kaspersky

Kaspersky Endpoint Security 14.1 for Windows

© 2026 AO Kaspersky Lab

Cuprins

Ajutor pentru Kaspersky Endpoint Security for Windows

- Noutăți
- Probleme rezolvate
- Întrebări frecvente

Kaspersky Endpoint Security for Windows

- Moduri ale aplicației: Standard, EDR Agent, Light Agent
- Kitul de distribuire
- Cerințe hardware și software
- Compararea caracteristicilor disponibile ale aplicațiilor, în funcție de tipul de sistem de operare
- Compararea funcțiilor aplicației în funcție de instrumentele de gestionare
- Compatibilitatea cu alte aplicații

Instalarea și eliminarea aplicației

- Implementarea prin Kaspersky Security Center
  - Instalarea standard a aplicației
  - Crearea unui pachet de instalare
  - Actualizarea bazelor de date în pachetul de instalare
  - Crearea unui pachet de instalare la distanță
- Instalarea locală a aplicației folosind Expertul
- Instalarea la distanță a aplicației folosindu-se System Center Configuration Manager
- Descrierea setărilor fișierului setup.ini
- Modificare componente ale aplicației
- Upgradarea unei versiuni anterioare a aplicației
  - Efectuarea upgrade-ului aplicației fără repornire
  - Actualizarea SMU a aplicației
- Eliminarea aplicației

Licența aplicației

- Despre Acordul de licență pentru utilizatorul final
- Despre licență
- Despre certificatul de licență
- Despre abonament
- Despre cheia de licență
- Despre codul de activare
- Despre fișierul cheie
- Comparația funcționalității aplicației în funcție de tipul licenței pentru stații de lucru
- Compararea funcționalității aplicației în funcție de tipul licenței pentru servere
- Activarea aplicației
- Eliminarea unei chei de licență
- Vizualizarea informațiilor despre licență
- Achiziționarea unei licențe
- Reînnoirea abonamentului

Noțiuni de bază

- Despre upgrade-ul Plug-inului de gestionare al Kaspersky Endpoint Security for Windows
- Considerații speciale privind lucrul cu versiuni diferite de plug-inuri de gestionare

- Considerații speciale atunci când se utilizează protocoale criptate pentru interacțiunea cu servicii externe
- Interfața aplicației
  - Pictograma aplicației din zona de notificare a barei de activități
  - Interfață aplicație simplificată
  - Configurarea afișării interfeței aplicației
- Pregătirea aplicației pentru utilizare
- Gestionarea politicilor
  - Crearea unei politici
  - Exportarea și importarea unei polițe
  - Indicator nivel de securitate
- Gestionare activităților
- Configurarea setărilor generale ale aplicației
- Pornirea și oprirea Kaspersky Endpoint Security
- Trecerea în pauză și reluarea protecției și controlului computerului
- Crearea și folosirea unui fișier de configurare
- Restaurarea setărilor implicite ale aplicației
- Performanța și compatibilitatea produsului Kaspersky Endpoint Security cu alte aplicații
  - Activarea sau dezactivarea modului de economisire a energiei
  - Activarea sau dezactivarea cedării de resurse pentru alte aplicații
  - Cele mai bune practici pentru optimizarea performanței Kaspersky Endpoint Security

Scanare malware
- Scanarea computerului
- Scanarea unităților amovibile atunci când sunt conectate la computer
- Scanare în fundal
- Scanare din meniu contextual
- Verificare integritate aplicație
- Editarea domeniului de scanare
- Executarea unei scanări planificate
- Executarea unei scanări ca utilizator diferit
- Optimizarea scanării

Actualizarea bazelor de date și modulelor aplicației
- Scenarii de actualizare a bazei de date și a modulului de aplicație
  - Actualizarea din depozitul unui server
  - Actualizarea dintr-un director partajat
  - Actualizarea folosind Utilitarul de actualizare Kaspersky
  - Actualizarea în modul Mobil
- Pornirea și oprirea unei activități de actualizare
- Pornirea unei activități de actualizare utilizând drepturile altui cont de utilizator
- Selectarea modului de executare a activității de actualizare
- Adăugarea unei surse de actualizare
- Actualizarea modulelor aplicației
- Utilizarea unui server proxy pentru actualizări
- Derulare înapoi ultima actualizare

Tehnologia de dezinfectare avansată
- Dezinfectarea amenințărilor active pe stațiile de lucru
- Dezinfectarea amenințărilor active de pe servere

Eliminarea amenințărilor neprocesate

Protecția computerului
File Threat Protection
Activarea și dezactivarea componentei File Threat Protection
Punerea automată în pauză a componentei File Threat Protection
Modificarea acțiunii efectuate asupra fișierelor infectate de către componenta File Threat Protection
Specificarea domeniului de protecție al componentei File Threat Protection
Utilizarea metodelor de scanare
Folosirea tehnologiilor de scanare în funcționarea componentei File Threat Protection
Optimizarea scanării de fișiere
Scanarea fișierelor compuse
Schimbarea modului de scanare
Scanare containere
Host Intrusion Prevention
Activarea și dezactivarea componentei Host Intrusion Prevention
Administrarea grupurilor de încredere pentru aplicații
Modificarea grupului de încredere al unei aplicații
Configurarea drepturilor grupului de încredere
Selectarea unui grup de încredere pentru aplicații lansate înainte de Kaspersky Endpoint Security
Selectarea unui grup de încredere pentru aplicații necunoscute
Selectarea unui grup de încredere pentru aplicațiile semnate digital
Gestionarea drepturilor pentru aplicație
Protejarea resurselor sistemului de operare și a datelor personale
Ștergerea informațiilor despre aplicațiile neutilizate
Monitorizarea Host Intrusion Prevention
Protejarea accesului la componentele audio și video
BadUSB Attack Prevention
Activarea și dezactivarea componentei BadUSB Attack Prevention
Utilizarea tastaturii vizuale pentru autorizarea dispozitivelor USB
Autorizarea scanerului de coduri de bare
Protecție AMSI
Activarea și dezactivarea componentei Protecție AMSI
Optimizarea scanării fișierelor de către componenta Protecție AMSI
Web Threat Protection
Activarea și dezactivarea Web Threat Protection
Configurarea metodelor de detectare a adreselor web rău intenționate
Anti-Phishing
Crearea listei de adrese web de încredere
Exportul și importul listei de adrese URL de încredere
Mail Threat Protection
Activarea și dezactivarea Mail Threat Protection
Schimbarea acțiunii de efectuat asupra mesajelor de e-mail infectate
Specificarea domeniului de protecție al componentei Mail Threat Protection
Scanarea fișierelor compuse atașate la mesaje de e-mail
Filtrarea atașărilor mesajelor de e-mail
Exportul și importul extensiilor pentru filtrarea atașamentelor
Scanarea e-mailurilor în Microsoft Office Outlook
Scanarea e-mailurilor în Thunderbird, MyOffice, R7-Office

Network Threat Protection
- Activarea și dezactivarea componentei Network Threat Protection
- Blocarea unui computer atacator
- Configurarea adreselor de excluderi de la blocare
- Exportul și importul listei de excluderi de la blocare
- Configurarea componentei Network Threat Protection în funcție de tip

Firewall
- Activarea sau dezactivarea Firewall
- Modificarea tipului conexiunii la rețea
- Gestionarea regulilor pentru pachetele de rețea
  - Crearea unei reguli pentru pachetul de rețea
  - Activarea sau dezactivarea unei reguli pentru pachete de rețea
  - Modificarea acțiunii Firewall pentru o regulă pentru pachete de rețea
  - Modificarea priorității unei reguli pentru pachete de rețea
  - Exportul și importul regulilor de pachete de rețea
  - Definirea regulilor pentru pachetele de rețea în XML
- Administrarea regulilor de rețea ale aplicației
  - Crearea unei reguli de rețea pentru aplicație
  - Activarea și dezactivarea unei reguli de rețea pentru o aplicație
  - Modificarea acțiunii componentei Firewall pentru o regulă de rețea pentru o aplicație
  - Modificarea priorității unei reguli de rețea pentru o aplicație
- Monitorizare rețea

Exploit Prevention
- Activarea și dezactivarea componentei Exploit Prevention
- Protecție memorie pentru procese de sistem

Behavior Detection

Anti-Cryptor
- Activarea sau dezactivarea protecției directoarelor partajate împotriva criptării externe
- Configurarea perioadei de blocare a unui computer care nu are încredere
- Editarea domeniului de protecție
- Adăugarea de computere de încredere pentru criptarea datelor externe
- Exportarea și importarea unei liste de excluderi de la protecția directoarelor partajate împotriva criptării externe

Remediation Engine

Kaspersky Security Network
- Activarea și dezactivarea utilizării Kaspersky Security Network
- Limitări ale Kaspersky Private Security Network
- Activarea și dezactivarea modului cloud pentru componentele de protecție
- Setări proxy KSN
- Verificarea reputației unui fișier în Kaspersky Security Network

Scanare conexiuni criptate
- Activarea scanării conexiunii criptate
- Instalarea certificatelor rădăcină de încredere
- Scanarea conexiunilor criptate cu un certificat care nu este de încredere
- Adăugarea certificatului Kaspersky la propriul magazin de certificate
- Excluderea conexiunilor criptate de la scanare

Ștergere date

Controlul computerului
Control Web
Adăugarea unei reguli de acces la resursele web
Filtrare după adresele resurselor Web
Filtrare după conținutul resurselor Web
Testarea regulilor de acces la resurse Web
Exportul și importul regulilor Control Web
Exportul și importul adreselor resurselor web ale regulii Control Web
Monitorizarea activității pe Internet a utilizatorilor
Editarea șabloanelor de mesaje ale componentei Control Web
Editarea măștilor pentru adrese de resurse Web
Control web pentru mașini virtuale
Variabile în șabloanele de mesaje pentru Control Web
Control dispozitive
Despre regulile de acces
Gestionarea accesului la dispozitive în funcție de tip
Gestionarea accesului la dispozitive prin magistrala de conectare
Diferențierea drepturilor de acces ale utilizatorilor la dispozitive
Gestionarea accesului la dispozitivele mobile
Gestionarea accesului la dispozitivele Bluetooth
Controlul imprimării
Controlul conexiunilor Wi-Fi
Monitorizarea utilizării unităților amovibile
Modificarea duratei memorării în cache
Acțiuni cu dispozitive de încredere
Adăugarea unui dispozitiv la lista De încredere din interfața aplicației
Adăugarea unui dispozitiv la lista De încredere din Kaspersky Security Center
Exportul și importul listei de dispozitive de încredere
Obținerea accesului la un dispozitiv blocat
Modul online pentru acordarea accesului
Modul offline pentru acordarea accesului
Editarea șabloanelor mesajelor componentei Control dispozitive
Anti-Bridging
Activarea Anti-Bridging
Modificarea stării unei reguli de conectare
Modificarea priorității unei reguli de conectare
Control adaptiv al anomaliilor
Instruire componentă Control adaptiv al anomaliilor
Activarea și dezactivarea unei reguli Control adaptiv al anomaliilor
Modificarea acțiunii efectuate la declanșarea unei reguli Control adaptiv al anomaliilor
Crearea unei excluderi pentru o regulă Control adaptiv al anomaliilor
Exportarea și importarea de excluderi pentru reguli Control adaptiv al anomaliilor
Aplicarea de actualizări pentru reguli Control adaptiv al anomaliilor
Editarea șabloanelor de mesaje aferente componentei Control adaptiv al anomaliilor
Monitorizarea operațiunilor componentei Control adaptiv al anomaliilor

- Application Control
  - Limitări în funcționalitatea componentei Application Control
  - Primirea de informații despre aplicațiile instalate pe computerele utilizatorilor
  - Cum se activează modul Aplicații blocate
  - Application Control bazat pe un sistem de referință
  - Administrarea regulilor Application Control
    - Adăugarea unei condiții de declanșare pentru o regulă Application Control
    - Adăugarea fișierelor executabile din directorul Fișiere executabile în categoria de aplicații
    - Adăugarea fișierelor executabile asociate evenimentelor în categoria de aplicații
    - Adăugarea unei reguli Application Control
    - Modificarea stării unei reguli Application Control folosind Kaspersky Security Center
    - Exportul și importul regulilor Application Control
    - Vizualizarea evenimentelor rezultate din funcționarea componentei Application Control
    - Vizualizarea unui raport despre aplicațiile blocate
  - Testarea regulilor Application Control
    - Activarea și dezactivarea testării regulii Application Control
    - Vizualizarea unui raport despre aplicațiile blocate în modul de testare
    - Vizualizarea evenimentelor rezultate din testarea funcționării componentei Application Control
  - Monitorizare activitate aplicație
  - Reguli pentru crearea măștilor de nume pentru fișiere sau directoare
  - Editarea șabloanelor de mesaje aferente componentei Application Control
  - Variabile în șabloanele de mesaje pentru Application Control
  - Cele mai bune practici pentru implementarea unei liste de aplicații permise
    - Configurarea modului listă permise pentru aplicații
    - Testarea modului listă permise
    - Compatibilitate pentru modul listă permise
- Monitorizarea porturilor de rețea
  - Activarea monitorizării tuturor porturilor de rețea
  - Crearea unei liste de porturi de rețea monitorizate
  - Crearea unei liste de aplicații pentru care sunt monitorizate toate porturile de rețea
  - Exportul și importul listelor de porturi monitorizate
- Inspecție jurnal
  - Configurarea regulilor predefinite
  - Adăugarea de reguli personalizate
- Monitorizare integritate sistem
  - Despre regulile Monitorizare integritate sistem
  - Monitorizare în timp real a integrității sistemului
  - Componenta Verificare integritate sistem la cerere
  - Exportul și importul regulilor Monitorizare integritate sistem
  - Vizualizarea rapoartelor Monitorizare integritate sistem
  - Resetarea stării de integritate a sistemului
- Cloud Discovery

