Event configuration** van het beleid en stel de bewaarperiode in voor de algemene gebeurtenis Systeemintegriteitscontrole: *File or folder change was detected*.

Device connection / disconnection is detected

Status	ⓘ / ⚠ / !
Onderdeel	Systeemintegriteitscontrole
Windows-gebeurtenissen ID	2952
Kaspersky Security Center gebeurtenis ID	00000b88
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Om de bewaarperiode voor deze gebeurtenis te configureren, ga naar de **Event configuration** van het beleid en stel de bewaarperiode in voor de algemene gebeurtenis Systeemintegriteitscontrole: *File or folder change was detected*.

Bereik van bewaking bevat onjuiste objecten

Status	ⓘ / ⚠ / !
Onderdeel	Systeemintegriteitscontrole
Windows-gebeurtenissen ID	2903
Kaspersky Security Center gebeurtenis ID	00000b89
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Om de bewaarperiode voor deze gebeurtenis te configureren, ga naar de **Event configuration** van het beleid en stel de bewaarperiode in voor de algemene gebeurtenis Systeemintegriteitscontrole: *File or folder change was detected*.

The prohibited operation was allowed in test mode

Status	⚠
Onderdeel	Systeemintegriteitscontrole
Windows-gebeurtenissen ID	2961
Kaspersky Security Center gebeurtenis ID	00000b91
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Kan al meer dan 30 minuten geen verbinding maken met de Integratieserver. Controleer de status en netwerkinstellingen van de Integratieserver

Status	⚠
Onderdeel	Light Agent
Windows-gebeurtenissen ID	3102
Kaspersky Security Center gebeurtenis ID	00000c1e
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Kan geen verbinding maken met de Integratieserver. Controleer de status van de Integratieserver en de netwerkinstellingen

Status	⚠
Onderdeel	Light Agent
Windows-gebeurtenissen ID	3101
Kaspersky Security Center gebeurtenis ID	00000c1d
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Virtuele machine-sjabloon moet worden bijgewerkt

Status	⚠
Onderdeel	Light Agent
Windows-gebeurtenissen ID	3181
Kaspersky Security Center gebeurtenis ID	00000c6d
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

The Standard license is terminated. The application is running under the Enterprise license

Status	⚠
Onderdeel	Light Agent
Windows-gebeurtenissen ID	3171
Kaspersky Security Center gebeurtenis ID	00000c64
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)	–

Self-Defense restricted access to the protected resource

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 Mail Threat Protection Gedragsdetectie Anti-Cryptor Host Intrusion Prevention Sandbox Malware-scan
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 Host Intrusion Prevention Malware-scan
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 Web Threat Protection Mail Threat Protection AMSI-bescherming Host Intrusion Prevention Malware-scan
Windows-gebeurtenissen ID	322
Kaspersky Security Center gebeurtenis ID	GNRL_EV_PASSWD_ARCHIVE_FOUND
Gebeurtenisparameters	• GNRL_EA_PARAM_2 is de naam van het object. • GNRL_EA_PARAM_3 is de datum van aanmaak van het object (optioneel). • GNRL_EA_PARAM_7 is de naam van de sessiegebruiker. • GNRL_EA_PARAM_9 is bijkomende informatie over het gedetecteerde object: Programmacomponent (engine). Threat detection technology (method). Dreiging gedetecteerd door Privaat KSN (denylist): true of false.
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Information about detected object

Status	ⓘ
Onderdeel	File Threat Protection Web Threat Protection Mail Threat Protection AMSI-bescherming Host Intrusion Prevention Malware-scan
Windows-gebeurtenissen ID	332
Kaspersky Security Center gebeurtenis ID	0000014c
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

The object is in the Kaspersky Private Security Network allowlist

Status	ⓘ
Onderdeel	File Threat Protection Web Threat Protection Mail Threat Protection AMSI-bescherming Host Intrusion Prevention Malware-scan
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 Exploit-preventie Gedragsdetectie Anti-Cryptor Malware-scan
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 File Threat Protection Web Threat Protection Mail Threat Protection Malware-scan
Windows-gebeurtenissen ID	301
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Object skipped

Status	ⓘ
Onderdeel	Host Intrusion Prevention File Threat Protection AMSI-bescherming Malware-scan
Windows-gebeurtenissen ID	315
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Archive detected

Status	ⓘ
Onderdeel	Host Intrusion Prevention File Threat Protection Web Threat Protection Mail Threat Protection AMSI-bescherming Malware-scan
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 File Threat Protection Web Threat Protection Mail Threat Protection AMSI-bescherming Malware-scan
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	Update
Windows-gebeurtenissen ID	1001
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Proxyserver is geselecteerd

Status	ⓘ
Onderdeel	Update
Windows-gebeurtenissen ID	1002
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

The link is in the Kaspersky Private Security Network 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 Anti-Cryptor Exploit-preventie 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 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 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	• `GNRL_EA_PARAM_1` is de naam van de regel voor Adaptieve controle op afwijkingen. • `GNRL_EA_PARAM_2` is de ID van de heuristische regel. • `GNRL_EA_PARAM_3` is de naam van de sessiegebruiker. • `GNRL_EA_PARAM_4` is het bronproces. • `GNRL_EA_PARAM_5` is het bronobject. • `GNRL_EA_PARAM_6` is het doelproces. • `GNRL_EA_PARAM_7` is het doelobject. • `GNRL_EA_PARAM_8` is bijkomende informatie over het gedetecteerde object: Hashes van bronproces / object en doelproces / object. Proces geblokkeerd (`verdict_type`): `true` of `false`. User security ID (SID).
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	• GNRL_EA_PARAM_2 is de naam van de sessiegebruiker. • GNRL_EA_PARAM_3 is de handmatig aangemaakte categorie-ID. • GNRL_EA_PARAM_4 is de veiligheidsidentificatie van de account (SID). • GNRL_EA_PARAM_5 is informatie over de digitale handtekening van het programma. • GNRL_EA_PARAM_6 is de naam van het uitvoerbare bestand van het programma (bijvoorbeeld chrome.exe). • GNRL_EA_PARAM_7 is het pad naar het uitvoerbare bestand. • GNRL_EA_PARAM_8 is de hash van het object (SHA256). • GNRL_EA_PARAM_9 is de versie van het programma die de gebruiker probeert uit te voeren.
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	• GNRL_EA_PARAM_2 is de naam van de sessiegebruiker. • GNRL_EA_PARAM_3 is de handmatig aangemaakte categorie-ID. • GNRL_EA_PARAM_4 is de veiligheidsidentificatie van de account (SID). • GNRL_EA_PARAM_5 is informatie over de digitale handtekening van het programma.

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	• `GNRL_EA_PARAM_1` is de bestandsbewerking (schrijven of wissen). • `GNRL_EA_PARAM_2` is het pad naar het bestand. • `GNRL_EA_PARAM_3` is de naam van het apparaat. • `GNRL_EA_PARAM_4` is de naam van de sessiegebruiker. • `GNRL_EA_PARAM_5` is de Hardware-ID (HWID).
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

No available updates

Status	
Onderdeel	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	Update
Windows-gebeurtenissen ID	1022
Kaspersky Security Center gebeurtenis ID	000003fe
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Downloading files

Status	ⓘ
Onderdeel	Update
Windows-gebeurtenissen ID	1003
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

File downloaded

Status	ⓘ
Onderdeel	Update
Windows-gebeurtenissen ID	1004
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

File installed

Status	ⓘ
Onderdeel	Update
Windows-gebeurtenissen ID	1005
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

File updated

Status	ⓘ
Onderdeel	Update
Windows-gebeurtenissen ID	1006
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

File rolled back due to update error

Status	ⓘ
Onderdeel	Update
Windows-gebeurtenissen ID	1007
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Updating files

Status	ⓘ
Onderdeel	Update
Windows-gebeurtenissen ID	1008
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Distributing updates

Status	ⓘ
Onderdeel	Update
Windows-gebeurtenissen ID	1009
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Rolling back files

Status	ⓘ
Onderdeel	Update
Windows-gebeurtenissen ID	1010
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Creating the list of files to download

Status	ⓘ
Onderdeel	Update
Windows-gebeurtenissen ID	1013
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Downloading patches

Status	ⓘ
Onderdeel	Update
Windows-gebeurtenissen ID	2150
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Installing patch

Status	ⓘ
Onderdeel	Update
Windows-gebeurtenissen ID	2151
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Patch installed

Status	ⓘ
Onderdeel	Update
Windows-gebeurtenissen ID	2152
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Rolling back patch

Status	ⓘ
Onderdeel	Update
Windows-gebeurtenissen ID	2154
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Patch rolled back

Status	ⓘ
Onderdeel	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)	✓

Resumed applying file encryption / decryption rules

Status	ⓘ
Onderdeel	Gegevensencryptie
Windows-gebeurtenissen ID	905
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

File encryption / decryption started

Status	ⓘ
Onderdeel	Gegevensencryptie
Windows-gebeurtenissen ID	910
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