Zonă de încredere

- Crearea unei excluderi de la scanare
- Crearea unei excluderi după tipul obiectelor detectate
- Editarea listei de aplicații de încredere
- Crearea unei zone de încredere locale

- Exportul și importul zonei de încredere
- Gestionarea aplicațiilor cu o semnătură digitală de încredere
- Appendix. Excluderi de la scanare și aplicații de încredere predefinite
  - Server SQL
  - Server Microsoft Exchange
  - System Center Configuration Manager
  - Citrix
  - VMware
- Gestionarea copiilor de rezervă
  - Configurarea perioadei maxime de stocare pentru fișierele din Copie de rezervă
  - Configurarea dimensiunii maxime pentru Copie de rezervă
  - Restaurarea fișierelor din Copie de rezervă
  - Ștergerea copiilor de rezervă ale fișierelor din Copie de rezervă
- Serviciul de notificare
  - Configurarea setărilor pentru jurnalul de evenimente
  - Configurarea afișării și livrării notificărilor
  - Configurarea afișării avertizărilor despre starea aplicației în zona de notificare
  - Mesajele între utilizatori și administrator
- Gestionarea rapoartelor
  - Vizualizarea rapoartelor
  - Configurarea duratei maxime de stocare a rapoartelor
  - Configurarea dimensiunii maxime a fișierului raport
  - Salvarea unui raport într-un fișier
  - Golire rapoarte
- Autoprotecția aplicației Kaspersky Endpoint Security
  - Activarea și dezactivarea Autoprotecției
  - Activarea și dezactivarea suportului pentru AM-PPL
  - Protejarea serviciilor aplicației împotriva gestionării externe
  - Acceptarea aplicațiilor de administrare la distanță
  - Protecția prin parolă
    - Activarea protecției prin parolă
    - Acordarea de permisiuni utilizatorilor individuali sau grupurilor
    - Utilizarea unei parole temporare pentru acordarea de permisiuni
    - Revocarea parolei temporare
    - Aspecte speciale ale permisiunilor Protecție prin parolă
    - Resetarea parolei KLAdmin
  - Protecție conexiune la Serverul de administrare
- Data Encryption
  - Limitările funcționalității de criptare
  - Modificarea lungimii cheii de criptare (AES56/AES256)
  - Kaspersky Disk Encryption
    - Caracteristici speciale ale criptării unității SSD
    - Pornirea Kaspersky Disk Encryption
    - Crearea unei liste de unități de hard disk excluse de la criptare
    - Exportarea și importarea unei liste de unități de hard disk excluse de la criptare
    - Activarea tehnologiei Single Sign-On (SSO)
    - Gestionarea conturilor Agentului de Autentificare

- Folosirea unui simbol/card inteligent cu Agentul de Autentificare
- Decriptarea unităților de hard disk
- Restabilirea accesului la o unitate protejată de tehnologia Kaspersky Disk Encryption
- Conectarea cu ajutorul contul serviciului Agent de Autentificare
- Actualizarea sistemului de operare
- Eliminarea erorilor de actualizare a funcționalității de criptare
- Urmărirea Agentului de autentificare
- Editarea textelor de ajutor ale Agentului de Autentificare
- Eliminarea obiectelor și datelor rămase după testarea funcționării Agentului de Autentificare
- Gestionare Bitlocker
  - Pornirea BitLocker Drive Encryption
  - Decriptarea unei unități de hard disk protejată de BitLocker
  - Restaurare acces la o unitate de hard disk protejată cu BitLocker
  - Punerea în pauză a protecției BitLocker pentru actualizarea software-ului
- File Level Encryption pe unitățile locale ale computerului
  - Criptarea fișierelor de pe unitățile locale ale computerului
  - Crearea regulilor de acces la fișiere criptate pentru aplicații
  - Criptarea fișierelor create sau modificate de aplicații specifice
  - Generarea unei reguli de decriptare
  - Decriptarea fișierelor de pe unitățile locale ale computerului
  - Crearea pachetelor criptate
  - Restaurarea accesului la fișierele criptate
  - Restaurarea accesului la date criptate după o eroare de sistem
  - Editarea șabloanelor de mesaje pentru acces la fișiere criptate
- Criptare unități amovibile
  - Lansarea criptării unităților amovibile
  - Adăugarea unei reguli de criptare pentru unități amovibile
  - Exportul și importul unei liste de reguli de criptare pentru unitățile amovibile
  - Modul portabil pentru accesarea fișierelor criptate de pe unități amovibile
  - Decriptarea unităților amovibile
- Vizualizarea detaliilor de criptare date
  - Vizualizarea stării de criptare
  - Vizualizarea statisticilor de criptare pe tablourile de bord Kaspersky Security Center
  - Vizualizarea erorile de criptare fișiere pe unitățile locale ale computerului
  - Vizualizarea raportului de criptare a datelor
- Lucrul cu dispozitive criptate atunci când nu există acces la acestea
  - Recuperarea datelor utilizând Utilitarul de restaurare FDERT
  - Crearea unui disc de recuperare pentru sistemul de operare

Soluțiile Detection and Response

- Licențiere MDR și EDR Optimum
- Compatibilitatea cu soluțiile EDR terțe
- Kaspersky Endpoint Agent
  - Migrarea configurării [KES+KEA] la [KES+built-in agent]
  - Migrarea politicilor și activităților pentru Kaspersky Endpoint Agent
- Endpoint Detection and Response Agent (EDR Agent)
  - Instalarea EDR Agent
  - Integrarea EDR Agent cu MDR

- Integrarea EDR Agent cu EDR (KATA)
- Integrarea EDR Agent cu NDR (KATA)
- Integrarea EDR Agent cu EDR Expert (on-premises)
- Compatibilitatea cu aplicațiile EPP terțe

Managed Detection and Response

- Integrarea agentului încorporat cu MDR
- Ghid pentru migrarea KEA la KES pentru MDR

Endpoint Detection and Response

- Integrarea agentului încorporat cu EDR Optimum / EDR Expert
- Scanare pentru descoperirea indicatorilor de compromitere (activitate standard)
- Telemetrie extinsă pentru scanarea IOC
- Mută fișierul în Carantină
- Obținere fișier
- Ștergere fișiere
- Pornire proces
- Terminare proces
- Prevenirea executării
- Izolarea rețelei de calculatoare
- Cloud Sandbox
- Ghid pentru migrarea KEA la KES pentru EDR Optimum

Kaspersky Sandbox

- Integrarea agentului încorporat cu Kaspersky Sandbox
- Scanare pentru descoperirea indicatorilor de compromitere (activitate independentă)
- Ghid pentru migrarea KEA la KES pentru Kaspersky Sandbox

Kaspersky Anti Targeted Attack Platform

- Integrarea agentului încorporat cu EDR / NDR (KATA)
- Configurarea telemetriei EDR (KATA)
- Excluderi telemetrie EDR (KATA)
  - Exemplul 1. Procese excluse
  - Exemplul 2. Comunicații în rețea excluse
  - Exemplul 3. Operațiunile cu fișiere excluse
  - Exemplul 4. Modificările de registry excluse
- KATA Sandbox
  - Integrarea agentului încorporat cu KATA Sandbox
  - Configurarea acțiunilor Răspuns la amenințare
- Ghid de migrare KEA la KES pentru EDR (KATA)

Endpoint Detection and Response Expert (on-premises)

- Integrarea agentului încorporat cu EDR Expert (on-premises)
- Configurarea setărilor de telemetrie EDR Expert (on-premises)
- Excluderi telemetrie EDR Expert (on-premises)
- Exportarea și importarea filtrelor de evenimente EDR Expert (on-premises)
- Aspecte speciale la utilizarea profilurilor de politici pentru a configura integrarea cu EDR Expert (on-premises) și EDR (KATA)

Endpoint Detection and Response Expert (cloud)

- Integrarea agentului încorporat cu EDR Expert (cloud)
- Configurarea setărilor de telemetrie EDR Expert (cloud)

Excluderi telemetrie EDR Expert (cloud)
Exportarea și importarea filtrelor de evenimente EDR Expert (cloud)
Gestionarea carantinei
Configurarea dimensiunii maxime a Carantinei
Trimiterea datelor despre fișierele carantinate către Kaspersky Security Center
Restaurarea fișierelor din Carantină
Monitorizarea acțiunilor EDR
Kaspersky Unified Monitoring and Analysis Platform (KUMA)
Integrarea Kaspersky Endpoint Security cu KUMA
Filtrarea evenimentelor care urmează să fie trimise către KUMA
Exportarea și importarea filtrelor pentru evenimente KUMA
Ghid de migrare KSWS la KES
Corespondența dintre componentele KSWS și KES
Corespondența setărilor KSWS și KES
Migrarea componentelor KSWS
Migrarea activităților și politicilor KSWS
Migrarea zonei de încredere KSWS
Migrarea regulilor Control lansare aplicații KSWS
Instalarea KES în loc de KSWS
Migrarea configurării [KES+KEA] la [KES+agent încorporat]
Asigurați-vă că Kaspersky Security for Windows Server a fost eliminat cu succes
Activarea KES cu o cheie KSWS
Considerații speciale pentru migrarea serverelor cu încărcare mare
Gestionarea aplicației pe un server în modul Server Core
Migrarea de la [KSWS+KEA] la [KES+agent încorporat]
Modul Light Agent pentru protejarea mașinilor virtuale
Considerații speciale pentru modul Light Agent
Configurarea preliminară a mașinii virtuale
Compatibilitatea cu tehnologia Citrix App Layering
Compatibilitatea cu tehnologia Citrix Provisioning (Citrix Provisioning Services)
Compatibilitatea cu tehnologia Omnissa App Volumes
Instalarea Light Agent
Conectarea Light Agent la SVM
Descoperire SVM
Configurarea algoritmului de selectare a SVM pentru Light Agent
Distribuirea conexiunilor Light Agents la SVM-uri (etichete)
Protecția conexiunii dintre un Light Agent și SVM
Activarea Light Agent
Ghid de migrare de la KSVLA Light Agent la KES Light Agent
Instalarea KES Light Agent în loc de KSVLA Light Agent
Corespondența componentelor KSVLA Light Agent și KES Light Agent
Migrarea activităților și politicilor KSVLA Light Agent
Migrarea configurației [KSVLA Light Agent+KEA] la configurația [KES Light Agent+agent încorporat]
Gestionarea aplicației din linia de comandă
Setup. Instalarea aplicației
Setup /x. Eliminarea aplicației
msiexec /i. Recuperarea aplicației

Comenzi AVP
- SCAN. Scanare malware
- UPDATE. Actualizarea bazelor de date și modulelor aplicației
- ROLLBACK. Derulare înapoi ultima actualizare
- TRACES. Urmărirea
- START. Pornirea unui profil
- STOP. Oprirea unui profil
- STATUS. Starea profilului
- STATISTICS. Statistici de funcționare a profilului
- RESTORE. Restaurarea fișierelor din Copie de rezervă
- EXPORT. Exportarea setărilor aplicației
- IMPORT. Importarea setărilor aplicației
- ADDKEY. Aplicarea unui fișier cheie
- LICENSE. Licențiere
- RENEW. Achiziționarea unei licențe
- PBATESTRESET. Resetarea rezultatele verificării discului înainte de criptarea discului
- EXIT. Părăsirea aplicației
- EXITPOLICY. Dezactivarea politicii
- STARTPOLICY. Activarea politicii
- DISABLE. Dezactivarea protecției
- SPYWARE. Detectarea programelor spyware
- KSN. Comutarea între KSN / KPSN
- SERVERBINDINGDISABLE. Dezactivarea protecției conexiunii la server

Comenzi KESCLI
- Scan. Scanare malware
- GetScanState. Starea finalizării scanării
- GetLastScanTime. Determinarea orei finalizării scanării
- GetThreats. Obținerea datelor despe amenințările detectate
- UpdateDefinitions. Actualizarea bazelor de date și modulelor aplicației
- GetDefinitionState. Determinarea datei și orei ultimei actualizări a bazelor de date
- EnableRTP. Activarea protecției
- GetRealTimeProtectionState. Starea File Threat Protection
- GetEncryptionState. Starea criptării discului
- Version. Identificarea versiunii aplicației

Comenzi de gestionare Detection and Response
- SANDBOX. Gestionarea Sandbox
- PREVENTION. Gestionarea prevenirii executării
- ISOLATION. Gestionarea Izolării rețelei
- RESTORE. Restaurarea fișierelor din Carantină
- IOCSCAN. Scanare pentru descoperirea indicatorilor de compromitere (IOC)
- MDRLICENSE. Activare MDR
- EDRKATA. Integrarea cu EDR (KATA)
- KUMA. Integrare cu KUMA
- YARA. Se execută Scanarea YARA
- TELEMETRYFILTERS. Filtrarea evenimentelor care urmează să fie trimise către KUMA

Comenzi de gestionare a Light Agent
KSVLAINFO. Determinarea modului Light Agent
VIISINFO. Starea conexiunii Light Agent la Serverul de integrare
SVMINFO. Starea conexiunii Light Agent la Serverul de protecție
Coduri de eroare
Appendix. Profiluri de aplicații
Gestionarea aplicației prin API REST
Instalarea aplicației cu API REST
Lucrul cu API
Surse de informații despre aplicație
Contactarea Serviciului de asistență tehnică
Conținutul și zona de stocare pentru fișierele de urmărire
Urmărirea funcționării aplicațiilor
Urmărirea performanței aplicațiilor
Scrierea imaginilor
Protejarea fișierelor imagine și de urmărire
Obținerea datelor despre sistemul de operare (Kaspersky Get System Info)
Limitări și avertizări
Glosar
Activitate
Adresă normalizată pentru o resursă Web
Agent de Autentificare
Agent de rețea
Alarmă falsă
Arhivă
Autentificare Kerberos
Bază de date de adrese Web de phishing
Bază de date de adrese Web periculoase
Baze de date antivirus
Certificat licență
Cheie activă
Cloud Discovery
Dezinfectare
Domeniu de protecție
Domeniu de scanare
Emitent certificat
Fișier infectabil
Fișier infectat
Fișier IOC
Grup de administrare
IOC
Light Agent
Manager de fișiere portabil
Mască
Obiect OLE
OpenIOC
Server de integrare