File encryption / decryption completed

Status	ⓘ
Onderdeel	Gegevensencryptie
Windows-gebeurtenissen ID	911
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

File has not been encrypted because it is an exclusion

Status	ⓘ
Onderdeel	Gegevensencryptie
Windows-gebeurtenissen ID	913
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Portable mode enabled

Status	ⓘ
Onderdeel	Gegevensencryptie
Windows-gebeurtenissen ID	950
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Portable mode disabled

Status	ⓘ
Onderdeel	Gegevensencryptie
Windows-gebeurtenissen ID	952
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Device encryption / decryption started

Status	ⓘ
Onderdeel	Gegevensencryptie
Windows-gebeurtenissen ID	1301
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Device encryption / decryption completed

Status	ⓘ
Onderdeel	Gegevensencryptie
Windows-gebeurtenissen ID	1302
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Device encryption / decryption resumed

Status	ⓘ
Onderdeel	Gegevensencryptie
Windows-gebeurtenissen ID	1304
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Device is not encrypted

Status	ⓘ
Onderdeel	Gegevensencryptie
Windows-gebeurtenissen ID	1307
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Device encryption / decryption process has been switched to active mode

Status	ⓘ
Onderdeel	Gegevensencryptie
Windows-gebeurtenissen ID	1308
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Device encryption / decryption process has been switched to passive mode

Status	ⓘ
Onderdeel	Gegevensencryptie
Windows-gebeurtenissen ID	1309
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Encryption module loaded

Status	ⓘ
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

Status	
Onderdeel	Gegevensencryptie
Windows-gebeurtenissen ID	1330
Kaspersky Security Center gebeurtenis ID	00000532
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Authentication Agent account deleted

Status	
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

Status	
Onderdeel	Gegevensencryptie
Windows-gebeurtenissen ID	1332
Kaspersky Security Center gebeurtenis ID	00000534
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Successful Authentication Agent login

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 recovery key was saved to a removable drive

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	Endpoint Detection and Response Expert (on-premises)
Windows-gebeurtenissen ID	2853
Kaspersky Security Center gebeurtenis ID	00000b25
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Status	ⓘ
Onderdeel	Gegevens wissen
Windows-gebeurtenissen ID	2253
Kaspersky Security Center gebeurtenis ID	000008cd
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Object quarantined (Sandbox)

Status	ⓘ
Onderdeel	Sandbox
Windows-gebeurtenissen ID	2602
Kaspersky Security Center gebeurtenis ID	00000a2a
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Object deleted (Sandbox)

Status	ⓘ
Onderdeel	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	Sandbox
Windows-gebeurtenissen ID	2606
Kaspersky Security Center gebeurtenis ID	–

Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Status	ⓘ
Onderdeel	Sandbox
Windows-gebeurtenissen ID	2609
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Status	ⓘ
Onderdeel	Sandbox
Windows-gebeurtenissen ID	2610
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

Status	ⓘ
Onderdeel	Sandbox
Windows-gebeurtenissen ID	2616
Kaspersky Security Center gebeurtenis ID	–
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	–

De Administration Server waarmee uw apparaat is verbonden, is ingesteld als vertrouwd

Status	ⓘ
Onderdeel	Administration Server verbindingsbescherming
Windows-gebeurtenissen ID	3300
Kaspersky Security Center gebeurtenis ID	00000ce4
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Uw apparaat is verbonden met de nieuwe vertrouwde Administration Server

Status	ⓘ
Onderdeel	Administration Server verbindingsbescherming
Windows-gebeurtenissen ID	3302
Kaspersky Security Center gebeurtenis ID	00000ce6
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

De Administration Server waarmee uw apparaat is verbonden, is niet langer ingesteld als vertrouwd

Status	ⓘ
Onderdeel	Administration Server verbindingsbescherming
Windows-gebeurtenissen ID	3303
Kaspersky Security Center gebeurtenis ID	00000ce7
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Asynchronous Sandbox detection

Status	ⓘ
Onderdeel	Sandbox
Windows-gebeurtenissen ID	2619
Kaspersky Security Center gebeurtenis ID	GNRL_EV_APP_INCIDENT_OCCURED
Gebeurtenisparameters	• GNRL_EA_PARAM_1 zijn de parameters van de Sandbox-onderdelen. • GNRL_EA_PARAM_2 is het pad naar het object. • GNRL_EA_PARAM_3 is de incident-ID. • GNRL_EA_PARAM_4 is de hash van het object (SHA256).
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

The scan task has been successfully sent to Sandbox by a user

Status	ⓘ
Onderdeel	Sandbox
Windows-gebeurtenissen ID	2622
Kaspersky Security Center gebeurtenis ID	00000a3e
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	• GNRL_EA_PARAM_1 is de Hardware-ID (HWID). • GNRL_EA_PARAM_2 is de naam van de sessiegebruiker.
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	• GNRL_EA_PARAM_1 is de Hardware-ID (HWID). • GNRL_EA_PARAM_2 is de naam van de sessiegebruiker.
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Error removing the previous version of the application

Status	ⓘ
Onderdeel	Systeemaudit
Windows-gebeurtenissen ID	246
Kaspersky Security Center gebeurtenis ID	000000f6
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Successful connection to the EDR Expert server

Status	ⓘ
Onderdeel	Endpoint Detection and Response Expert (on-premises)
Windows-gebeurtenissen ID	2853
Kaspersky Security Center gebeurtenis ID	00000b25
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Succesvolle verbinding met de EDR Expert reactieserver

Status	ⓘ
Onderdeel	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows-gebeurtenissen ID	2853
Kaspersky Security Center gebeurtenis ID	00000b25
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Succesvolle verbinding met de EDR Expert telemetrieverzamelingsserver

Status	ⓘ
Onderdeel	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows-gebeurtenissen ID	2857
Kaspersky Security Center gebeurtenis ID	00000b26
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Succesvolle verbinding met de NDR-server

Status	ⓘ
Onderdeel	Network Detection and Response (KATA)
Windows-gebeurtenissen ID	3083
Kaspersky Security Center gebeurtenis ID	00000c0b
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Starting the cloud service client application is allowed

Status	ⓘ
Onderdeel	Cloud Discovery
Windows-gebeurtenissen ID	2210
Kaspersky Security Center gebeurtenis ID	000008a2
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Access to the cloud service is allowed

Status	ⓘ
Onderdeel	Cloud Discovery
Windows-gebeurtenissen ID	2211
Kaspersky Security Center gebeurtenis ID	000008a3
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Toegang tot het beschermde gebied

Status	ⓘ
Onderdeel	Systeemaudit
Windows-gebeurtenissen ID	2004
Kaspersky Security Center gebeurtenis ID	000007d4
Windows gebeurtenislogboek - EventLogItem.	✓
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

File or folder change was detected

Status	ⓘ / ⚠ / ⓘ
Onderdeel	Systeemintegriteitscontrole
Windows-gebeurtenissen ID	2950
Kaspersky Security Center gebeurtenis ID	00000b86
Windows gebeurtenislogboek - EventLogItem.	–

Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Om de bewaarperiode voor deze gebeurtenis te configureren, ga naar de **Event configuration** van het beleid en stel de bewaarperiode in voor de algemene gebeurtenis Systeemintegriteitscontrole: *File or folder change was detected*.

Object changes too often. Event aggregation started

Status	ⓘ / ⚠ / ⓘ
Onderdeel	Systeemintegriteitscontrole
Windows-gebeurtenissen ID	2955
Kaspersky Security Center gebeurtenis ID	00000b8b
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Report on object modification for the aggregation period

Status	ⓘ / ⚠ / ⓘ
Onderdeel	Systeemintegriteitscontrole
Windows-gebeurtenissen ID	2956
Kaspersky Security Center gebeurtenis ID	00000b8c
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Om de bewaarperiode voor deze gebeurtenis te configureren, ga naar de **Event configuration** van het beleid en stel de bewaarperiode in voor de algemene gebeurtenis Systeemintegriteitscontrole: *File or folder change was detected*.

Registry change was detected

Status	ⓘ / ⚠ / ⓘ
Onderdeel	Systeemintegriteitscontrole
Windows-gebeurtenissen ID	2951
Kaspersky Security Center gebeurtenis ID	00000b87
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Om de bewaarperiode voor deze gebeurtenis te configureren, ga naar de **Event configuration** van het beleid en stel de bewaarperiode in voor de algemene gebeurtenis Systeemintegriteitscontrole: *File or folder change was detected*.

Device connection / disconnection is detected

Status	ⓘ / ⚠ / ⓘ
Onderdeel	Systeemintegriteitscontrole
Windows-gebeurtenissen ID	2952
Kaspersky Security Center gebeurtenis ID	00000b88

Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Om de bewaarperiode voor deze gebeurtenis te configureren, ga naar de **Event configuration** van het beleid en stel de bewaarperiode in voor de algemene gebeurtenis Systeemintegriteitscontrole: *File or folder change was detected*.

Bereik van bewaking bevat onjuiste objecten

Status	ⓘ / ⚠ / ⓘ
Onderdeel	Systeemintegriteitscontrole
Windows-gebeurtenissen ID	2903
Kaspersky Security Center gebeurtenis ID	00000b89
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Om de bewaarperiode voor deze gebeurtenis te configureren, ga naar de **Event configuration** van het beleid en stel de bewaarperiode in voor de algemene gebeurtenis Systeemintegriteitscontrole: *File or folder change was detected*.

Baseline created

Status	ⓘ
Onderdeel	Systeemintegriteitscontrole
Windows-gebeurtenissen ID	2957
Kaspersky Security Center gebeurtenis ID	00000b8d
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Baseline updated

Status	ⓘ
Onderdeel	Systeemintegriteitscontrole
Windows-gebeurtenissen ID	2958
Kaspersky Security Center gebeurtenis ID	00000b8e
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

An operation is performed by the trusted user

Status	ⓘ
Onderdeel	Systeemintegriteitscontrole
Windows-gebeurtenissen ID	2962
Kaspersky Security Center gebeurtenis ID	00000b92
Windows gebeurtenislogboek - EventLogItem.	–

Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Om de bewaarperiode voor deze gebeurtenis te configureren, ga naar de **Event configuration** van het beleid en stel de bewaarperiode in voor de algemene gebeurtenis Systeemintegriteitscontrole: *File or folder change was detected*.

Connected to SVM

Status	ⓘ
Onderdeel	Light Agent
Windows-gebeurtenissen ID	3152
Kaspersky Security Center gebeurtenis ID	00000c50
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

A new temporary password was created

Status	ⓘ
Onderdeel	Systeemaudit
Windows-gebeurtenissen ID	265
Kaspersky Security Center gebeurtenis ID	00000109
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Connected to the Integration Server

Status	ⓘ
Onderdeel	Light Agent
Windows-gebeurtenissen ID	3105
Kaspersky Security Center gebeurtenis ID	00000c21
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Restoring connection to the Integration Server

Status	ⓘ
Onderdeel	Light Agent
Windows-gebeurtenissen ID	3104
Kaspersky Security Center gebeurtenis ID	00000c20
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Succesvolle verbinding met de KUMA-server

Status	ⓘ
Onderdeel	KUMA-integratie

Windows-gebeurtenissen ID	2857
Kaspersky Security Center gebeurtenis ID	00000b29
Windows gebeurtenislogboek - EventLogItem.	–
Kaspersky Security Center-gebeurtenislogboek (standaard)	✓

Appendix 7. 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 doc dot docm docx dotx dotm docb
WordPad	wordpad.exe	docx rtf
Microsoft Excel	excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw
Microsoft PowerPoint	powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm

Programmanaam	Uitvoerbaar bestand	Bestandsextensie
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 8. Ondersteunde scriptinterprekers voor Preventie van uitvoering

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
- msiexec.exe
- perl.exe

- powershell.exe
- python.exe
- reg.exe
- regedit.exe
- regedt32.exe
- regsvr32.exe
- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacycplelevated.exe
- wscript.exe
- wwahost.exe

Preventie van uitvoering ondersteunt het werken met Java-applicaties in de Java Runtime-omgeving (java.exe- en javaw.exe-processen).

Appendix 9. IOC-scanbereik in het register (RegistryItem)

Wanneer u het gegevenstype **Windows registry - 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\Aedebug

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
```

Appendix 10. 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.
- Na het uploaden van IOC-bestanden kunt u de bestanden handmatig bewerken in de ingebouwde editor, rechtstreeks in de taakeigenschappen. Kaspersky Endpoint Security ondersteunt de bewerking van IOC-bestanden die voldoen aan de OpenIOC 1.1-standaard. Het is niet mogelijk om de inhoud van IOC-bestanden die compatibel zijn met OpenIOC versie 1.0 te wijzigen.
- 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 Scan* 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-scantaak 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.

DOWNLOAD HET BESTAND IOC_TERMS.XLSX

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	OpenIOC 1.0:
	
	`is`
	`isnot` (als uitzondering van de set)
	`contains`
	`containsnot` (als uitzondering van de set)
	OpenIOC 1.1:
	
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`
	
	Voor de termen E-mail/* worden alleen de `contains` en `is` voorwaarden ondersteund. Voor een correcte werking van Retrospective IOC Scan bij gebruik van de `is` voorwaarde, moeten e-mailadressen in IOC-bestanden worden opgegeven in de volgende indeling: `"name@example.org" <SMTP:name@example.org>` . Tijdens het normaal uitvoeren van de *IOC-scan*-taak is het voldoende om het e-mailadres in de volgende indeling op te geven: `name@example.org`.

Ondersteunde conditie-attributen	OpenIOC 1.1:
	
	`preserve-case`
	`negate`

Ondersteunde operators	`AND` `OR`
Ondersteunde gegevenstypes	`"date"`: datum (toepasselijke condities: `is`, `greater-than`, `less-than`) `"int"`: integer (toepasselijke condities: `is`, `greater-than`, `less-than`) `"string"`: string (toepasselijke condities: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"`: duur in seconden (toepasselijke condities: `is`, `greater-than`, `less-than`)

Kenmerken van interpretatie van gegevenstype	De gegevenstypes `"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"` en `"base64Binary"` worden geïnterpreteerd als string.
	
	Het programma ondersteunt de interpretatie van de instelling `Content` voor de gegevenstypes `int` en `date` wanneer het is ingesteld in de vorm van intervallen:
	
	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`.

Appendix 11. API voor EDR Threat Response

Kaspersky Endpoint Security 12.9 voor Windows introduceert ondersteuning voor EDR-acties voor Threat Response (EDR responses) met behulp van Kaspersky Security Center OpenAPI. Dat wil zeggen dat u OpenAPI-methoden kunt oproepen om de reactie op EDR-bedreigingen te automatiseren met behulp van Python. U kunt deze methoden oproepen wanneer ze zijn geïntegreerd met SIEM oplossingen. *Kaspersky Unified Monitoring and Analysis Platform*, de SIEM oplossing van Kaspersky ondersteunt de EDR Threat Response OpenAPI vanaf versie 3.4.1. Raadpleeg de KUMA-documentatie voor voorbeeldscripts.

Als u acties voor EDR Treat Response wilt uitvoeren, moet u een verzoek aanmaken en versturen met KSC Open API (`AddIncident`). Nadat het verzoek is verwerkt, wordt een speciale taak aangemaakt in de Kaspersky Security Center-console.

Als u taken wilt aanmaken voor het reageren op EDR-dreigingen, moet u een verbinding op de achtergrond tot stand brengen tussen de Administration Server en de Kaspersky Security Center Web Console. De verbindingsservice op de achtergrond is beschikbaar in Kaspersky Security Center Windows 14.2 of hoger en in Kaspersky Security Center Linux 15.2 of hoger. Andere consoles, waaronder consoles van Kaspersky Detection and Response-oplossingen, worden niet ondersteund.

Voor EDR Threat Response moet u basisverzoekparameters opgeven, bijvoorbeeld in JSON-indeling:

- `task` is het type taak (zie hieronder).
- `targetHost` is de ID van de computer waarop het script moet worden uitgevoerd. Vereist argument. Het script haalt dit argument uit de gebeurtenis.
- `responseEventIncidentArea` is de naam van het programma dat het script heeft uitgevoerd (bijvoorbeeld `KUMA`). Deze parameter wordt toegevoegd aan de naam van de gemaakte taak.

Als u EDR Threat Response wilt configureren, moet u de taakinstellingen in JSON-indeling opgeven in de parameter `"KLINCDT_BODY": json.dumps(data)`. Als gevolg hiervan maakt het programma de `[Response][KUMA] <task type> - <Date> <Time> - <ID>` aan in de Kaspersky Security Center-console.

Verbinding maken met Kaspersky Security Center OpenAPI

Als onderdeel van EDR Threat Response maakt het programma speciale taken aan in de console van Kaspersky Security Center . Voor het maken van deze taken moet u een verbinding tot stand brengen tussen de computer en Kaspersky Security Center. Hiervoor moeten de verbindingsparameters van Kaspersky Security Center in het verzoek worden opgegeven.

In Kaspersky XDR versie 2.1 is de methode voor het autoriseren van verzoeken gewijzigd. Kaspersky XDR gebruikt PAT-tokens in plaats van gebruikersnaam- en wachtwoordverificatie. Daarom is het niet mogelijk om scripts uit te voeren in Kaspersky XDR. Voor meer informatie over het aanvragen van autorisatie raadpleeg de: Help van Kaspersky XDR.

Verbindingsparameters van Kaspersky Security Center

Parameter	Type	Beschrijving
`kscHost`	`string`	Adres Administration Server van het Kaspersky Security Center. Vereiste parameter.
`kscPort`	`int`	Verbindingspoort Administration Server. Vereiste parameter.
`kscCert`	`string`	Pad naar een certificaatbestand voor de verbinding met de Administration Server van Kaspersky Security Center. Standaard is de parameter ingesteld op `False`.
`kscUser`	`string`	Naam van gebruikersaccount. Vereiste parameter.
`kscPassword`	`string`	Wachtwoord van gebruikersaccount. Vereiste parameter.

Voorbeeld