SVM
Trusted Platform Module
Anexe
Anexa 1. Setări aplicație
File Threat Protection
Web Threat Protection
Mail Threat Protection
Network Threat Protection
Firewall
BadUSB Attack Prevention
Protecție AMSI
Exploit Prevention
Behavior Detection
Host Intrusion Prevention
Remediation Engine
Kaspersky Security Network
Inspecție jurnal
Anti-Cryptor
Control Web
Control dispozitive
Application Control
Control adaptiv al anomaliilor
Monitorizare integritate sistem
Endpoint Sensor
Sandbox
Managed Detection and Response
Endpoint Detection and Response
Endpoint Detection and Response Expert (on-premises)
Network Detection and Response (KATA)
Integrare cu KUMA
Full Disk Encryption
File Level Encryption
Criptare unități amovibile
Șabloane (criptarea datelor)
Excluderi
Setări aplicație
Rapoarte și spații de stocare
Setări de rețea
Interfață
Gestionare setări
Actualizarea bazelor de date și modulelor aplicației
Anexa 2. Grupurile de încredere pentru aplicații
Anexa 3. Extensii de fișiere pentru scanarea rapidă a unităților amovibile
Anexa 4. Tipuri de fișiere pentru filtrarea atașărilor Mail Threat Protection
Anexa 5. Setări de rețea pentru interacțiunea cu servicii externe

Anexa 6. Evenimente aplicație
Critică
Eroare funcțională
Avertisment
Mesaj de informare
Anexa 7. Extensii de fișiere acceptate pentru prevenirea executării
Anexa 8. Interpreți de script acceptați pentru Prevenirea executării
Anexa 9. Domeniu de scanare IOC în registru (RegistryItem)
Anexa 10. Cerințe privind fișierele IOC
Anexa 11. API pentru Răspunsul la amenințare EDR
Anexa 12. Conturi de utilizatori în regulile componentelor aplicației
Informații juridice
Furnizarea datelor
Furnizarea datelor conform Acordului de licență pentru utilizatorul final
Furnizarea datelor când folosiți Kaspersky Security Network
Furnizarea datelor atunci când se utilizează soluțiile Detection and Response
Kaspersky Endpoint Detection and Response
Kaspersky Sandbox
Kaspersky Endpoint Detection and Response Expert (on-premises)
Kaspersky Network Detection and Response (KATA)
Integrare cu Kaspersky Unified Monitoring and Analysis Platform (KUMA)
Respectarea legislației Uniunii Europene (GDPR)
Note privind mărcile comerciale
Informații despre codurile de la terți

Ajutor pentru Kaspersky Endpoint Security for Windows

Noutăți

Actualizare 14.1

Kaspersky Endpoint Security 14.1 for Windows conține următoarele caracteristici și îmbunătățiri:

1. A fost adăugat suport pentru sistemul de operare Windows Server 2025.

2. A fost crescută limita numărului de reguli de filtrare a evenimentelor de telemetrie pentru Expert în Endpoint Detection and Response (on-premises) și Kaspersky Endpoint Detection and Response Expert (cloud). Kaspersky Endpoint Security acceptă până la 10.000 de reguli de filtrare a evenimentelor de includere și excludere în total.

3. Acum poți configura ca activitățile să se execute doar în anumite zile ale săptămânii, la un interval specificat în săptămâni. Planificarea este disponibilă în Kaspersky Security Center 16.1 sau versiunile ulterioare.

4. Pentru activitatea *Scanare malware*, acum poți specifica un interval de timp în care activitatea va fi pusă în pauză, de exemplu, pentru a minimiza impactul asupra performanței computerului în perioadele de încărcare crescută.

5. Performanța subsistemului hard diskului de pe computerul protejat a fost optimizată prin reducerea numărului de operațiuni I/O.

6. La dezvoltarea acestei versiuni a Kaspersky Endpoint Security, am încorporat modificările incluse în următoarele corecții private: 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.

Actualizare 14.0

Kaspersky Endpoint Security 14.0 for Windows conține următoarele caracteristici și îmbunătățiri:

1. Calculatoarele bazate pe arhitectura ARM sunt acum acceptate. Puteți instala aplicația fie în modul standard, fie în modul EDR Agent. Totuși, aplicația are mai multe limitări (de exemplu, dintre tehnologiile de criptare a datelor, este acceptat doar BitLocker).

2. Auditul extins al politicilor este acceptat în Kaspersky Security Center Web Console versiunea 15.0 sau o versiune ulterioară. Acum puteți vizualiza revizuirile politicilor și să le salvați într-un fișier. O *revizuire* este un set de parametri modificați, salvați de utilizator. Revizuirile vă permit să comparați și să anulați modificările aduse parametrilor politicii.

3. Utilizatorii Kaspersky Endpoint Detection and Response au acum la dispoziție noi evenimente de telemetrie. Aceste noi evenimente îmbunătățesc capacitățile de detectare a amenințărilor ale soluțiilor Kaspersky EDR.

4. La dezvoltarea acestei versiuni a Kaspersky Endpoint Security for Windows, am încorporat modificările incluse în următoarele corecții private: 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.

Actualizare 12.12

Kaspersky Endpoint Security 12.12 for Windows conține următoarele caracteristici și îmbunătățiri:

1. Protecția directoarelor partajate împotriva criptării externe, care făcea parte din componenta Behavior Detection, este acum o componentă separată, numită Anti-Cryptor.

2. A fost adăugat suport pentru protocolul Kerberos pentru autentificarea aplicației prin intermediul unui server proxy pentru acces la Internet.

3. Acum poți specifica un hash de fișier pentru o aplicație de încredere și nu doar o cale completă.

4. Mai multe caracteristici ale activității *Scanare IOC* sunt disponibile utilizatorilor soluțiilor Endpoint Detection and Response (EDR). Funcționalitatea Scanare IOC retrospectivă este acum disponibilă. *Scanare IOC retrospectivă* este un mod al activității *Scanare IOC* în care Kaspersky Endpoint Security scanează pentru a descoperi indicatorii de compromitere utilizând datele pentru o anumită perioadă de timp. Acest mod este destinat detectării indicatorilor de compromitere din datele activității de rețea a computerului. Kaspersky Endpoint Security analizează datele din jurnalele sistemului de operare și jurnalele browserului de pe computer.

5. Utilizatorii Kaspersky Endpoint Detection and Response (EDR) pot elimina limita de dimensiune pentru carantină. Acest lucru poate fi necesar pentru scanarea YARA, deoarece aplicația poate salva un fișier de imagine de memorie mare. Acum poți folosi tot spațiul liber pe disc pentru carantină.

6. Compresia HTTPS este acum acceptată pentru optimizarea exportului evenimentelor către Kaspersky Unified Monitoring and Analysis Platform (KUMA). Acest lucru ajută la reducerea traficului de ieșire.

7. La dezvoltarea acestei versiuni a Kaspersky Endpoint Security for Windows, am încorporat modificările incluse în următoarele corecții private: 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.

Actualizare 12.11

Kaspersky Endpoint Security 12.11 for Windows oferă următoarele caracteristici și îmbunătățiri:

1. Aplicația verifică configurația componentelor de control înainte de a salva setările. Verificarea a fost adăugată pentru componentele Application Control, Device Control, System Integrity Monitoring. Aplicația afișează acum un avertisment dacă setările curente ale componentei de control pot crește încărcarea computerului sau pot cauza defecțiuni ale sistemului. De exemplu, în cazul componentei Application Control, dacă ai selectat modul care blochează toate aplicațiile, cu excepția celor permise, și nu ai adăugat nicio regulă de permitere, aplicația afișează un avertisment, deoarece o astfel de configurare poate cauza defecțiuni ale sistemului.

2. A fost adăugat suport pentru trimiterea automată a fișierelor către KATA Sandbox pentru revizuire. *KATA Sandbox* este o componentă a Kaspersky Anti Targeted Attack Platform care execută fișiere pe imagini virtuale ale sistemelor de operare. Sandbox analizează comportamentul obiectelor pentru a detecta activitatea rău intenționată și activitatea caracteristică atacurilor țintite asupra infrastructurii IT a organizației. Sandbox analizează și scanează obiecte de pe servere speciale cu imagini virtuale implementate ale sistemelor de operare Microsoft Windows (servere Sandbox). Pentru ca KATA Sandbox să funcționeze în modul automat, trebuie implementat Kaspersky Anti Targeted Attack Platform 8.0 sau o versiune ulterioară.

3. Trimiterea telemetriei EDR optimizate. Acum poți specifica lungimea maximă a pachetului.

4. Diagnosticare îmbunătățită a conexiunii la Kaspersky Security Network. Informații detaliate privind erorile de conectare pentru Kaspersky Security Network pentru a rezolva eventualele probleme.

5. A fost adăugat suport pentru configurarea listelor de evenimente care urmează să fie trimise către Kaspersky Unified Monitoring and Analysis Platform (KUMA). Acum, în plus față de listele de evenimente predefinite din KUMA, poți adăuga manual evenimente la telemetrie sau poți exclude evenimente după ID-ul lor din Jurnalul de evenimente Windows.

6. A fost actualizată interfața politicii în Web Console. Dispunerea secțiunilor politicii a fost modificată pentru un acces mai rapid la funcțiile esențiale.

7. Compatibilitate pentru Windows 11 25H2.

8. La dezvoltarea acestei versiuni a Kaspersky Endpoint Security for Windows, am încorporat modificările incluse în următoarele corecții private: 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.

Actualizare 12.10

Kaspersky Endpoint Security 12.10 for Windows oferă următoarele caracteristici și îmbunătățiri:

1. Pentru componenta BadUSB Attack Prevention, a fost adăugată opțiunea de autorizare a scanerelor de coduri de bare prin citirea unui cod de bare de pe ecran. Acum nu mai trebuie să introduci un cod folosind tastatura de pe ecran pentru a autoriza scanerele de coduri de bare.

2. Următoarele funcții și îmbunătățiri sunt disponibile pentru utilizatorii soluțiilor Endpoint Detection and Response (EDR) de la Kaspersky:

   - Acum poți gestiona funcția Izolare rețea a computerului în detaliile alertei. În plus, în detaliile alertei poți specifica perioada de timp pentru Izolare rețea a computerului și poți adăuga excluderi.

   - Completarea detaliilor alertei cu date noi. Acum, detaliile alertei conțin mai multe informații despre amenințare, inclusiv despre cum se comportă aplicația atunci când răspunde la amenințările EDR.

   - Procesarea fișierelor IOC a fost îmbunătățită. Acum poți vizualiza și edita conținutul fișierelor IOC în interfața Kaspersky Security Center Web Console. După încărcarea unui fișier IOC, aplicația afișează un raport despre aplicarea termenilor IOC.

   - Răspuns îmbunătățit la IOC-urile detectate. Acum poți carantina fișierele detectate de activitatea *Scanare IOC* direct în rezultatele detectării IOC din proprietățile activității. De asemenea, poți izola computerele din rețea în proprietățile activității.

   - Acum poți crea fișiere IOC direct în proprietățile activității *Scanare IOC* pe baza listelor de hash-uri de fișiere, adrese IP sau nume DNS generate într-un fișier TXT.

   - Domeniu de scanare extins pentru activitatea *Scanare IOC*. Acum poți defini un domeniu de aplicare pentru scanarea IOC a registry-ului (**Windows Registry – RegistryItem**). În versiunile anterioare ale aplicației, puteai utiliza doar un domeniu de aplicare pentru Scanare IOC predefinit în registry.

3. A fost adăugată o nouă permisiune pentru Protecție prin parolă, *Setări export*. În mod implicit, numai utilizatorul KLAdmin poate crea un fișier de configurare cu setările Kaspersky Endpoint Security în interfața aplicației. Pentru a acorda acces altor utilizatori, trebuie să le acorzi permisiunea corespunzătoare.

4. La dezvoltarea acestei versiuni a Kaspersky Endpoint Security for Windows, am încorporat modificările incluse în următoarele corecții private: 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.

Actualizare 12.9

Kaspersky Endpoint Security 12.9 for Windows oferă următoarele caracteristici și îmbunătățiri:

1. A fost adăugată o nouă funcționalitate pentru *gestionarea parolelor temporare*. Parola temporară îți permite să oferi acces la Kaspersky Endpoint Security cu funcția Protecție prin parolă activată pentru un computer separat. Gestionarea parolelor temporare permite salvarea istoricului parolelor (până la 30 de zile), monitorizarea stării parolelor temporare (*Activ*, *Expirat*, *Anulează*) și revocarea parolelor temporare.

2. A fost adăugată opțiunea de a întrerupe conexiunea la resursele web interzise de regulile componentei Control Web imediat după aplicarea politicii. În versiunile anterioare ale aplicației, componenta Control Web restricționa doar conexiunile noi la resursele web interzise.

3. Pentru utilizatorii Kaspersky Anti Targeted Attack Platform, a fost adăugată o opțiune de a executa verificarea YARA local pe computer. Pentru aceasta, trebuie să descarci un fișier cu regulile YARA și să execuți comanda în CMD.

4. S-a remediat comportamentul aplicației atunci când BitLocker este activat pe computerele pe care unitățile sunt deja protejate de BitLocker folosind instrumente terțe. Kaspersky Endpoint Security inițiază procedura de recuperare pentru a trimite cheia de recuperare către Kaspersky Security Center. Astfel, gestionarea componentei BitLocker este transferată în consola Kaspersky Security Center.

5. O nouă secțiune, și anume **Response history**, este disponibilă pentru utilizatorii soluțiilor Detection and Response de la Kaspersky. Această secțiune conține informații despre acțiunile de răspuns la amenințări efectuate pe computer. Astfel de acțiuni includ, de exemplu, rularea activității *Termină procesul* sau izolarea computerului față de rețea. Istoric răspunsuri este disponibilă numai pentru utilizatorii următoarelor soluții Kaspersky: MDR, EDR, KATA.

6. Pentru utilizatorii Kaspersky Unified Monitoring and Analysis Platform, suportul pentru acțiunile de răspuns la amenințări EDR este acum disponibil. Atunci când răspunde la amenințări, KUMA execută scripturi care creează activități EDR corespunzătoare. Pentru a executa acțiuni EDR, trebuie să creezi o regulă de răspuns pentru scriptul personalizat în consola KUMA și să selectezi evenimente.

7. La dezvoltarea acestei versiuni a Kaspersky Endpoint Security for Windows, am încorporat modificările incluse în următoarele corecții private: 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.

Actualizare 12.8

Kaspersky Endpoint Security 12.8 for Windows oferă următoarele caracteristici și îmbunătățiri:

1. Aplicația acceptă acum Modul Light Agent pentru protejarea mediilor virtuale. Acum poți implementa aplicația ca Light Agent ca parte a soluției Kaspersky Security for Virtualization Light Agent 6.2.

2. Interceptarea operațiunilor cu fișiere în containerele Docker pe servere este acum acceptată. Un *container* este un mediu izolat în care o aplicație se poate executa fără a interacționa direct cu sistemul de operare. Kaspersky Endpoint Security scanează fișierele din containerele la care utilizatorul obține acces. Când este detectată o amenințare, aplicațiile blochează această activitate rău intenționată și încearcă să dezinfecteze fișierul din interiorul containerului. Dacă fișierul nu poate fi dezinfectat, aplicația oprește containerul.

3. Acum poți defini un domeniu de protecție pentru protecția directoarelor partajate împotriva criptării externe (componenta Behavior Detection). Acum poți specifica directoarele partajate pe care aplicația trebuie să le monitorizeze pentru activitatea fișierelor. De asemenea, poți exclude fișiere din domeniul de protecție. În versiunile anterioare ale aplicației, componenta Behavior Detection a monitorizat toate directoarele partajate pentru activitatea fișierelor.

4. Acum poți configura diferite seturi de componente pentru diferite tipuri de sisteme de operare în pachetul de instalare. Adică, poți implementa aplicația pe stații de lucru și servere folosind același pachet de instalare. Componentele care nu sunt disponibile pentru un anumit tip de sistem de operare sunt excluse automat din proprietățile pachetului de instalare.

5. A fost adăugată opțiunea de selectare excluderi de la scanare predefinite și aplicații de încredere. Excluderile de la scanare predefinite și aplicațiile de încredere permit configurarea rapidă a zonei de încredere pentru aplicație într-un mediu virtual (Citrix, VMware). Astfel de excluderi includ, de exemplu, fișierele VHD și VHDX ale mașinilor virtuale. Excluderile pot fi adăugate în momentul creării unui pachet de instalare a aplicației, al creării unei politici sau la instalarea Kaspersky Endpoint Security.

6. Telemetria EDR include acum evenimente pentru operațiuni cu dispozitive conectate prin USB. De asemenea, poți adăuga aceste evenimente la excluderile din telemetria EDR.

7. A fost adăugată opțiunea de a bloca conexiunile de rețea prin protocolul TLS 1.0 învechit. TLS 1.0 are un nivel de securitate scăzut, de aceea este recomandat să dezactivezi acest protocol și să utilizezi versiunile mai noi TLS 1.2 sau TLS 1.3. În mod implicit, Kaspersky Endpoint Security blochează conexiunile TLS 1.0. După actualizarea versiunii aplicației, funcționarea serviciilor terțe care utilizează protocolul TLS 1.0 poate eșua. Pentru a evita problemele în funcționarea serviciilor de la terți, poți permite utilizarea protocolului TLS 1.0 în politica de grup înainte de a actualiza versiunea aplicației.

8. La dezvoltarea acestei versiuni a Kaspersky Endpoint Security for Windows, am încorporat modificările incluse în următoarele corecții private: 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.

Actualizare 12.7

Kaspersky Endpoint Security 12.7 for Windows oferă următoarele caracteristici și îmbunătățiri:

1. Acum poți limita utilizarea resurselor CPU pentru activitățile *Scanare malware*. Pentru a face acest lucru, în setările aplicației, specifică procentul maxim de încărcare a procesorului pentru toate nucleele care pot fi utilizate în timpul scanării computerului.

2. Acum poți să trimiteți fișiere pentru scanare în KATA Sandbox manual. *KATA Sandbox* este o componentă a Kaspersky Anti Targeted Attack Platform care execută fișiere pe imagini virtuale ale sistemelor de operare. Sandbox analizează comportamentul obiectelor pentru a detecta activitatea rău intenționată și activitatea caracteristică atacurilor țintite asupra infrastructurii IT a organizației. Sandbox analizează și scanează obiecte de pe servere speciale cu imagini virtuale implementate ale sistemelor de operare Microsoft Windows (servere Sandbox). Pentru a trimite un fișier pentru scanare către KATA Sandbox, selectează comanda relevantă din meniul contextual al fișierului.

3. Acum poți configura integrarea cu soluția care protejează LAN-ul corporativ, *Kaspersky Network Detection and Response*. Kaspersky Network Detection and Response (NDR) face parte din Kaspersky Anti Targeted Attack Platform. Poți configura interacțiunea cu NDR în modul standard, precum și în modul EDR Agent.

4. A fost adăugat suport pentru clientul de mail Microsoft Office Outlook versiunea 2021 la extensia Mail Threat Protection. Extensia permite scanarea mesajelor la nivelul unui client de e-mail și nu la nivelul protocolului. Pe lângă mesaje, extensia vă permite să scanați obiectele primite prin interfața MAPI din depozitele Microsoft Exchange (de exemplu, obiecte din Calendar). Această scanare are loc în clientul de e-mail.

5. La dezvoltarea acestei versiuni a Kaspersky Endpoint Security for Windows, am încorporat modificările incluse în următoarele corecții private: PF10049, PF10355, PF12114, PF13109, PF14056, PF15038, PF15045, PF16037, PF16042, PF16047, PF17014, PF17018, PF17021, PF17024, PF18006, PF18007.

Actualizare 12.6

Kaspersky Endpoint Security 12.6 for Windows oferă următoarele caracteristici și îmbunătățiri:

1. A fost adăugată funcționalitatea pentru integrarea cu soluția Kaspersky SIEM – *Kaspersky Unified Monitoring and Analysis Platform (KUMA).* Acum este posibil să trimiteți evenimente din jurnalele de evenimente Windows către colectorul KUMA. Acest lucru permite KUMA să primească evenimente Windows (este acceptat un set limitat de EventID-uri) de la toate computerele pe care este instalat Kaspersky Endpoint Security, fără a instala agenți KUMA pe aceste computere.

2. A fost adăugată o nouă componentă *Monitorizare integritate sistem* pentru a înlocui componenta File Integrity Monitor. Componenta Monitorizare integritate sistem include toate funcționalitățile File Integrity Monitor și, în plus, permite monitorizarea modificărilor registry-ului și conectarea dispozitivelor externe. Componenta Monitorizare integritate sistem monitorizează modificările din sistemul de operare care pot indica încălcări ale securității computerului. Când sunt detectate astfel de modificări, Kaspersky Endpoint Security generează evenimente corespunzătoare și alertează administratorul. File Integrity Monitor nu mai face parte din aplicație. Setările componentei File Integrity Monitor migrează automat la componenta Monitorizare integritate sistem atunci când actualizați aplicația. Pentru a asigura funcționarea corectă a componentei Monitorizare integritate sistem, atât aplicația Kaspersky Endpoint Security, cât și plug-in-ul de gestionare trebuie actualizate la versiunea 12.6.

3. Starea EDR Agent încorporat instalat (KATA) a fost adăugată la proprietățile computerului din consola Kaspersky Security Center. Acum, dacă aveți instalat un EDR Agent (KATA) încorporat, coloana **Stare Endpoint Sensor** afișează starea curentă a componentei (de exemplu, *Se execută*, *Oprit*, *Nu este acceptat de licență* etc.).

4. A fost adăugată opțiunea de selectare excluderi de la scanare predefinite și aplicații de încredere. Excluderile de la scanare și aplicațiile de încredere predefinite ajută la configurarea rapidă a zonei de încredere utilizând aplicația pe serverele SQL, serverele Microsoft Exchange și System Center Configuration Manager. Astfel de excluderi includ, de exemplu, fișierele de baze de date MDF și LDF. Excluderile pot fi adăugate în momentul creării unei noi politici, al modificării unei politici existente sau la instalarea Kaspersky Endpoint Security.

5. Afișarea detaliilor alertelor pentru Kaspersky Endpoint Detection and Response Optimum a fost mutată din plug-in-ul de gestionare Kaspersky Endpoint Security într-un plug-in de gestionare separat Kaspersky Endpoint Detection and Response. Pluginul de gestionare EDR este un plugin unic pentru lucrul cu agenți pe sistemele de operare Windows, Mac și Linux. Acum, când lucrați cu EDR Optimum, veți avea nevoie de plug-in-ul de gestionare Kaspersky Endpoint Security pentru a crea activități de răspuns la amenințări și de plug-in-ul de management EDR pentru a vizualiza detaliile alertelor.

6. Compatibilitate pentru Windows 11 24H2.

7. La dezvoltarea acestei versiuni de Kaspersky Endpoint Security for Windows, am încorporat modificările incluse în următoarele patch-uri private: pf10048, pf10353, pf12106, pf12107, pf12108, pf13090, pf13100, pf15031, pf15034, pf15036, pf16021, pf16023, pf16029, pf17002.

Actualizare 12.5

Kaspersky Endpoint Security 12.5 for Windows oferă următoarele caracteristici și îmbunătățiri:

1. A fost adăugată opțiunea de gestionare a excluderilor de telemetrie. *Telemetrie* este o listă de evenimente care au avut loc pe computerul protejat. Datele de telemetrie sunt folosite de Kaspersky Anti Targeted Attack Platform (EDR) pentru a monitoriza și proteja infrastructura IT a organizației. Configurarea excluderilor de telemetrie contribuie la îmbunătățirea performanței computerului și optimizarea transmiterii datelor către serverul de colectare a telemetriei.

2. Interfața zonei de încredere a aplicației a fost îmbunătățită. Kaspersky Endpoint Security ascunde acum obiectele din zona de încredere de utilizator dacă administratorul i-a interzis utilizatorului să adauge propriile excluderi de la scanare (locale) și aplicații de încredere. Acest lucru previne accesul neautorizat la zona de încredere de către un intrus, crescând nivelul de securitate al computerului.

3. A fost adăugată opțiunea de scanare a traficului pentru clienții de e-mail MyOffice Mail și R7-Office Organizer. Acum, componenta Mail Threat Protection scanează nu doar fișierele atașate la mesaje în momentul descărcării, ci și mesajele trimise și primite.

4. A fost adăugată o nouă categorie de resurse web *Instrumente de AI generativă*. Poți configura accesul la site-uri web din noua categorie, utilizând Control Web.

5. Acum poți selecta locația unei reguli pentru pachetele de rețea în lista Firewall. Locația unei reguli pentru pachetele de rețea în listă determină prioritatea acesteia. În versiunile anterioare ale aplicației, o nouă regulă putea fi adăugată doar la sfârșitul listei, după care trebuia să mutați manual regula prin listă pentru a o prioritiza. Acum, când adăugați o regulă, puteți alege dacă regula să fie plasată la începutul, la sfârșitul listei sau lângă regula selectată.

6. În regulile componentelor Kaspersky Endpoint Security, acum poți selecta utilizatori nu doar din Active Directory, ci și din lista de utilizatori din Kaspersky Security Center. De asemenea, poți introduce manual datele contului de utilizator local. Această posibilitate a fost adăugată pentru regulile următoarelor componente: Controlul aplicațiilor, Controlul dispozitivelor, Controlul web, Control adaptiv al anomaliilor și Inspecție jurnal.

7. Raportul de detectare a atacurilor de rețea include acum o coloană cu adresa MAC a computerului atacator (componenta Network Threat Protection). Acum puteți vedea adresa MAC a computerului atacator în raport, în plus față de adresa IP a acestuia. Acest lucru este util pentru investigarea incidentului. Rapoartele, care conțin adresa MAC a computerului atacator, vor fi disponibile și în consola Kaspersky Security Center Linux versiunea 15.1 și versiunile ulterioare.

8. A fost sporit nivelul cerințelor privind protecția computerului. Nivelul ridicat de protecție necesită acum activarea Protejarea serviciilor aplicației împotriva gestionării externe. Verifică indicatorul nivelului de securitate în partea de sus a ferestrei politicii. Dacă ai un nivel de securitate mediu sau scăzut, poți activa Protejarea serviciilor aplicației împotriva gestionării externe în fereastra de recomandare a indicatorului nivelului de securitate.

9. Suport pentru noi evenimente de detectare a obiectelor atunci când aplicația se execută în configurația Endpoint Detection and Response Agent (EDR Agent). a fost adaugată. Aceste evenimente au fost deja acceptate în configurația [KES+agent încorporat].

10. La dezvoltarea acestei versiuni a componentei Kaspersky Endpoint Security for Windows, am încorporat modificările incluse în următoarele corecții private: pf9640, pf9830, pf9831, pf10047, pf10351, pf12102, pf12105, pf13084, pf13089, pf14040, pf14047, pf15026, pf15028, pf16013.

Actualizare 12.4

Kaspersky Endpoint Security 12.4 for Windows oferă următoarele caracteristici și îmbunătățiri:

1. A fost adăugată o nouă funcționalitate pentru a proteja conexiunea computerului la Kaspersky Security Center. Noua activitate *Protecție conexiune Server de administrare* permite setarea unei parole pentru conectarea la un server de încredere. Aceasta înseamnă că nu este posibilă reconectarea computerului și executarea comenzilor de pe un alt server fără această parolă.