```
# KSC connection info
# reads Environment variables by default, change with corresponding values
# KSC host, string, required
kscHost = "kscHost"
# KSC port, required, default is "13299"
kscPort = "13299"
# KSC certificate file path, default is False
kscCert = False
# KSC user, string, required
kscUser = "kscUser"
# KSC password, string, required
kscPassword = "kscPassword"

server_url = 'https://' + kscHost + ':' + str(kscPort)
    server = KlAkAdmServer.Create(
        server_url, kscUser, kscPassword, verify=kscCert)

    params = validate(args)

    data = {"targetHost": <MyHost>,
            "task": task,
            "params": params,
            "responseEventIncident": True,
            "responseEventIncidentArea":"Kuma"}

    oHostGroup = KlAkHostGroup(server)

    incdnt = oHostGroup.AddIncident({"KLINCDT_SEVERITY": 2,
                                     "KLINCDT_ADDED": paramDateTime(datetime.datetime.now()),
                                     "KLINCDT_BODY": json.dumps(data),
                                     "KLHST_WKS_HOSTNAME":  args.targetHost}).RetVal()

    oHostGroup.UpdateIncident(incdnt, {"KLINCDT_IS_HANDLED": False,
                                       "KLHST_WKS_HOSTNAME":  args.targetHost})
```

De gegevens van het gebruikersaccount zijn niet beschermd. Daarom moet u een aparte gebruiker aanwijzen die alleen deze acties mag uitvoeren.

Bestand ophalen – getFile

Instellingen van Bestand ophalen-taak

Parameter	Type	Beschrijving
`md5hash`	`string`	MD5-hash van het bestand dat u wilt ophalen.
`sha256hash`	`string`	SHA256-hash van het bestand dat u wilt ophalen.
`path`	`string`	Pad naar het bestand dat u wilt ophalen.

Voorbeeld

```
type getFile = {
  task: 'getFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

Bestand verwijderen – deleteFile

Instellingen van Bestand verwijderen-taak

Parameter	Type	Beschrijving
`md5hash`	`string`	MD5-hash van het bestand dat u wilt verwijderen.
`sha256hash`	`string`	SHA256-hash van het bestand dat u wilt verwijderen.
`path`	`string`	Pad naar het bestand dat u wilt verwijderen.
`searchInSubfolders?`	`boolean`	Zoek het bestand dat u wilt verwijderen in submappen.

Voorbeeld

```
type deleteFile = {
  task: 'deleteFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
    // recursive search for a file (subfolder), optional
    searchInSubfolders?: boolean;
  };
  responseEventIncidentArea: string;
};
```

Bestand in Quarantaine plaatsen – quarantineFile

Instellingen van Bestand in Quarantaine plaatsen-taak

Parameter	Type	Beschrijving
`md5hash`	`string`	MD5-hash van het bestand dat u in quarantaine wilt plaatsen.
`sha256hash`	`string`	SHA256-hash van het bestand dat u in quarantaine wilt plaatsen.
`path`	`string`	Pad naar het bestand dat u in quarantaine wilt plaatsen.

Voorbeeld

```
type quarantineFile = {
  task: 'quarantineFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

IOC-scan – iocScan

Instellingen van IOC-scan-taak

Parameter	Type	Beschrijving
`ioc`	`string`	Pad naar het ZIP-archief met IOC-bestand die u wilt gebruiken voor het scannen.
`isolateHost`	`boolean`	Isoleer de computer van het netwerk wanneer een indicator of compromise wordt gedetecteerd om te voorkomen dat de dreiging zich verspreidt.
`scanCriticalAreas`	`boolean`	Start de taak *Kritieke Gebiedenscan* wanneer een indicator of compromise wordt gedetecteerd.
`quarantineObject`	`boolean`	Verwijder het kwaadaardige object wanneer een indicator of compromise wordt gedetecteerd. 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.

Voorbeeld

```
type iocScan = {
  task: 'iocScan';
  targetHost: string;
  params: {
    // the path to the zip archive with ioc files in base64 encoding
    ioc: string;
    // isolation of the computer from the network
    isolateHost: boolean;
    // critical areas scan
    scanCriticalAreas: boolean;
    // quarantine the file
    quarantineObject: boolean;
  };
  responseEventIncidentArea: string;
};
```

Process starten – startProcess

Instellingen van Process starten-taak

Parameter	Type	Beschrijving
executablePath	string	Pad naar het uitvoerbare bestand dat wordt gebruikt om het proces te starten.
arguments?	string	Aanvullende opdrachtregelargumenten om het proces te starten.
workingFolder?	string	Pad naar de werkmap van het proces.

Voorbeeld

```
type startProcess = {
  task: 'startProcess';
  targetHost: string;
  params: {
    // the path to the file
    executablePath: string;
    // command line arguments, optional
    arguments?: string;
    // a working folder, optional
    workingFolder?: string;
  };
  responseEventIncidentArea: string;
};
```

Proces beëindigen – terminateProcess

Instellingen van Proces beëindigen-taak

Parameter	Type	Beschrijving
md5hash	string	MD5-hash van het bestand waarvan u het proces wilt beëindigen.
sha256hash	string	SHA256-hash van het bestand waarvan u het proces wilt beëindigen.
path	string	Pad naar het bestand dat u wilt verwijderen.
caseSensitive	boolean	Hoofdlettergevoeligheid bij het zoeken naar het bestand.

Voorbeeld

```
type terminateProcess = {
  task: 'terminateProcess';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

Computer isoleren van netwerk – isolateHost

Instellingen voor Computer isoleren van netwerk

Parameter	Type	Beschrijving
`action`	`string`	Werkingsmodus van Netwerkisolatie.

Voorbeeld

```
type isolateHost = {
  task: 'isolateHost';
  targetHost: string;
  params: {
    // 0 - turning off network isolation, 1 - turning on network isolation
    action: number;
  };
  responseEventIncidentArea: string;
};
```

Preventie van uitvoering – preventExecution

Instellingen preventie van uitvoering

Parameter	Type	Beschrijving
`hash`	`string`	MD5-hash van het bestand dat u niet wil uitvoeren.
`path`	`string`	Pad naar het bestand dat u niet wilt uitvoeren.
`caseSensitive`	`boolean`	Hoofdlettergevoeligheid bij het zoeken naar het bestand.

Voorbeeld

```
type preventExecution = {
  task: 'preventExecution';
  targetHost: string;
  params: {
    // a valid md5 hash of the file
    hash: string;
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

Malware-scan – onDemandScan

Instellingen van Malware-scan-taak

Parameter	Type	Beschrijving
`path`	`string`	Een door spaties gescheiden lijst met bestanden en mappen voor Aangepaste Scan.
`recursive`	`boolean`	Recursieve scanmodus.

Parameter	Type	Beschrijving
type	`number`	Scanbereik.

```
ScanObjectType = Enum("ScanObjectType",
                      [
                          ("SystemMemory", 14),
                          ("StartupObjectsAndRunningProcesses", 15),
                          ("DiskBootSectors", 16),
                          ("SystemBackupStorage", 17),
                          ("Email", 18),
                          ("Folder", 22),
                          ("AllRemovableDrives", 23),
                          ("AllNetworkDrives", 24),
                          ("AllFixedDrives", 25)])
```

Voorbeeld

```
type onDemandScan = {
  task: 'onDemandScan';
  targetHost: string;
  // please note, this is an array
  // array of scan object
  params: [{
    // enabling the scan object
    enabled: boolean;
    // an empty string or the path to the folder to scan
    path: string;
    // recursive scan mode
    recursive: boolean;
    // ID scan object
    type: number;
  }];
  responseEventIncidentArea: string;
};
```

Appendix 12. Gebruikersaccounts in regels voor programma-onderdelen

Om bepaalde programma-onderdelen te configureren, moet je speciale regels toevoegen. Voor webcontrole moet je bijvoorbeeld een regel toevoegen met een lijst van webadressen waarvan je wilt dat het programma ze blokkeert. In regels voor programma-onderdelen, kun je ook een schema configureren voor de onderdelen of bepaalde gebruikers waarvoor het programma de regel moet toepassen.

Regels moeten worden toegevoegd om de volgende programma-onderdelen te configureren:

- Programmacontrole.
- Webcontrole.
- Apparaatcontrole.
- Log Inspectie.
- Adaptieve controle op afwijkingen.
- Systeemintegriteitscontrole.

Vanaf Kaspersky Endpoint Security voor Windows 12.5, kun je nu niet alleen gebruikers selecteren uit je Active Directory, maar ook van de lijst van gebruikers in Kaspersky Security Center. U kunt ook handmatig lokale gebruikersaccountgegevens invoeren. Dit houdt in dat je gebruikers op de volgende manieren kunt toevoegen:

- Active Directory (aanbevolen)
- Lijst van gebruikers in Kaspersky Security Center
- Lokale gebruikersaccount

Om alle gebruikersselectiemethodes correct te gebruiken, moet je de Kaspersky Endpoint Security applicatie en beheerplugin updaten naar versie 12.5 of hoger.

Kaspersky raadt aan om locale gebruikersaccounts alleen in speciale gevallen te gebruiken, wanneer het niet mogelijk is om domeingebruikersaccounts te gebruiken. Voor details over de beveiligingsrisico' van het gebruik van lokale accounts, bekijk de Microsoft Knowledge Base. Je hebt volledige verantwoordelijkheid voor de beveiliging van een computer indien lokale gebruikersaccount gebruikt worden; in het bijzonder omvat dit de verantwoordelijkheid voor het beheren en beperken van toegang tot Kaspersky Endpoint Security-instellingen.

Het programma gebruikt de SID (veiligheidsidentificatie) van de gebruiker om gebruikers te identificeren. Bij het gebruik van gebruikersaccounts uit Active Directory of uit de Kaspersky Security Center-gebruikerslijst, bepaalt het programma de SID op de Administration Server. Dit hout in dat het programma de computer niet extra belast om een gebruiker te identificeren. Als je meer dan 1000 gebruikers aan een programmaregel hebt toegevoegd, maken de programma's contact met de domeinbeheerder om de gebruiker te identificeren. Dit betekent dat de belasting van de computer verhoogd is. Om de impact op de prestaties van de computer te optimaliseren, raden we aan om gebruikersaccounts uit Active Directory of de gebuikerslijst van Kaspersky Security Center te gebruiken.

Het programma gebruikt NetBIOS-namen voor de identificatie van handmatig toegevoegde gebruikersaccounts in de `<username>` en `<hostname>\<username>` formaten. Een NetBIOS-naam mag maximaal 16 bytes (15 tekens) lang zijn. Als de computernaam langer is dan 15 tekens, kan het programma de gebruiker niet identificeren. Vervolgens schakelt het programma de regel uit en genereert het een fout, bijvoorbeeld *Web Control: rule triggering disabled for user accounts without matching security identifier (SID)*. Om de regel te laten werken, moet u de computernaam handmatig inkorten. U kunt gebruikersaccounts toevoegen vanuit Active Directory of Kaspersky Security Center. In dit geval zal het programma de computernaam automatisch inkorten.

Kaspersky Endpoint Security ondersteunt ook ingebouwde gebruikers en groepen (zoals de groep "Alle") in regels. Vanwege de manier waarop de SID van een gebruiker wordt bepaald, staat het programma het gebruik van alleen ingebouwde gebruikersaccounts toe die zijn toegevoegd vanuit Active Directory of de lijst met gebruikers in Kaspersky Security Center. Regels waarbij een ingebouwd gebruikersaccount lokaal wordt toegevoegd, werken niet.

Juridische informatie

Gegevensverstrekking

Deze sectie bevat informatie over de gegevens die het Kaspersky Endpoint Security-programma op het apparaat kan opslaan en automatisch naar Kaspersky kan verzenden tijdens de werking ervan.

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.

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);
- het unieke verzoek-ID voor de services van de Rechthebbende;
- 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 actuele 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 programmagebruik 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 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.

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 schadelijke 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 verbindingsstatus, 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, Verwisselbare 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 gebeurtenistracering (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-prestatiemetriek (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 geheugentoewijzing), 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-systeemmappen (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 Kaspersky Endpoint Detection and Response, Kaspersky Sandbox En Kaspersky Anti Targeted Attack Platform 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 waardenaam)
- Register instelling
- Systeem (omgeving)

- Naam en versie van het besturingssysteem dat op de computer is geïnstalleerd
- Netwerknaam 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-query 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` of `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-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 waardenaam)
- Register instelling
- Systeem (omgeving)

- Naam en versie van het besturingssysteem dat op de computer is geïnstalleerd
- Netwerknaam 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-query heeft gedaan

Kaspersky Endpoint Detection and Response Expert (on-premises)

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

Service gegevens

De ingebouwde agent van Kaspersky Endpoint Security slaat de volgende gegevens lokaal op:

- Vereiste gegevens voor integratie met het onderdeel EDR Expert (on-premises):
  - Adres en poort voor verbinding met de KATA Central Node-server
  - Adres en poort voor verbinding met de server voor telemetrietransmissie
  - Adres en poort voor verbinding met de responsserver

    - Informatie over certificaten die worden gebruikt voor integratie met KATA Central Node
    - Informatie over certificaten die worden gebruikt voor integratie met de telemetrietransmissieserver
    - Informatie over certificaten die worden gebruikt voor integratie met de responsserver
- In quarantaine geplaatste bestanden

Gegevens van verzonden telemetriegebeurtenissen

- **Telemetrische gegevens**
    - Gegevens over bestanden:
        - Unieke ID's van het bestand
        - Bestandstype
        - Volledig bestandspad
        - Bestandsgrootte
        - Bestandskenmerken
        - Zone-aanduiding
        - Datum en tijd waarop het bestand is aangemaakt
        - Datum en tijd waarop het bestand voor het laatst is gewijzigd
        - Oorspronkelijke bestandsnaam
        - Programmanaam
        - Programmaversie
        - Programmaleverancier
        - Bestandsomschrijving
        - Bestandsversie
        - MD5- en SHA256-hashes van het object
        - Resultaat van de bestandshandtekeningsverificatie
        - Naam van certificaatuitgever
        - Naam van certificaathouder
        - Serienummer van certificaat

- Gegevens over AMSI-scan:
  - Unieke identificatie van het proces dat de activiteit tot stand heeft gebracht
  - Inhoudstype van het object doorgegeven aan AMSI
  - Inhoud van het object doorgegeven aan AMSI
  - Naam object
  - MD5- en SHA256-hashes van het object
- Gegevens over de blokkering van programma's:
  - Unieke identificatie van het proces dat de blokkering van het programma tot stand heeft gebracht
  - Unieke identificatie van het bovenliggende proces
  - Unieke systeemidentificatie van het proces
  - Gebruikte opdracht om een proces te starten
  - Gebruikersnaam sessie ID
  - Procesintegriteitsniveau
  - Processtatus
  - Unieke identificatie van het procesbestand
  - Verwerk de opdrachtregel
  - Lijst met unieke identificatie van geïnterpreteerde bestanden
- Gegevens over geblokkeerde bestandsopeningen:
  - Unieke identificatie van het proces dat het openen van het bestand tot stand heeft gebracht
  - Unieke ID's van het bestand
- Gegevens over het laden van stuurprogramma's:
  - Unieke identificatie van het geladen stuurprogramma