2. Pentru componenta Protecție prin parolă a fost adăugată posibilitatea de a selecta manual utilizatori nu doar din Active Directory. Adică, poți specifica manual un nume de utilizator și o parolă și poți atribui drepturi de acces la Kaspersky Endpoint Security pentru acest cont. Astfel, nu trebuie să partajezi parola KLAdmin cu alți utilizatori sau să creezi noi conturi Active Directory pentru a controla accesul la aplicație.

3. Compatibilitate pentru Windows 11 23H2.

Actualizare 12.3

Kaspersky Endpoint Security 12.3 for Windows oferă următoarele caracteristici și îmbunătățiri:

1. Acum puteți instala aplicația în configurația Endpoint Detection and Response Agent. Această configurație permite instalarea aplicației cu un set de componente solicitate de soluțiile Detection and Response de la Kaspersky: Kaspersky Managed Detection and Response și Kaspersky Anti Targeted Attack Platform (EDR). Puteți instala aplicația în această configurație alături de soluții terțe (de exemplu, Dr.Web, Dallas Lock, ESET). Acest lucru vă permite să utilizați instrumente de securitate ale infrastructurii terțe alături de Detection and Response de la Kaspersky.

2. Funcționarea Kaspersky Endpoint Security cu dispozitivele Bluetooth a fost îmbunătățită. Acum puteți configura excluderi și să restricționați accesul la toate dispozitivele Bluetooth, cu excepția dispozitivelor de intrare (tastaturi fără fir, mouse-uri etc.).

3. A fost optimizată funcționarea componentei Application Control cu baza de date a fișierelor executabile. Acum, Kaspersky Endpoint Security elimină automat informațiile despre fișier din baza de date dacă fieșierul este șters din computer. Acest lucru permite păstrarea bazei de date actualizată și economisirea resurselor Kaspersky Security Center.

4. A fost sporit nivelul cerințelor privind protecția computerului. Nivelul de protecție ridicat necesită acum activarea Protecției prin parolă. Verifică indicatorul nivelului de securitate din partea superioară a ferestrei politicii. Dacă ai un nivel mediu sau scăzut de protecție, poți activa funcția Protecție prin parolă în fereastra cu recomandări a indicatorului nivelului de protecție.

5. A fost adăugat suportul pentru protocolul HTTPS pentru a permite aplicației să funcționeze cu Kaspersky Security Network. Activați utilizarea HTTPS în proprietățile Serverului de administrare din setările serverului proxy KSN.

Actualizare 12.2

Kaspersky Endpoint Security 12.2 for Windows oferă următoarele caracteristici și îmbunătățiri:

1. A fost adăugat suport pentru protocolul WPA3 pentru a controla conexiunile la rețelele Wi-Fi (Control dispozitive). Acum puteți selecta protocolul WPA3 în setările rețelei Wi-Fi de încredere și să refuzați conexiunea la rețea folosind un protocol mai puțin sigur.

2. Acum puteți alege un protocol și porturi pentru excluderile Network Threat Protection. Acum, pe lângă specificarea adreselor IP ale dispozitivelor de încredere, puteți selecta și un port și un protocol. Acest lucru vă permite să excludeți fluxurile de date individuale și să preveniți atacurile de rețea de la adrese IP de încredere.

3. Ordine diferită a surselor de actualizare pentru *activitatea locală Actualizarea modulelor bazelor de date și ale aplicațiilor* dacă se aplică o politică computerului. Serverul Kaspersky Security Center este acum utilizat implicit ca primă sursă de actualizare în locul serverelor Kaspersky. Acest lucru ajută la economisirea traficului atunci când utilizatorul execută activitatea locală *Actualizarea modulelor bazelor de date și ale aplicațiilor*.

Actualizare 12.1

Kaspersky Endpoint Security 12.1 for Windows oferă următoarele caracteristici și îmbunătățiri:

1. A fost adăugat un agent încorporat pentru soluția Kaspersky Anti Targeted Attack Platform. Nu mai aveți nevoie de Kaspersky Endpoint Agent pentru a utiliza EDR (KATA). Toate funcțiile Kaspersky Endpoint Agent vor fi efectuate de Kaspersky Endpoint Security. Pentru a migra politicile Kaspersky Endpoint Agent, utilizați Expertul de migrare. După actualizarea aplicației, Kaspersky Endpoint Security comută la utilizarea agentului încorporat și elimină Kaspersky Endpoint Agent. Kaspersky Endpoint Agent a fost adăugat la lista de software-uri incompatibile. Kaspersky Endpoint Security are agenți încorporați pentru toate soluțiile Detection and Response, prin urmare, instalarea Kaspersky Endpoint Agent pentru a se integra cu soluțiile respective nu mai este necesară.

2. Modul de compatibilitate Azure WVD este acum acceptat. Această funcție asigură afișarea corectă a stării mașinii virtuale Azure în consola Kaspersky Anti Targeted Attack Platform. Modul de compatibilitate Azure WVD permite alocarea unui ID al senzorului unic permanent către aceste mașini virtuale.

3. Acum puteți configura accesul utilizatorilor la dispozitivele mobile în iTunes sau în aplicații similare. Adică, puteți, de exemplu, să permiteți ca dispozitivul mobil să fie utilizat numai în iTunes și să blocați utilizarea dispozitivului mobil ca unitate amovibilă. Aplicația acceptă, de asemenea, aceste reguli pentru aplicația Android Debug Bridge (ADB).

4. Kaspersky Security Center versiunea 11 nu mai este acceptată. Actualizați Kaspersky Security Center la cea mai recentă versiune.

Probleme rezolvate

Tabelul de mai jos listează toate problemele descoperite în versiunile anterioare ale Kaspersky Endpoint Security și remediate în versiunea curentă.

Lista problemelor remediate în versiunea 14.1

ID-ul problemei	Descrierea problemei
10140523	Activarea NVMe nativ în Windows 11 poate duce la un comportament instabil al aplicației.
9340076	Pe un dispozitiv cu aplicația instalată și componenta File Encryption activată, Windows Explorer nu reîmprospătează automat conținutul unui director de rețea după ce acesta este modificat de pe un alt dispozitiv.
9722863	Raportul Control dispozitive nu include evenimentul de deconectare a token-ului USB.
10006481	După aplicarea unei reguli care respinge traficul de intrare, conexiunile TCP active la servicii externe pot fi terminate prematur din cauza calculării incorecte a perioadei de expirare.
10140912	Aplicația nu detectează dispozitivul PDA BHT1100B.

ID-ul problemei	Descrierea problemei
10157563	Folder Redirection este posibil să nu funcționeze după o repornire pe stațiile de lucru VDI .
10158494	Controlul dispozitivelor înregistrează mai multe evenimente de conectare și deconectare a unui dispozitiv amovibil fără ca acesta să fie reconectat fizic.

Întrebări frecvente

GENERAL

Pe ce computere poate funcționa Kaspersky Endpoint Security?

Ce s-a schimbat de la ultima versiune?

Cu ce alte aplicații Kaspersky poate funcționa Kaspersky Endpoint Security?

Cum pot conserva resursele computerului în timpul funcționării Kaspersky Endpoint Security?

IMPLEMENTARE

Cum instalez Kaspersky Endpoint Security pe toate computerele unei organizații?

Ce setări de instalare pot fi configurate în linia de comandă?

Cum dezinstalez de la distanță Kaspersky Endpoint Security?

UPDATE

Ce metode sunt disponibile pentru actualizarea bazelor de date?

Ce ar trebui să fac dacă apar probleme după o actualizare?

Cum actualizez bazele de date în afara rețelei corporative?

Pot să utilizez un server proxy pentru actualizări?

SECURITATE

Cum scanează Kaspersky Endpoint Security e-mailul?

Cum exclud un fișier de încredere din scanări?

Cum protejez un computer împotriva virușilor de pe unitățile flash?

Cum pot executa o scanare malware care este ascunsă față de utilizator?

Cum întrerup temporar protecția Kaspersky Endpoint Security?

Cum pot restaura un fișier pe care Kaspersky Endpoint Security l-a șters în mod eronat?

Cum protejez Kaspersky Endpoint Security împotriva dezinstalării de către un utilizator?

INTERNET

Kaspersky Endpoint Security scanează conexiunile criptate (HTTPS)?

Cum permit utilizatorilor să se conecteze numai la rețelele Wi-Fi de încredere?

Cum blochez rețelele de socializare?

APLICAȚII

Cum aflu ce aplicații sunt instalate pe computerul unui utilizator (inventar)?

Cum pot preveni executarea jocurilor pe calculator?

Cum verific dacă componenta Application Control a fost configurată corect?

Cum adaug o aplicație în lista de încredere?

DISPOZITIVE

Cum pot bloca utilizarea unităților flash?

Cum adaug un dispozitiv la lista de încredere?

Este posibilă obținerea accesului la un dispozitiv blocat?

CRIPTARE

În ce condiții este imposibilă criptarea?

Cum folosesc o parolă pentru a restricționa accesul la o arhivă?

Este posibilă utilizarea cardurilor inteligente și simbolurilor cu criptarea?

Este posibil să obțin acces la datele criptate dacă nu există nicio conexiune cu Kaspersky Security Center?

Ce ar trebui să fac în cazul în care sistemul de operare al computerului eșuează, dar datele rămân criptate?

ASISTENȚĂ

Unde este stocat fișierul de raport?

Cum pot crea un fișier de urmărire?

Cum activez scrierea fișierelor imagine?

Kaspersky Endpoint Security for Windows

Kaspersky Endpoint Security for Windows (denumit în continuare Kaspersky Endpoint Security) asigură protecție completă împotriva diferitelor tipuri de amenințări, atacuri de rețea și atacuri de tip phishing.

Aplicația nu este destinată utilizării în procese tehnologice care implică sisteme automate de control. Pentru a proteja dispozitivele din astfel de sisteme, se recomandă utilizarea aplicației Kaspersky Industrial CyberSecurity for Nodes.

Tehnologii de detectare a amenințărilor



Învățare automată

Kaspersky Endpoint Security utilizează un model pentru tehnologia machine learning. Modelul a fost dezvoltat de experții Kaspersky. Ulterior, modelul este completat continuu cu date despred amenințări de la KSN (instruire model).



Analiză Cloud

Kaspersky Endpoint Security primește date despre amenințări de la Kaspersky Security Network. *Kaspersky Security Network (KSN)* este o infrastructură de servicii în cloud care oferă acces la Baza de cunoștințe online Kaspersky, care conține informații despre reputația fișierelor, a resurselor Web și a programelor software.



Analiză de specialitate

Kaspersky Endpoint Security utilizează datele despre amenințări adăugate de analiștii de viruși ai Kaspersky. Analiștii de viruși evaluează obiectele, dacă reputația unui obiect nu poate fi determinată automat.



Analiză comportamentală

Kaspersky Endpoint Security analizează activitatea unui obiect în timp real.



Analiză automată

Kaspersky Endpoint Security primește date de la un sistem automat de analiză a obiectelor. Sistemul procesează toate obiectele care sunt trimise către Kaspersky. Sistemul determină apoi reputația obiectului și adaugă datele la bazele de date antivirus. Dacă sistemul nu poate determina reputația obiectului, sistemul îi întreabă pe analiștii de viruși ai Kaspersky.



Sandbox

Kaspersky Endpoint Security procesează obiectul de pe o mașină virtuală. Kaspersky Sandbox analizează comportamentul obiectului și ia o decizie privind reputația acestuia. Această tehnologie este disponibilă doar dacă utilizați soluția Kaspersky Sandbox.



Cloud Sandbox

Kaspersky Endpoint Security scanează obiecte într-un mediu izolat oferit de Kaspersky. Tehnologia Cloud Sandbox este activată permanent și este disponibilă pentru toți utilizatorii Kaspersky Security Network, indiferent de tipul de licență pe care îl folosesc. Dacă ai instalat deja soluția Endpoint Detection and Response, poți activa un contor separat pentru amenințările detectate de Cloud Sandbox.

Arborele de selecție

Fiecare tip de amenințare este tratat de o componentă specială. Componentele pot fi activate sau dezactivate în mod individual, iar setările acestora pot fi configurate.