- Gegevens over evenementen:
  - Unieke identificatie van de gebeurtenis
  - Datum en tijd van de gebeurtenis
- Gegevens over bestandswijziging:
  - Unieke identificatie van het proces dat de bestandswijziging tot stand heeft gebracht
  - Unieke ID's van het bestand

    - Type van de wijzigingsbewerking
    - Vlag die aangeeft dat het bestand wordt verwijderd nadat de computer opnieuw is opgestart
    - Unieke identificatie van het gewijzigde bestand
    - Unieke identificatie van het bestand vóór wijziging
    - Set bitvlaggen die bepalen hoe het bestand is geopend
    - Gegevens over bewerkingen in de toegangscontrolelijst
    - Gegevens over wijzigingen in het eigendom of de bovenliggende groep van het bestand
- Inlogsessiegegevens:
    - Gebruikersnaam sessie ID
    - Naam van de aangemelde gebruiker
    - Type gebruikersaccount
    - Sessietype
- Gegevens over netwerkverbindingen:
    - Unieke identificatie van het proces dat de verbinding tot stand heeft gebracht
    - Lokaal IP-adres dat gebruikt is om de verbinding tot stand te brengen
    - Extern IP-adres van het eindpunt van de verbinding
    - Verbindingsrichting
    - Gegevensoverdrachtsprotocol
    - HTTP-methode
    - Pad zonder de hostnaam
    - Hostnaam
    - Dynamische processtatus op het moment van de verbinding
    - Vlag die aangeeft dat de verbinding open is op raw socketniveau
    - TLS-versie gebruikt in de verbindingssessie
    - Naam van de TLS-server
    - MD5- en SHA1-hashes van het TLS-servercertificaat
    - Lijst met alternatieve namen (SAN) van het certificaat
    - Naam van de uitgever van het TLS-certificaat

    - Serienummer van certificaat
    - Gebruikt encryptie-algoritme
    - Begin- en einddatum van het certificaat
    - JA3-vingerafdruk van de TLS-client
    - JA3S-vingerafdruk van de server
- Gegevens die zijn vastgelegd tijdens het luisteren via een netwerkpoort:
    - Unieke identificatie van het proces dat de verbinding tot stand heeft gebracht
- Invoergegevens via de opdrachtregel:
    - Unieke identificatie van het proces dat de console-invoer tot stand heeft gebracht
    - Invoertype console
    - Tekst ingevoerd door een gebruiker of een proces
- Gegevens over het aanmaken van processen:
    - Unieke identificatie van het proces
    - Unieke identificatie van het bovenliggende proces
    - Unieke systeemidentificatie van het proces
    - Gebruikte opdracht om een proces te starten
    - Gebruikersnaam sessie ID
    - Procesintegriteitsniveau
    - Unieke identificatie van het procesbestand
    - Lijst met unieke identificatie van geïnterpreteerde bestanden
    - Procestype
- Gegevens over de module die door het proces is geladen:
    - Unieke identificatie van het proces dat de download tot stand heeft gebracht
    - Volledig pad naar het bestand dat naar het proces is geüpload
    - Unieke identificatie van het modulebestand
    - Volledige naam van de .NET-assembly, als het geladen bestand een .NET-module is
    - Vlaggen van de .NET-assembly gedefinieerd in het manifest

- Gegevens over procesbeëindiging:
  - Unieke identificatie van het beëindigde proces
- Gegevens over wijzigingen in het register:
  - Unieke identificatie van het proces dat de registerwijziging tot stand heeft gebracht
  - Type registerbewerking
  - Volledig pad naar de registersleutel
  - Naam van de waarde in een registersleutel
  - Type gegevens opgeslagen in de waarde van de registersleutel
  - Gegevens opgegeven in de waarde van de registersleutel
  - Naam van de sleutel vóór hernoemen
  - Informatie over een verandering in het eigendom van de sleutel of primaire sleutelgroep
  - Lijst met wijzigingen in de toegangscontrolelijst (ACL) van de sleutel
- Gegevens over de gedetecteerde dreiging en de verwerking ervan:
  - Vlag die aangeeft dat dreigingsdetectie op de achtergrond werd uitgevoerd
  - Dreigingsoordeel
  - Naam van het verdict
  - Unieke identificatie van het databaserecord
  - Tijdstip waarop de dreigingsrecord is opgeslagen in de database
  - Modus voor het verwerken van bedreigingen
  - Geïnfecteerd objecttype
  - Naam van geïnfecteerd object
  - MD5- en SHA256-hashes van het object
  - Unieke identificatie van geïnfecteerd object
  - Unieke identificatie van het proces dat het geïnfecteerde object van internet heeft gedownload
  - URL waarvandaan het geïnfecteerde object is gedownload
  - E-mailadres van de afzender die het geïnfecteerde object heeft verzonden
  - Netwerkprotocol waarmee het geïnfecteerde object is ontvangen
  - Lokaal adres vanwaar het geïnfecteerde object is ontvangen

    - Extern adres vanwaar het geïnfecteerde object is ontvangen
    - Objectinhoudstype
    - Objectinhoud
- Gegevens over toegang tot processen:
    - Unieke identificatie van het proces dat toegang probeerde te verkrijgen
    - Unieke identificatie van het doelproces dat is geopend
    - Set van gevraagde rechten van het doelproces
    - Soort bewerking
    - Aantal oproepen op het moment dat een proces wordt geopend
    - Descriptor van het bronproces
    - Descriptor van het doelproces
- Gegevens over DNS:
    - Unieke identificatie van het proces dat de DNS-query tot stand heeft gebracht
    - IP-adres van DNS-server
    - Vlaggen die het gedrag van een DNS-query beheren
    - Verzoek van voltooiing van scan
    - Volledig gekwalificeerde domeinnaam opgegeven in de DNS-query
    - Gegevenstype in de DNS-query
    - Antwoorden van de DNS-server
- Gegevens over code-injectie:
    - Unieke identificatie van het proces dat code probeerde te injecteren
    - Gebruikte toegangsmethode
    - Aantal oproepen op het moment dat de geïnjecteerde code werd gedetecteerd
    - Unieke identificatie van het doelproces waarnaar de code is geüpload
    - Gegevens over wijzigingen in de volgorde van opdrachten van het doelproces
    - Adres van doelproces
    - Naam van de DLL-bibliotheek die naar het doelproces is geüpload
    - Volledige pad naar het DDL-bestand

- Gegevens over bewerkingen met benoemde kanalen:
  - Unieke identificatie van het proces dat het kanaal heeft gemaakt of ermee verbonden is
  - Volledige naam van het genoemde kanaal
  - Type bewerking (aanmaak of verbinding)
- Gegevens over WMI-query's:
  - Unieke identificatie van het proces dat de WMI-bewerking tot stand heeft gebracht
  - Type WMI-bewerking
  - Naam van het doelapparaat voor de WMI-query
  - Gebruikersaccount waarmee de WMI-query is gestart
  - Tekst van de WMI-query
  - Naamruimte waarin de WMI-query wordt uitgevoerd
  - Naam WMI-filter
  - Naam van het consumentenobject
  - Tekst die de actie van het consumentenobject beschrijft
- Gegevens over LDAP-query's:
  - Unieke identificatie van het proces dat het LDAP-query heeft gedaan
  - Zoekbereik van LDAP query's
  - LDAP filter
  - Parameter die de Active Directory-partitie aangeeft waarnaar de query is gericht
  - LDAP zoekkenmerken
- Gegevens over aangesloten USB-apparaten:
  - Type bewerking USB-apparaat
  - USB-apparaattype
  - Identificatie van het USB-apparaat
  - USB-apparaatnaam
  - Pad naar het USB-apparaat
  - Vlag die aangeeft dat het USB-apparaat een systeemstation is
- Gegevens over het maken, verwijderen en wijzigen van een geplande taak

- Gegevens over het maken, verwijderen en wijzigen van services
- Gegevens over het aan- en afkoppelen van het bestandssysteem
- Gegevens over de werking van het on-premises onderdeel van EDR Expert:
  - Informatie over het starten/stoppen van de agent
  - Informatie over het installeren en verwijderen van de agent
  - Unieke ID voor de start van de agent
  - Systeem-ID van het agentproces
  - Unieke identificatie van het agentproces
  - Reden voor de beëindiging van de agent
  - Beëindigingscode agentproces
- Instellingen voor gebeurtenisfiltering:
  - Module namen
  - Volledige paden naar objecten
  - MD5- en SHA256-hashes van de objecten
  - Identificaties van de vermeldingen in het Windows-gebeurtenislogboek
  - Instellingen voor digitale certificaten
  - Verkeersrichting, IP-adressen, poorten, protocollen, volledige paden naar uitvoerbare bestanden
  - Gebruikersnamen
  - Aanmeldingstypen voor gebruikers
  - Typen telemetriegebeurtenissen waarvoor filters worden toegepast

Gegevens van verzoeken van het onderdeel EDR Expert aan de ingebouwde agent van Kaspersky Endpoint Security

- Algemene taakinstellingen:
  - Type taak
  - Instellingen voor taakschema's
  - Namen en wachtwoorden van de accounts waaronder de taken kunnen worden uitgevoerd
  - Versies van instellingen

- ID's van in quarantaine geplaatste objecten
- Paden naar de objecten
- MD5- en SHA256-hashes van de objecten
- Opdrachtregel om het proces met de argumenten te starten
- Vlaggen van de aanvullende acties die zijn uitgevoerd na voltooiing van taken
- IOC-bestands-ID's die van de server moeten worden opgehaald
- IOC-bestanden
- Service naam
- Type opstartservice