Arborele de selecție

Secțiune	Componentă
Essential Threat Protection	**File Threat Protection** Componenta File Threat Protection îți permite să previi infectarea sistemului de fișiere al unui computer. În mod implicit, componenta File Threat Protection se află permanent în memoria RAM a computerului și scanează în timp real toate fișierele deschise, salvate sau executate. Componenta scanează fișierele de pe toate unitățile computerului, inclusiv de pe unitățile conectate. Componenta oferă protecție computerului cu ajutorul bazelor de date antivirus, a serviciului cloud Kaspersky Security Network și a analizei euristice. **Web Threat Protection** Componenta Web Threat Protection previne descărcarea de pe Internet a fișierelor rău intenționate și, de asemenea, blochează site-urile web rău intenționate și de phishing. Componenta oferă protecție computerului cu ajutorul bazelor de date antivirus, a serviciului cloud Kaspersky Security Network și a analizei euristice. **Mail Threat Protection** Componenta Mail Threat Protection scanează atașările mesajelor de e-mail primite și trimise în vederea detectării virușilor și a altor amenințări. Componenta oferă protecție computerului cu ajutorul bazelor de date antivirus, a serviciului cloud Kaspersky Security Network și a analizei euristice. Mail Threat Protection poate scana atât mesajele primite, cât și cele trimise. Aplicația acceptă POP3, SMTP, IMAP și NNTP în următorii clienți de e-mail: • Microsoft Office Outlook • Mozilla Thunderbird • Windows Mail • MyOffice Mail • R7-Office Organizer Pentru a scana traficul în clienții de e-mail Mozilla Thunderbird, MyOffice Mail și R7-Office Organizer, trebuie să adaugi un certificat Kaspersky la magazinul de certificate și să selectezi propriul magazin de certificate. Mail Threat Protection nu acceptă alte protocoale și clienți de e-mail. Este posibil ca Mail Threat Protection să nu poată obține întotdeauna acces *la nivel de protocol* la mesaje (de exemplu, atunci când utilizați soluția Microsoft Exchange). Din acest motiv, Mail Threat Protection include o extensie pentru Microsoft Office Outlook. Extensia permite scanarea mesajelor la *nivelul clientului de mail*. Extensia Mail Threat Protection acceptă versiunile pe 32 de biți și pe 64 de biți ale Outlook 2010, 2013, 2016, 2019, 2021, 2024 și 365. Pe computerele bazate pe arhitectura Arm, extensia Mail Threat Protection acceptă versiunile pe 32 de biți și 64 de biți ale Outlook 2016, Outlook 2021, Outlook 2024 și Outlook 365 pentru Arm64. **Network Threat Protection** Componenta *Network Threat Protection* (numită și Intrusion Detection System, IDS) monitorizează traficul de rețea de intrare pentru activitatea caracteristică atacurilor de rețea. Când aplicația detectează o încercare de atac asupra rețelei pe computerul unui utilizator, aceasta blochează conexiunea la rețea cu respectivul computer atacator. Descrierile tipurilor de atacuri de rețea cunoscute în prezent și ale modurilor de combatere a acestora sunt furnizate în bazele de date ale aplicației. Lista de atacuri de rețea pe care le detectează componenta Network Threat Protection este actualizată în cursul actualizărilor bazelor de date și modulelor aplicației. **Firewall** Componenta Firewall blochează conexiunile neautorizate la un computer în timp ce lucrezi pe Internet sau într-o rețea locală. Firewall-ul controlează, de asemenea, activitatea de rețea a aplicațiilor de pe computer. Acest lucru vă permite să vă protejați rețeaua LANl corporativă împotriva furturilor de identitate și a altor atacuri. Componenta oferă protecție computerului cu ajutorul bazelor de date antivirus, a serviciului cloud Kaspersky Security Network și a *regulilor de rețea* predefinite. **BadUSB Attack Prevention** Componenta BadUSB Attack Prevention împiedică dispozitivele USB infectate care emulează o tastatură să se conecteze la computer. **Protecție AMSI** Componenta Protecție AMSI are rolul de a susține interfața Antimalware Scan Interface de la Microsoft. *Antimalware Scan Interface (AMSI)* permite aplicațiilor terțe cu suport AMSI să trimită obiecte (de exemplu, scripturi PowerShell) către Kaspersky Endpoint Security pentru scanare suplimentară și primește apoi rezultatele scanării pentru aceste obiecte.

Secțiune	Componentă
Advanced Threat Protection 	**Kaspersky Security Network** *Kaspersky Security Network (KSN)* este o infrastructură de servicii în cloud care oferă acces la Baza de cunoștințe online Kaspersky, care conține informații despre reputația fișierelor, a resurselor Web și a programelor software. Utilizarea datelor de la Kaspersky Security Network asigură răspunsul mai rapid prin Kaspersky Endpoint Security la noile amenințări, îmbunătățește eficiența unor componente ale protecției și reduce posibilitatea alarmelor false. Dacă participați la Kaspersky Security Network, serviciile KSN furnizează componentei Kaspersky Endpoint Security informații despre reputația adreselor web scanate, precum și informații despre categoria și reputația fișierelor scanate . **Behavior Detection** Componenta Behavior Detection primește date despre acțiunile aplicațiilor de pe computer și transmite aceste informații altor componente de protecție pentru a le îmbunătăți performanța. Componenta Behavior Detection utilizează Semnăturile de flux de comportamental (Behavior Stream Signatures, BSS) pentru aplicații. Dacă activitatea aplicației corespunde unei semnături de șir comportamental, Kaspersky Endpoint Security execută acțiunea de răspuns selectată. Funcționalitatea Kaspersky Endpoint Security se bazează pe semnături de flux comportamental și oferă o apărare proactivă pentru computer. Componenta Behavior Detection monitorizează suplimentar porturile de rețea pentru procese ale aplicațiilor care pot amenința securitatea computerului. Aplicația obține informații despre astfel de procese cu ajutorul bazelor de date antivirus. **Anti-Cryptor** Componenta Anti-Cryptor analizează activitatea din directoarele partajate. Dacă această activitate corespunde unei semnături de flux comportamental care este tipică pentru criptare externă, Kaspersky Endpoint Security execută acțiunea selectată. **Exploit Prevention** Componenta Exploit Prevention detectează codul programului care profită de vulnerabilitățile de pe un computer pentru a exploata privilegiile de administrator sau pentru a efectua activități dăunătoare. De exemplu, exploiturile pot utiliza un atac de supraîncărcare a memoriei tampon. Pentru a face acest lucru, exploitul trimite o cantitate mare de date unei aplicații vulnerabile. Atunci când prelucrează aceste date, aplicația vulnerabilă execută un cod rău intenționat. În urma acestui atac, exploitul poate porni instalarea neautorizată a unui program malware. Atunci când se încearcă executarea unui fișier executabil al unei aplicații vulnerabile care nu a fost efectuată de utilizator, Kaspersky Endpoint Security blochează executarea acestui fișier sau notifică utilizatorul. Componenta Exploit Prevention monitorizează suplimentar porturile de rețea pentru procese ale aplicațiilor care pot amenința securitatea computerului. Aplicația obține informații despre astfel de procese cu ajutorul bazelor de date antivirus. **Host Intrusion Prevention** Componenta Host Intrusion Prevention împiedică aplicațiile să execute acțiuni care ar putea fi periculoase pentru sistemul de operare și asigură controlul accesului la resursele sistemului de operare și la datele personale. Componenta oferă protecție computerului cu ajutorul bazelor de date antivirus și a serviciului cloud Kaspersky Security Network. **Remediation Engine** Componenta Remediation Engine permite Kaspersky Endpoint Security să deruleze înapoi acțiuni care au fost executate de către programe malware în sistemul de operare.
Security Controls 	**Application Control** Application Control administrează pornirea aplicațiilor pe computerele utilizatorilor. Acest lucru vă permite să implementați o politică de securitate corporativă atunci când utilizați aplicații. Application Control reduce, de asemenea, riscul de infectare a computerului prin restricționarea accesului la aplicații. **Control dispozitive** Componenta Control dispozitive gestionează accesul utilizatorilor la dispozitivele instalate pe sau conectate la un computer (de exemplu, hard diskuri, camere video sau module Wi-Fi). Acest lucru îți permite să protejezi computerul împotriva infectării atunci când sunt conectate astfel de dispozitive și să împiedici pierderea sau scurgerea datelor. **Control Web** Componenta Control Web gestionează accesul utilizatorilor la resursele web. Acest lucru ajută la reducerea traficului și la utilizarea necorespunzătoare a timpului de muncă. Când un utilizator încearcă să deschidă un site web care este restricționat de Control Web, Kaspersky Endpoint Security blochează accesul sau afișează un avertisment. **Control adaptiv al anomaliilor** Componenta Control adaptiv al anomaliilor monitorizează și blochează acțiunile care nu sunt specifice pentru computerele din rețeaua unei companii. Componenta Control adaptiv al anomaliilor utilizează un set de reguli pentru a urmări comportamentul atipic (de exemplu, regula *Pornire Microsoft PowerShell din aplicația Office*). Regulile sunt create de specialiștii Kaspersky pe baza scenariilor tipice de activitate periculoasă. Puteți configura modul în care componenta Control adaptiv al anomaliilor controlează fiecare regulă și, de exemplu, permite executarea scripturilor PowerShell care automatizează anumite activități ale fluxului de lucru. Kaspersky Endpoint Security actualizează setul de reguli împreună cu bazele de date ale aplicațiilor. **Inspecție jurnal** Componenta Inspecție jurnal monitorizează integritatea mediului protejat pe baza analizei jurnalului de evenimente Windows. Când aplicația detectează semne de comportament atipic în sistem, informează administratorul, deoarece acest comportament poate indica o tentativă de atac cibernetic. **Monitorizare integritate sistem** Componenta Monitorizare integritate sistem monitorizează modificările din sistemul de operare care pot indica încălcări ale securității computerului. Când sunt detectate astfel de modificări, Kaspersky Endpoint Security generează evenimente corespunzătoare și alertează administratorul.

Secțiune	Componentă
Activități 	**Scanare malware** Kaspersky Endpoint Security scanează computerul în căutarea virușilor și a altor amenințări. Scanarea malware ajută la excluderea posibilității de răspândire a programelor malware care nu au fost detectate de componentele de protecție, de exemplu din cauza unui nivel scăzut de securitate. **Actualizarea modulelor bazelor de date și ale aplicațiilor** Kaspersky Endpoint Security descarcă baze de date actualizate și module actualizate ale aplicației. Actualizarea vă păstrează computerul protejat împotriva celor mai noi viruși și a altor amenințări. Aplicația se actualizează automat în mod implicit, dar, dacă este necesar, poți actualiza manual bazele de date și modulele aplicației. **Derulare înapoi ultima actualizare** Kaspersky Endpoint Security derulează înapoi ultima actualizare a bazelor de date și a modulelor. Acest lucru îți permite să derulezi înapoi bazele de date și modulele de aplicații la versiunile lor anterioare atunci când este necesar, de exemplu când noua versiune de bază de date conține o semnătură nevalidă care determină Kaspersky Endpoint Security să blocheze o aplicație sigură. **Verificare integritate aplicație** Kaspersky Endpoint Security verifică modulele aplicației din directorul de instalare a aplicației pentru a vedea dacă sunt deteriorate sau modificate. Dacă un modul al aplicației are o semnătură digitală incorectă, modulul este considerat deteriorat.
Criptare date 	**File Level Encryption** Componenta permite crearea regulilor de criptare a fișierelor. Puteți selecta directoare predefinite pentru criptare, puteți selecta manual un director sau puteți selecta fișiere individuale după extensie. **Full Disk Encryption** Componenta permite criptarea unității de hard disc folosind Kaspersky Disk Encryption sau BitLocker Drive Encryption. **Criptare unități amovibile** Componenta permite protejarea datelor de pe unitățile amovibile. Puteți utiliza Full Disk Encryption (FDE) sau File Level Encryption (FLE).

Secțiune	Componentă
Detection and Response 	**Endpoint Detection and Response Optimum** Agent încorporat pentru soluția Kaspersky Endpoint Detection and Response Optimum (denumită în continuare „EDR Optimum"). *Kaspersky Endpoint Detection and Response* este o soluție pentru protejarea infrastructurii IT corporative împotriva amenințărilor cibernetice avansate. Funcționalitatea soluției combină detectarea automată a amenințărilor cu capacitatea de a reacționa la aceste amenințări pentru a contracara atacurile avansate, inclusiv exploatările, programele ransomware, atacurile fără fișiere noi, precum și metode care utilizează instrumente de sistem legitime. Pentru mai multe informații despre soluție, consultați Ajutorul Kaspersky Endpoint Detection and Response Optimum. **Endpoint Detection and Response Expert** Agent încorporat pentru soluția Kaspersky Endpoint Detection and Response Expert (denumită în continuare „EDR Expert"). EDR Expert oferă o funcționalitate mai bună de monitorizare și răspuns decât EDR Optimum. Pentru mai multe informații despre soluție, consultați Ajutorul Kaspersky Endpoint Detection and Response Expert. **Endpoint Detection and Response Expert (on-premises)** și **Network Detection and Response (KATA)** Agenți încorporați pentru gestionarea componentelor Endpoint Detection and Response și Network Detection and Response care fac parte din soluția Kaspersky Anti Targeted Attack Platform. *Kaspersky Anti Targeted Attack Platform* este o soluție concepută pentru detectarea în timp util a amenințărilor sofisticate, cum ar fi atacuri direcționate, amenințări persistente avansate (APT), atacuri zero-day și altele. Kaspersky Anti Targeted Attack Platform include trei unități funcționale: • Kaspersky Anti Targeted Attack Platform (*KATA*) • Kaspersky Endpoint Detection and Response (*EDR (KATA)*) • Network Detection and Response (*NDR (KATA)*) Poți achiziționa separat toate unitățile funcționale sau unitățile funcționale individuale. Pentru informații detaliate despre soluție, consultați Ajutor pentru Kaspersky Anti Targeted Attack Platform. **Sandbox** Agent încorporat pentru Sandbox. Componenta *Sandbox* detectează și blochează automat amenințările avansate de pe computere. Sandbox analizează comportamentul obiectelor pentru a detecta activitatea rău intenționată și activitatea caracteristică atacurilor țintite asupra infrastructurii IT a organizației. Sandbox analizează și scanează obiecte de pe servere speciale cu imagini virtuale implementate ale sistemelor de operare Microsoft Windows (servere Sandbox). Pentru informații detaliate despre soluție, consultați Ajutor pentru Kaspersky Sandbox și Ajutor pentru Kaspersky Anti Targeted Attack Platform. **Managed Detection and Response** Agent încorporat pentru a sprijini funcționarea soluției Kaspersky Managed Detection and Response. Soluția *Kaspersky Managed Detection and Response (MDR)* detectează și analizează automat incidentele de securitate din infrastructura dvs. Pentru aceasta, MDR folosește date de telemetrie primite de la puncte finale și învățarea programată. MDR trimite datele incidentelor către experții Kaspersky. Experții pot procesa apoi incidentul și, de exemplu, pot adăuga o nouă intrare în bazele de date antivirus. Alternativ, experții pot emite recomandări privind procesarea incidentului și, de exemplu, pot sugera izolarea computerului de rețea. Pentru informații detaliate despre modul în care funcționează soluțiile, consultați pagina Ajutor Kaspersky Managed Detection and Response.

Moduri ale aplicației: Standard, EDR Agent, Light Agent

Kaspersky Endpoint Security for Windows face parte din multe soluții Kaspersky. În funcție de soluție, trebuie să selectezi un mod pentru aplicație.