- Mappen waarvoor de resultaten van de *Get forensic* taak moeten worden ontvangen
- Maskers van de objectnamen en extensies voor de *Get forensic* taak

- Instellingen voor netwerkisolatie:
  - Soorten instellingen
  - Versies van instellingen
  - Lijsten met netwerkisolatie-uitsluitingen en uitsluitingsinstellingen: verkeersrichting, IP-adressen, poorten, protocollen en volledige paden naar uitvoerbare bestanden
  - Vlaggen van de aanvullende acties
  - Tijdstip van automatische uitschakeling van de isolatie
- Instellingen preventie van uitvoering:
  - Soorten instellingen
  - Versies van instellingen
  - Lijsten met uitvoeringspreventieregels en regelinstellingen: paden naar objecten, typen objecten, MD5- en SHA256-hashes van objecten
  - Vlaggen van de aanvullende acties

Gegevens van verzoeken die door Kaspersky Endpoint Security naar het onderdeel EDR Expert worden verzonden

Bij integratie met de EDR Expert (on-premises) oplossing worden de volgende gegevens lokaal op de computers opgeslagen.

- Bij synchronisatieverzoeken:
  - Unieke ID
  - Basisgedeelte van het webadres van de server
  - Computer naam
  - IP-adres van de computer
  - MAC-adres van de computer
  - Lokale tijd op de computer
  - Zelfverdedigingsstatus van Kaspersky Endpoint Security
  - Naam en versie van het besturingssysteem dat op de computer is geïnstalleerd
  - Versie van Kaspersky Endpoint Security
  - Versies van de applicatie-instellingen en taakinstellingen
  - Taakstatussen: identifiers van taken, uitvoeringsstatussen, foutcodes
- In verzoeken om bestanden van de server te verkrijgen:
  - Unieke identificatiegegevens van bestanden
  - Unieke identificatie van Kaspersky Endpoint Security
  - Unieke identificatiecodes van certificaten
  - Basisgedeelte van het webadres van de server waarop de Central Node-component is geïnstalleerd
  - Host IP-adres
- In de rapporten over de resultaten van de taakuitvoering:
  - Host IP-adres
  - Informatie over de gedetecteerde objecten tijdens een IOC-scan of YARA-scan
  - Vlaggen van de aanvullende acties die zijn uitgevoerd na voltooiing van taken
  - Taakuitvoeringsfouten en retourcodes
  - Voltooiingsstatussen van taken

- Voltooiingstijd van de taak
- Versies van de instellingen die worden gebruikt voor de uitvoering van de taken
- Informatie over de objecten die naar de server zijn verzonden, in quarantaine geplaatste objecten en objecten die uit quarantaine zijn hersteld: paden naar objecten, MD5- en SHA256-hashes, identifiers van in quarantaine geplaatste objecten
- Informatie over de processen die zijn gestart of gestopt op een computer op verzoek van de server: PID en UniquePID, foutcode, MD5- en SHA256-hashes van de objecten
- Informatie over de services die op een computer zijn gestart of gestopt op verzoek van de server: servicenaam, opstarttype, foutcode, MD5- en SHA256-hashes van bestandsafbeeldingen van de services
- Informatie over de objecten waarvoor een geheugendump is gemaakt voor een YARA-scan (paths, dump file identifier)
- Bestanden aangevraagd door de server

- Gegevens over lopende processen:
  - Uitvoerbare bestandsnaam, inclusief volledig pad en extensie
  - Parameters voor automatisch starten verwerken
  - Proces-ID
  - Gebruikersnaam sessie ID
  - Naam aanmeldingssessie
  - Datum en tijd waarop het proces is gestart
  - MD5- en SHA256-hashes van het object
- Gegevens over bestanden:
  - Het bestandspad
  - Bestandsnaam
  - Bestandsgrootte
  - Bestandskenmerken
  - Datum en tijd waarop het bestand is aangemaakt
  - Datum en tijd waarop het bestand voor het laatst is gewijzigd
  - Bestandsomschrijving
  - Bedrijfsnaam

- MD5- en SHA256-hashes van het object
- Registersleutel (voor punten voor automatisch starten)

- Gegevens in fouten die optreden wanneer informatie over objecten werd opgehaald:
  - Volledige naam van het object dat werd verwerkt toen er een fout optrad
  - Foutcode
- Gegevens in YARA scanresultaten

  De ingebouwde agent van Kaspersky Endpoint Security draagt automatisch YARA-scanresultaten over naar Kaspersky Anti Targeted Attack Platform om een ontwikkelingsketen voor bedreigingen op te bouwen.

  De gegevens worden tijdelijk lokaal opgeslagen in de wachtrij voor het verzenden van taakuitvoeringsresultaten naar de Kaspersky Anti Targeted Attack Platform-server. Na verzending worden de gegevens uit de tijdelijke opslag verwijderd.
  - MD5- en SHA256-hashes van het bestand
  - Volledige naam van het bestand
  - Het bestandspad
  - Bestandsgrootte
  - 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
- Gegevens in IOC scanresultaten
  - IP-adres uit de ARP-tabel
  - Fysiek adres uit de ARP-tabel
  - DNS-recordnaam
  - DNS-recordtype
  - Hostnaam
  - IP-adres
  - Gebeurtenis-ID in het logboek

- Naam gegevensbron in het logboek
- Lognaam
- Gebruikersnaam
- Datum en tijd waarop de gebeurtenis is gegenereerd, in ISO-indeling
- MD5- en SHA256-hashes van het bestand
- Volledige naam van het bestand
- Bestandsgrootte
- Extern IP-adres en poort waarmee tijdens het scannen verbinding is gemaakt
- IP-adres en poort van de lokale adapter
- Protocol
- 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
- Pad naar de registersleutel
- Naam van registersleutel
- Tekstwaarde van de registersleutel
- Service naam
- Dienstbeschrijving
- Pad en naam van de DLL-service
- Pad en naam van het uitvoerbare servicebestand
- Windows-ID (PID) van de service
- Servicetype
- Service status
- Servicestartmodus

- Naam van het besturingssysteem
- Versie van het besturingssysteem
- Naam van computernetwerk zonder domein
- Domein of werkgroep
- Gebruikersnaam
- Volumenaam
- Volume brief
- Volumetype

Kaspersky Network Detection and Response (KATA)

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

Telemetrische gegevens

- **Gegevens over bestanden:**
  - Unieke ID's van het bestand
  - Bestandstype
  - Volledig bestandspad
  - Bestandsgrootte
  - Bestandskenmerken
  - Zone-aanduiding
  - Datum en tijd waarop het bestand is aangemaakt
  - Datum en tijd waarop het bestand voor het laatst is gewijzigd
  - Oorspronkelijke bestandsnaam
  - Programmanaam
  - Programmaversie
  - Programmaleverancier

- Bestandsomschrijving
- Bestandsversie
- MD5- en SHA256-hashes van het object
- Resultaat van de bestandshandtekeningsverificatie
- Datum en tijd waarop de bestandshandtekening is aangemaakt
- In het handtekeningbestand gebruikte certificaatketens
- Type certificaatketen
- Certificaten in de keten
- Naam van certificaatuitgever
- Naam van certificaathouder
- Serienummer van certificaat
- Algoritme van vingerafdruk van certificaat
- Vingerafdruk van certificaat
- Geldigheidsperiode van het certificaat

- **Inlogsessiegegevens**
  - Gebruikersnaam sessie ID
  - Accountnaam van de aangemelde gebruiker
  - Type gebruikersaccount
  - Sessietype
  - IP-adres van het apparaat geprobeerd is aan te melden
  - IP-adres van het lokale apparaat waarvoor is geprobeerd aan te melden
  - Vlag die aangeeft dat de sessie die door deze gebeurtenis wordt vertegenwoordigd, verhoogde privileges en administratieve rechten heeft
  - Parameter die aangeeft of andere sessies zijn gekoppeld aan deze inlogsessie
  - Voor de terminalsessie gebruikt protocol
  - Voor de terminalsessie gebruikt IPv4-protocol

- **Gegevens over netwerkcommunicatie**
  - Begin en einde van het tijdsinterval waarin de gegevens zijn verzameld
  - Lijst van verbindingen
  - Lokaal IP-adres van de computer
  - Lokaal MAC-adres van de computer
  - Extern IP-adres van de computer
  - Extern MAC-adres van de computer
  - Gateway-IP-adres
  - Aantal verzonden datapakketten
  - Aantal ontvangen datapakketten
  - Totaal aantal overgedragen bytes
  - Gegevensoverdrachtsprotocol
  - Ethernet-frame EtherType-veld
  - Payload-voorvoegsel van het eerste pakket in het interval
  - IPv4-adres van de netwerkinterface waarmee de communicatie is vastgelegd
- **Gegevens over netwerkverbinding**
  - Unieke identificatie van het proces dat de verbinding tot stand heeft gebracht
  - Gegevensoverdrachtsprotocol
  - Lokaal IP-adres dat gebruikt is om de verbinding tot stand te brengen
  - Extern IP-adres van het eindpunt van de verbinding
  - HTTP-methode
  - Pad zonder de hostnaam
  - Hostnaam
  - Dynamische processtatus op het moment van de verbinding
  - Verbindingsrichting
  - Dynamische processtatus
  - Ethernet-frame EtherType-veld

- **Gegevens die zijn vastgelegd tijdens het luisteren via een netwerkpoort**
  - Unieke identificatie van het proces dat de verbinding tot stand heeft gebracht
  - Gegevensoverdrachtsprotocol
  - Lokaal adres
  - Dynamische processtatus op het moment van de verbinding
- **Resultaat van verbindingsverificatie**
  - Hostnetwerkinstellingen
  - Netwerkinterfacebeschrijving
  - DNS-domeinnaam
  - Lokaal MAC-adres van de computer
  - Metrisch nummer van IP-verbinding
  - Lijst met IP-adressen
  - IP-adres
  - Netwerkmasker