Modul standard

Acesta este modul principal și implicit al aplicației. Poți instala aplicația în acest mod ca parte a Kaspersky soluțiilor EPP (Endpoint Protection Platform). De exemplu, Kaspersky Endpoint Security în modul Standard face parte din Kaspersky Endpoint Security for Business. Kaspersky Endpoint Security oferă o protecție completă a stațiilor de lucru și a serverelor împotriva diferitelor amenințări, atacuri de rețea și escrocherii. În modul standard, agenții încorporați sunt disponibili și pentru integrare cu soluțiile Kaspersky Detection and Response, inclusiv EDR, MDR, KUMA și altele.



EDR Agent

Acest mod permite implementarea soluțiilor Kaspersky Detection and Response împreună cu soluții EPP terțe. Soluțiile Detection and Response includ Kaspersky Managed Detection and Response (MDR) și Kaspersky Anti Targeted Attack Platform (KATA). EDR Agent acceptă și soluția Kaspersky SIEM, Kaspersky Unified Monitoring and Analysis Platform (KUMA).

În acest mod, componentele standard de protecție, cum ar fi File Threat Protection sau Web Threat Protection, nu sunt disponibile. Protecția standard a computerului este asigurată de soluția EPP terță. Agentul EDR monitorizează continuu procesele care se execută pe aceste computere, conexiunile de rețea deschise și fișierele care sunt modificate și interacționează cu soluțiile Detection and Response.



Light Agent

Acest mod este folosit pentru a proteja mediile virtuale. Kaspersky Endpoint Security în modul Light Agent face parte din soluția Kaspersky Hybrid Cloud Security. Light Agent protejează mașinile virtuale cu sisteme de operare invitate pentru stații de lucru și servere. Aceleași componente de protecție și control sunt disponibile în acest mod ca și în modul Standard. Diferența este că obiectele sunt scanate pentru viruși și alte programe malware de o componentă specială a soluției instalată pe o mașină virtuală separată, SVM (Secure Virtual Machine). Astfel, Light Agent folosește resursele SVM pentru a asigura securitatea infrastructurii în locul resurselor mașinii virtuale.

Kitul de distribuire

Kitul de distribuire include următoarele pachete de distribuire:

- **AES256**

  Acest pachet de distribuție este destinat instalării pe computere cu arhitectură x86/x64. Acest pachet de distribuire conține instrumente criptografice care implementează algoritmul de criptare AES (Advanced Encryption Standard) cu o lungime efectivă a cheii de 256 de biți.

- **AES56**

  Acest pachet de distribuție este destinat instalării pe computere cu arhitectură x86/x64. Acest pachet de distribuire conține instrumente criptografice care implementează algoritmul de criptare AES cu o lungime efectivă a cheii de 56 de biți.

- **Arm64**

  Acest pachet de distribuție este destinat instalării pe computere bazate pe arhitectura Arm. Acest pachet de distribuție nu este destinat instalării pe servere.

Înainte de instalare, asigură-te că pachetul de distribuție se potrivește cu arhitectura procesorului. Dacă pachetul de distribuție nu corespunde arhitecturii procesorului, programul de instalare va termina instalarea cu o eroare.

Pachetul de distribuție este o arhivă cu dezarhivare automată în format EXE. Pentru a vizualiza conținutul pachetului de distribuție, trebuie să dezarhivezi arhiva într-un director separat. Fiecare pachet de distribuire conține următoarele fișiere:

`kes_win.msi`	Pachetul de instalare pentru Kaspersky Endpoint Security.
`setup_kes.exe`	Fișierele necesare pentru instalarea aplicației folosindu-se oricare dintre metodele disponibile.
`kes_win.kud`	Fișier pentru crearea de pachete de instalare pentru Kaspersky Endpoint Security.
`klcfginst.msi`	Pachet de instalare pentru plug-in-ul de gestionare a aplicației în Kaspersky Security Center Administration Console.
`bases.cab`	Fișiere ale pachetului de actualizare utilizate în timpul instalării.
`cleaner_v2.cab` `cleanerapi_v2.cab`	Fișiere pentru eliminarea software-urilor incompatibile.
`incompatible.txt`	Fișier care conține lista software-urilor care pot cauza probleme de compatibilitate cu Kaspersky Endpoint Security. Kaspersky nu garantează compatibilitatea aplicației Kaspersky Endpoint Security cu software-ul din listă.
`ksn_<language ID>.txt`	Fișier în care puteți citi condițiile de participare la Kaspersky Security Network.
`license.txt`	Fișier unde poți citi Acordul de licență pentru utilizatorul final și Politica privind confidențialitatea.
`installer.ini`	Fișier care conține setările interne ale kitului de distribuire.
`kes.cab`	Fișiere pentru interfața grafică a aplicației.
`aes256.cab` / `aes56.cab`	Fișiere pentru algoritmul criptografic AES (nu sunt incluse în pachetul de distribuție Arm64).
`package.kcat`	Fișierul cu semnăturile kitului de distribuire a aplicației. Semnătura digitală garantează autenticitatea și integritatea kitului de distribuire a aplicației.

Nu se recomandă modificarea acestor setări. Dacă dorești să modifici opțiunile de instalare, folosește fișierul setup.ini.

Cerințe hardware și software

Acest articol listează versiunile de software pe care a fost testată aplicația și pentru care este garantată funcționarea corectă. Aplicația poate funcționa și cu alte versiuni de software, dar aceste configurații nu au trecut printr-un ciclu complet de testare și nu sunt incluse în lista de versiuni cu suport garantat.

Pentru a se asigura funcționarea corectă a aplicației Kaspersky Endpoint Security, computerul trebuie să îndeplinească următoarele cerințe:

Pentru a instala aplicația, aveți nevoie de drepturi de administrator pe computer.

Cerințe minime generale

Cerințe minime	Stație de lucru (x86/x64)	Server (x86/x64)	Arm
Spațiu de stocare	2 GB	2 GB	2 GB
Procesor	Suport pentru instrucțiunile SSE2, 1 GHz	Suport pentru instrucțiunile SSE2, 1,4 GHz	1 GHz, arhitectură Armv8.1
RAM	Stație de lucru (x86): 1 GB Stație de lucru (x64): 2 GB	2 GB Notă: Serverul necesită 8 GB de memorie pentru a instala aplicația cu agentul integrat destinat integrării cu Kaspersky Anti Targeted Attack Platform.	4 GB
Microsoft .NET Framework	4 sau o versiune ulterioară	4 sau o versiune ulterioară	4,8 sau o versiune ulterioară

Stații de lucru

Sisteme de operare acceptate pentru stații de lucru:

- 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-session
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise
- Windows 11 for Arm64 Home / Pro / Pro for Workstations / Education / Enterprise

Sistemele de operare Windows, începând cu versiunea 11 24H2, acceptă tehnologia UDP Receive Segment Coalescing Offload (URO). Tehnologia este activată în mod implicit dacă pe computer sunt instalate o placă de rețea și drivere compatibile. Dezactivarea URO pe computerul unui utilizator poate reduce semnificativ performanța aplicației.

Pentru a se garanta funcționarea corectă a Kaspersky Endpoint Security, serviciul Windows Security Center (wscsvc) trebuie să se execute pe computerul utilizatorului.

Kaspersky Endpoint Security nu poate fi instalat pe Microsoft Windows 7 fără ca actualizările sistemului de operare să fie instalate: KB4490628 (12 martie 2019) și KB4474419 (23 septembrie 2019). Pentru informații detaliate, consultați Baza de cunoștințe pentru suport tehnic.

Pentru detalii referitoare la suportul pentru sistemul de operare Microsoft Windows 10, consultați Baza de cunoștințe a Serviciului de asistență tehnică.

Pentru detalii referitoare la suportul pentru sistemul de operare Microsoft Windows 11, consultați Baza de cunoștințe a Serviciului de asistență tehnică.

Servere

Kaspersky Endpoint Security acceptă componentele principale ale aplicației pe computerele pe care se execută sisteme de operare Windows pentru servere. Poți utiliza Kaspersky Endpoint Security for Windows în loc de Kaspersky Security for Windows Server pe serverele și clusterele organizației tale (Cluster Mode). Aplicația acceptă, de asemenea, Server Core Mode (vezi problemele cunoscute).

Sisteme de operare acceptate pentru servere:

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

  Microsoft Small Business Server 2011 Standard (64 de biți) este acceptat numai dacă este instalat Service Pack 1 pentru Microsoft Windows Server 2008 R2.

- Windows MultiPoint Server 2011 (64 de biți);
- 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 (inclusiv modul Server Core);
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (inclusiv modul Server Core);
- Windows Server 2016 Essentials / Standard / Datacenter (inclusiv modul Server Core);
- Windows Server 2019 Essentials / Standard / Datacenter (inclusiv modul Server Core);
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (inclusiv modul Server Core);
- Windows Server 2025 Standard / Datacenter.

Kaspersky Endpoint Security nu poate fi instalat pe Microsoft Windows Server 2008 R2 fără ca actualizările sistemului de operare să fie instalate: KB4490628 (12 martie 2019) și KB4474419 (23 septembrie 2019).

Pentru informații detaliate despre asistența pentru sistemele de operare Microsoft Windows Server 2016 și Microsoft Windows Server 2019, consultați Baza de cunoștințe a Serviciului de asistență tehnică.

Pentru detalii referitoare la suportul pentru sistemul de operare Microsoft Windows Server 2022, consultați Baza de cunoștințe a suportului tehnic.

Sisteme de operare neacceptate pentru servere:

- 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

Platforme virtuale

Platforme virtuale acceptate pentru funcționarea aplicațiilor în modul standard:

- 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.

Aplicația acceptă mașini virtuale care execută Windows 11 Pro Arm64 create cu ajutorul Hyper-V.

Mașini virtuale pentru instalarea Light Agent

Instalarea Kaspersky Endpoint Security în modul Light Agent pe mașinile virtuale bazate pe arhitectura ARM nu este acceptată.

BIOS-ul mașinilor virtuale trebuie să accepte specificația SMBIOS versiunea 2.1 sau o versiune ulterioară.

Următoarele pachete și utilitare trebuie instalate pe mașinile virtuale:

- Când utilizezi Microsoft Hyper-V – pachetul de coponente de integrare.
- Când utilizezi VMware vSphere – pachetul VMware Tools.
- Când utilizezi XenServer – pachetul XenTools.
- Când utilizezi pachetul HUAWEI FusionSphere – HUAWEI Tools.
- Când se utilizează hipervizori bazați pe KVM – QEMU Guest Agent.

Consultă Ajutor pentru Kaspersky Security for Virtualization Light Agent pentru a vedea cerințele infrastructurii virtuale, în vederea executării aplicației în modul Light Agent.

Pentru ca aplicația să funcționeze corect, utilizează o interfață de rețea virtualizată cu o lățime de bandă de cel puțin 100 Mbit/s.

Servere terminale

Tipuri de terminale de server acceptate:

- Microsoft Remote Desktop Services bazat pe Windows Server 2008 R2 SP1;
- Microsoft Remote Desktop Services bazat pe Windows Server 2012.
- Microsoft Remote Desktop Services bazat pe Windows Server 2012 R2;
- Microsoft Remote Desktop Services bazat pe Windows Server 2016.
- Microsoft Remote Desktop Services bazat pe Windows Server 2019.
- Microsoft Remote Desktop Services bazat pe Windows Server 2022.
- Microsoft Remote Desktop Services bazat pe Windows Server 2025.
- Citrix RDSH de la Citrix Virtual Apps and Desktops 7 2507 LTSR

Suport Kaspersky Security Center

Kaspersky Endpoint Security acceptă funcționarea cu următoarele versiuni ale 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

Compararea caracteristicilor disponibile ale aplicațiilor, în funcție de tipul de sistem de operare

Setul de caracteristici disponibile ale aplicației Kaspersky Endpoint Security depinde de tipul sistemului de operare: stație de lucru sau server (consultați tabelul de mai jos).

Începând cu Kaspersky Endpoint Security12.8 for Windows, poți configura diferite seturi de componente pentru diferite tipuri de sisteme de operare în pachetul de instalare. Adică, poți implementa aplicația pe stații de lucru și servere folosind același pachet de instalare.

Instalarea Kaspersky Endpoint Security în modul Light Agent pe mașinile virtuale bazate pe arhitectura ARM nu este acceptată.

Comparație a caracteristicilor aplicației Kaspersky Endpoint Security

Caracteristică	Stație de lucru	Stație de lucru bazată pe arhitectura ARM	Server	Modul Server Core
Advanced Threat Protection				
Kaspersky Security Network	✓	✓	✓	✓
Behavior Detection	✓	✓	✓	✓
Anti-Cryptor	✓	✓	✓	✓
Exploit Prevention	✓	✓	✓	✓
Host Intrusion Prevention	✓	✓	–	–
Remediation Engine	✓	✓	✓	✓
Essential Threat Protection				
File Threat Protection	✓	✓	✓	✓
Web Threat Protection	✓	✓	✓	–
Mail Threat Protection	✓	✓	✓	–
Firewall	✓	✓	✓	✓
Network Threat Protection	✓	✓	✓	✓
BadUSB Attack Prevention	✓	✓	✓	–
Protecție AMSI	✓	✓	✓	✓
Security Controls				
Inspecție jurnal	–	–	✓	–
Application Control	✓	✓	✓	✓
Control dispozitive	✓	✓	✓	✓
Control Web	✓	✓	✓	–
Control adaptiv al anomaliilor	✓	✓	–	–
Monitorizare integritate sistem	–	–	✓	–
Cloud Discovery	✓	✓	–	–

Caracteristică	Stație de lucru	Stație de lucru bazată pe arhitectura ARM	Server	Modul Server Core
Criptare date				
Kaspersky Disk Encryption	✓	–	–	–
BitLocker Drive Encryption	✓	✓	✓	✓
File Level Encryption	✓	–	–	–
Criptare unități amovibile	✓	–	–	–
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)	✓	✓	✓	✓
Integrare KUMA	✓	✓	✓	✓

Compararea funcțiilor aplicației în funcție de instrumentele de gestionare

Setul de funcții disponibil în Kaspersky Endpoint Security depinde de instrumentele de gestionare (consultați tabelul de mai jos).