  - Gateway-IP-adres
  - Gateway-MAC-adres
  - Lijst met geïnstalleerde patches
  - Patchnummer
  - Installatiedatum patch
  - Apparaatmodel
  - Apparaatleverancier
  - Host-ID in Kaspersky Security Center
  - Beschrijving van het geïnstalleerde Kaspersky-antivirusprogramma
  - Onderdeelnaam van het geïnstalleerde Kaspersky-antivirusprogramma
  - Onderdeelversie van het geïnstalleerde Kaspersky-antivirusprogramma
  - Databaseversie van het geïnstalleerde Kaspersky-antivirusonderdeel
  - Datum van de laatste database-update van het geïnstalleerde Kaspersky-antivirusonderdeel
  - Onderdeelstatus van geïnstalleerde Kaspersky-antivirusonderdeel

- Lijst van licentiesleutels
- Serienummer van de sleutel
- Sleuteltype
- Verloopdatum van sleutel
- Sleutelstatus

- **Gegevens over het aanmaken van processen op de host**
  - Unieke identificatie van het proces
  - Unieke identificatie van het bovenliggende proces
  - Unieke systeemidentificatie van het proces
  - Gebruikte opdracht om een proces te starten
  - Gebruikersnaam sessie ID
  - Terminalsessie ID
  - Unieke identificatie van het procesbestand
  - Procesintegriteitsniveau
  - Lijst van procesrechtentokens
  - Atribuutrechten
  - Lijst met unieke identificatie van geïnterpreteerde bestanden
  - Processtatus
  - Gebruikte opdracht om een proces te starten
- **Gegevens over procesbeëindiging**
  - Unieke identificatie van het proces
- **Gegevens over gedetecteerde dreiging**
  - Dreigingsinformatie
  - Dreigingsoordeel
  - AMR-recordnummer
  - Antivirusdatabaseversie
  - Dreigingsdetectiemodus
  - Unieke bedreigingsidentificatie

- Beschermingstechnologie
- Informatie over geïnfecteerd object
- Geïnfecteerd objecttype
- Naam van geïnfecteerd object
- MD5- en SHA256-hashes van het object
- Unieke identificatie van geïnfecteerde proces
- Unieke identificatie van geïnfecteerd object
- Unieke identificatie van het proces dat het geïnfecteerde object van internet heeft gedownload
- URL waarvandaan het geïnfecteerde object is gedownload
- E-mailadres van de afzender die het geïnfecteerde object heeft verzonden
- Netwerkprotocol waarmee het geïnfecteerde object is ontvangen
- Lokaal adres vanwaar het geïnfecteerde object is ontvangen
- Extern adres vanwaar het geïnfecteerde object is ontvangen
- Objectinhoudstype
- Context van gedetecteerde dreiging
- Objectinhoud
- Vlag die aangeeft dat dreigingsdetectie op de achtergrond werd uitgevoerd

- **Gegevens over dreigingsverwerking**
  - Dreigingsinformatie
  - Dreigingsoordeel
  - AMR-recordnummer
  - Antivirusdatabaseversie
  - Dreigingsdetectiemodus
  - Naam van geïnfecteerd object
  - MD5- en SHA256-hashes van het object
  - Unieke identificatie van geïnfecteerde proces
  - Unieke identificatie van geïnfecteerd object
  - Netwerkprotocol waarmee het geïnfecteerde object is ontvangen

- Lokaal adres vanwaar het geïnfecteerde object is ontvangen
- Extern adres vanwaar het geïnfecteerde object is ontvangen
- Dreigingsverwerkingsstatus
- Reden waarom de dreiging niet kon worden verholpen
- Lokaal fysiek adres

- **Gegevens over gebruikers**
  - Gebruikers-SID
  - Gebruikers-ID
  - Gebruikersnaam
  - Volledige naam van de gebruiker
  - Gebruikersbeschrijving
  - Of het account actief of geblokkeerd is
  - Of het wachtwoord is verlopen
  - Of een wijziging van het wachtwoord vereist is
  - Of het wijzigen van het wachtwoord is toegestaan
  - Type gebruikersaccount
  - Of automatisch inloggen is ingeschakeld voor dit account
  - Lijst met groepen waartoe de gebruiker behoort

Integratie met Kaspersky Unified Monitoring and Analysis Platform (KUMA)

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

Bij de integratie met Kaspersky Unified Monitoring and Analysis Platform (KUMA) worden de gegevens van de verbindingsinstellingen en alle geregistreerde gebeurtenissen in Windows Logs overgedragen.

De belangrijkste gebeurtenislogboeken van Windows zijn Systeem, Beveiliging, Programma, ForwardedEvents en HardwareEvents. Gebruikers kunnen ook aangepaste logboeken maken en ermee werken om aan hun specifieke vereisten te voldoen.

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.

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 programmagebruik 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 Kaspersky Private Security Network (KPSN) of schakel het gebruik van KSN uit. Voor meer informatie over KPSN 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, gebruik een licentiebestand toe 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.

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 in de Verenigde Staten en/of andere landen.

Amazon, Amazon Web Services, AWS zijn handelsmerken van Amazon.com, Inc. of diens dochterondernemingen.

Apple, FireWire, iTunes, Mac en Safari zijn handelsmerken van Apple Inc.

Arm is een gedeponeerd handelsmerk van Arm Limited (of haar dochterondernemingen) in de VS en/of 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.

Cisco, Cisco AnyConnect, IOS zijn gedeponeerde handelsmerken of handelsmerken van Cisco Systems, Inc. en/of diens gelieerde ondernemingen in de Verenigde Staten en bepaalde andere landen.

Citrix, Citrix Provisioning, Citrix Provisioning Services, Citrix Virtual Apps and Desktop, XenDesktop en XenServer zijn gedeponeerde handelsmerken of handelsmerken van Cloud Software Group, Inc. en/of haar dochterondernemingen in de Verenigde Staten en/of andere landen.

Cloudflare, Cloudflare Workers en het Cloudflare-logo zijn handelsmerken en/of gedeponeerde handelsmerken van Cloudflare, Inc. in de Verenigde Staten en andere rechtsgebieden.

Core is een handelsmerk van Intel Corporation of haar dochterondernemingen.

dBase is een handelsmerk van dataBased Intelligence, Inc.

Dell Technologies, Dell, EMC en andere handelsmerken zijn handelsmerken van Dell Inc. of haar dochterondernemingen.

Docker en het Docker-logo zijn handelsmerken of gedeponeerde handelsmerken van Docker, Inc. in de Verenigde Staten en/of andere landen. Docker, Inc. en andere partijen kunnen ook handelsmerkrechten hebben in andere voorwaarden die hierin worden gebruikt.

ESET is een handelsmerk of geregistreerd handelsmerk van ESET spol. s r.o. of de respectieve ESET-entiteit.

Foxit is een gedeponeerd handelsmerk van Foxit Corporation.

Radmin is een gedeponeerd handelsmerk van Famatech.

Google, Android, Google Public DNS, Google Chrome, Chrome zijn handelsmerken van Google, LLC.

HUAWEI, FusionCompute en FusionSphere zijn handelsmerken van Huawei Technologies Co.

ICQ is een Handelsmerk en/of Dienstmerk van ICQ LLC.

Intel is een handelsmerk van Intel Corporation of haar dochterondernemingen.

IBM is een gedeponeerd handelsmerk van International Business Machines Corporation in veel jurisdicties wereldwijd.

Lenovo en Lenovo 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 handelsmerk van Mail.ru, LLC.

McAfee is het handelsmerk of geregistreerde handelsmerk van McAfee LLC of haar dochterondernemingen in de VS en/of andere landen.

Microsoft, Access, Active Directory, ActiveSync, Bing, BitLocker, Excel, Hyper-V, Internet Explorer, JScript, LifeCam Cinema, Microsoft Edge, MSDN, MS-DOS, MultiPoint, Office 365, Outlook, PowerPoint, PowerShell, Skype, SQL Server, Surface, Visual Basic, Visual FoxPro, Windows, Windows Live, Windows PowerShell, Windows Server en Windows Store zijn handelsmerken van de Microsoft-bedrijvengroep.

Mozilla, Firefox en Thunderbird zijn handelsmerken van de Mozilla Foundation in de VS en andere landen.

NetApp is het handelsmerk of het gedeponeerde handelsmerk van NetApp, Inc. in de Verenigde Staten en/of andere landen.

OpenSSL is een handelsmerk van de OpenSSL Software Foundation.

OpenStack is een gedeponeerd handelsmerk van de OpenStack Foundation in de Verenigde Staten en andere landen.

Oracle, Java en JavaScript zijn gedeponeerde handelsmerken van Oracle en/of diens gelieerde ondernemingen.

Python is een handelsmerk of gedeponeerd handelsmerk van de Python Software Foundation.

Realtek is een handelsmerk van de Realtek Semiconductor Corporation.

SAMSUNG is een handelsmerk van SAMSUNG in de Verenigde Staten of andere landen.

Thawte is een handelsmerk of gedeponeerd handelsmerk van Symantec Corporation of diens gelieerde ondernemingen in de VS en andere landen.

Trend Micro is een handelsmerk of geregistreerd handelsmerk van Trend Micro Incorporated.

VERISIGN is een gedeponeerd handelsmerk in de Verenigde Staten en elders, of een niet-gedeponeerd handelsmerk van VeriSign, Inc. en haar dochterondernemingen.

VMware ESX, VMware ESXi, VMware Horizon, VMware Workstation, VMware Tools, VMware vSphere zijn gedeponeerde handelsmerken en/of handelsmerken van VMware, Inc. in de Verenigde Staten en andere landen.

Informatie over code van derden

Informatie over code van derden bevindt zich in het bestand legal_notices.txt in de installatiemap van het programma.