Puteți gestiona aplicația folosind următoarele console ale Kaspersky Security Center:

- Consola de administrare. Utilitarul de completare snap-in pentru Microsoft Management Console (MMC) a fost instalat pe stația de lucru a administratorului.
- Web Console. Componenta Kaspersky Security Center care este instalată pe Serverul de administrare. Puteți lucra în Web Console printr-un browser, de pe orice computer care are acces la Serverul de administrare.

De asemenea, puteți gestiona aplicația folosind Kaspersky Security Center Cloud Console. *Kaspersky Security Center Cloud Console* este versiunea cloud a Kaspersky Security Center. Aceasta înseamnă că serverul de administrare și alte componente ale Kaspersky Security Center sunt instalate în infrastructura cloud a Kaspersky. Pentru detalii privind administrarea aplicației utilizând Kaspersky Security Center Cloud Console, consultați Ajutor pentru Kaspersky Security Center Cloud Console.

Kaspersky Endpoint Security face parte din soluția Kaspersky Next Pro View. Pentru mai multe informații despre caracteristicile aplicației disponibile atunci când funcționează ca parte a acestei soluții, consultă Ajutor Kaspersky Next.

Comparație a caracteristicilor aplicației Kaspersky Endpoint Security

Caracteristică	Kaspersky Security Center		Kaspersky Security Center
	Consola de administrare	Web Console	Cloud Console
Advanced Threat Protection			
Kaspersky Security Network	✓	✓	✓
Kaspersky Private Security Network	✓	✓	–

Caracteristică	Kaspersky Security Center		Kaspersky Security Center
	Consola de administrare	Web Console	Cloud Console
Behavior Detection	✓	✓	✓
Anti-Cryptor			
Exploit Prevention	✓	✓	✓
Host Intrusion Prevention	✓	✓	✓
Remediation Engine	✓	✓	✓
Essential Threat Protection			
File Threat Protection	✓	✓	✓
Web Threat Protection	✓	✓	✓
Mail Threat Protection	✓	✓	✓
Firewall	✓	✓	✓
Network Threat Protection	✓	✓	✓
BadUSB Attack Prevention	✓	✓	✓
Protecție AMSI	✓	✓	✓
Security Controls			
Inspecție jurnal	✓	✓	✓
Application Control	✓	✓	✓
Control dispozitive	✓	✓	✓
Control Web	✓	✓	✓
Control adaptiv al anomaliilor	✓	✓	✓
Monitorizare integritate sistem	✓	✓	✓
Cloud Discovery	–	–	✓
Criptare date			
Kaspersky Disk Encryption	✓	✓	–
BitLocker Drive Encryption	✓	✓	✓
File Level Encryption	✓	✓	–
Criptare unități amovibile	✓	✓	–
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)	✓	✓	✓
Integrare KUMA	✓	✓	✓
Activități			
Adaugă cheie	✓	✓	✓
Modificare componente ale aplicației	✓	✓	✓
Inventar	✓	✓	✓
Actualizare	✓	✓	✓
Derulare înapoi actualizare	✓	✓	✓

Caracteristică	Kaspersky Security Center		Kaspersky Security Center
	Consola de administrare	Web Console	Cloud Console
Scanare malware	✓	✓	✓
Verificare integritate aplicație	✓	✓	–
Șterge datele	✓	✓	✓
Gestionare conturi Agent de Autentificare (Kaspersky Disk Encryption)	✓	✓	–
Scanare IOC (EDR)	–	✓	✓
Mută fișierul în Carantină (EDR)	–	✓	✓
Obținere fișier (EDR)	–	✓	✓
Șterge fișier (EDR)	–	✓	✓
Pornește procesul (EDR)	–	✓	✓
Termină proces (EDR)	–	✓	✓

Compatibilitatea cu alte aplicații

Kaspersky Endpoint Security este incompatibil cu unele aplicații Kaspersky, precum și cu unele aplicații terțe. Prin urmare, înainte de instalare, actualizarea versiunii aplicației și modificarea componentelor aplicației, Kaspersky Endpoint Security scanează computerul pentru a vedea dacă există astfel de aplicații.

Compatibilitatea cu aplicațiile terțe

Kaspersky Endpoint Security este incompatibil cu aplicațiile care fac parte din sistemele de protecție a terminalelor terțe (Endpoint Protection Platform, EPP). Kaspersky Endpoint Security poate întâmpina și probleme de compatibilitate cu alte aplicații. Pentru a determina compatibilitatea, Kaspersky Endpoint Security consultă o listă de software-uri întocmită de Kaspersky. Această listă este încorporată în fișierul incompatible.txt. Acest fișier este inclus în kitul de distribuție.

Kaspersky nu garantează compatibilitatea aplicației Kaspersky Endpoint Security cu software-ul din listă. Dacă este descoperită o aplicație din listă, programul de instalare oprește implementarea componentei Kaspersky Endpoint Security. Programul de instalare poate șterge automat unele aplicații din listă. Dacă ești dispus să ignori riscurile și dorești să instalezi Kaspersky Endpoint Security și un program din listă pe același computer, poți sări peste verificarea computerului (consultă instrucțiunile de mai jos).

DESCARCĂ FIȘIERUL INCOMPATIBLE.TXT

Compatibilitatea cu aplicații de la Kaspersky

Aplicația Kaspersky Endpoint Security este incompatibilă cu următoarele aplicații Kaspersky:

- 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 ca parte a Kaspersky Anti Targeted Attack Platform și a soluțiilor Kaspersky Endpoint Detection and Response.
- Kaspersky Endpoint Agent ca parte a soluțiilor Detection and Response de la Kaspersky.

  Kaspersky comută toate soluțiile Detection and Response pentru a funcționa cu agentul încorporat Kaspersky Endpoint Security în loc de Kaspersky Endpoint Agent. Începând cu versiunea 12.1, aplicația acceptă toate soluțiile Detection and Response.

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

  Începând cu Kaspersky Endpoint Security12.0, puteți migra de la Kaspersky Security for Windows Server la Kaspersky Endpoint Security for Windows și puteți utiliza aceeași soluție pentru a proteja stațiile de lucru și serverele.

- Kaspersky Embedded Systems Security.

Dacă aplicațiile Kaspersky din această listă sunt instalate pe computer, Kaspersky Endpoint Security elimină aceste aplicații. Așteaptă terminarea acestui proces înainte de a continua instalarea aplicației Kaspersky Endpoint Security.

Omiterea verificării pentru detectarea software-ului care poate cauza probleme de compatibilitate

Dacă Kaspersky Endpoint Security detectează software-uri din lista incompatible.txt, instalarea aplicației va fi încheiată. Pentru a continua instalarea, trebuie să elimini acea aplicație. Cu toate acestea, dacă producătorul software-ului terț a indicat în documentația sa că software-ul său este compatibil cu Endpoint Protection Platform (EPP), poți instala Kaspersky Endpoint Security pe un computer care conține o aplicație de la acest producător. De exemplu, producătorul soluției Endpoint Detection and Response (EDR) poate declara compatibilitatea acesteia cu sistemele EPP terțe. În acest caz, trebuie să pornești instalarea componentei Kaspersky Endpoint Security fără a executa o verificare a software-ului instalat. Pentru a face acest lucru, transmiteți următorii parametri instalatorului:

- `SKIPPRODUCTCHECK=1`. Dezactivează verificarea pentru software-ul instalat. Lista programelor software care pot cauza probleme de incompatibilitate este disponibilă în fișierul incompatible.txt, care este inclus în kitul de

distribuție. Dacă nu este setată nicio valoare pentru acest parametru și este detectat un software din listă, instalarea aplicației Kaspersky Endpoint Security va fi oprită.

- `SKIPPRODUCTUNINSTALL=1`. Dezactivează eliminarea automată a software-ului detectat din lista incompatible.txt. Dacă nu este setată nicio valoare pentru acest parametru, Kaspersky Endpoint Security încearcă să elimine software-ul care poate cauza probleme de compatibilitate.

- `CLEANERSIGNCHECK=0`. Dezactivează verificarea semnăturii digitale a aplicațiilor găsite în urma verificării. Dacă acest parametru nu este setat, verificarea semnăturilor digitale este dezactivată la implementarea aplicației prin Kaspersky Security Center. Când aplicația este instalată local, verificarea semnăturii digitale este activată în mod implicit.

Puteți trece parametrii în linia de comandă când instalați local aplicația.

Dacă în timpul procesului de instalare ai omis scanarea pentru depistarea software-urilor care pot cauza probleme de compatibilitate, Kaspersky Endpoint Security poate efectua din nou această verificare atunci când componentele aplicației se modifică. Pentru a omite scanarea pentru detectarea software-urilor instalate, trebuie să configurezi activitatea *Modificare componente ale aplicației*.

Exemplu:

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

Pentru a instala de la distanță Kaspersky Endpoint Security, trebuie să adaugi parametrii corespunzători la fișierul de generare a pachetului de instalare numit `kes_win.kud` în `[Setup]` (vezi mai jos). Fișierul `kes_win.kud` este inclus în kitul de distribuție.

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
```

Instalarea și eliminarea aplicației

Aplicația Kaspersky Endpoint Security poate fi instalată pe un computer în următoarele moduri:

- local, folosind Expertul de configurare.
- local, din linia de comandă.
- de la distanță, folosind Kaspersky Security Center.
- la distanță, prin intermediul editorului de gestionare a politicilor de grup pentru Microsoft Windows (pentru mai multe detalii, vizitați site-ul web de suport tehnic Microsoft).
- la distanță, folosind System Center Configuration Manager.

Puteți configura setările de instalare a aplicației în mai multe moduri. Dacă utilizați simultan mai multe metode pentru configurarea setărilor, Kaspersky Endpoint Security aplică setările cu cea mai mare prioritate. Kaspersky Endpoint Security folosește următoarea ordine de priorități:

1. Setări primite din fișierul setup.ini.
2. Setări primite din fișierul installer.ini.
3. Setări primite de la linia de comandă.
4. Setări primite de la fișierul de configurare (install.cfg).

Recomandăm închiderea tuturor aplicațiilor în execuție înainte de a începe instalarea Kaspersky Endpoint Security (inclusiv instalarea la distanță).

Când instalezi Kaspersky Endpoint Security, sistemul de operare poate afișa propriile mesaje. Conexiunile la rețea și la Internet pot fi, de asemenea, întrerupte atunci când aplicația este instalată.

La instalarea, actualizarea sau dezinstalarea Kaspersky Endpoint Security, pot apărea erori. Pentru mai multe informații despre rezolvarea acestor erori, vă rugăm să consultați Baza de cunoștințe pentru suport tehnic.

Implementarea prin Kaspersky Security Center

Kaspersky Endpoint Security se poate implementa pe computere dintr-o rețea de companie în mai multe moduri. Poți să alegi cel mai potrivit scenariu de implementare pentru organizația ta sau să combini simultan mai multe scenarii de implementare. Înainte de a instala aplicația, trebuie să te asiguri că Kaspersky Security Center Network Agent este instalat pe computer. *Agentul de rețea* facilitează interacțiunea dintre Serverul de administrare și un computer client.

Kaspersky Security Center acceptă următoarele metode principale de implementare:

- Instalarea aplicației folosind Expertul de implementare a protecției.

  Metoda de instalare standard este convenabilă dacă ești mulțumit de setările implicite pentru Kaspersky Endpoint Security și organizația are o infrastructură simplă care nu necesită configurații speciale.

- Instalarea aplicației utilizând activitatea de instalare la distanță.

  Metodă de instalare universală, care permite configurarea setărilor pentru Kaspersky Endpoint Security și gestionarea flexibilă a activităților de instalare la distanță. Instalarea Kaspersky Endpoint Security constă din următorii pași:

  1. Crearea unui pachet de instalare.
  2. Crearea unui pachet de instalare la distanță.

Kaspersky Security Center acceptă și alte metode de instalare a aplicației Kaspersky Endpoint Security, cum ar fi implementarea într-o imagine a sistemului de operare. Pentru detalii despre alte metode de implementare, consultați Ajutor pentru Kaspersky Security Center.

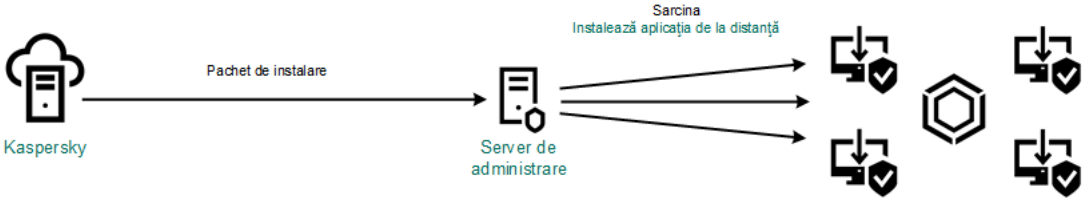
Instalarea standard a aplicației

Kaspersky Security Center furnizează un Expert de implementare a protecției pentru instalarea aplicației pe computerele companiei. Expertul de implementare a protecției include următoarele acțiuni principale:

1. Selectarea unui pachet de instalare pentru Kaspersky Endpoint Security.

   Un *pachet de instalare* este un set de fișiere create pentru instalarea la distanță a unei aplicații Kaspersky prin intermediul Kaspersky Security Center. Pachetul de instalare conține o serie de setări necesare pentru a instala aplicația și a o executa imediat după instalare. Pachetul de instalare este creat utilizându-se fișiere cu extensii .kpd și .kud incluse kitul de distribuție al aplicației. Pachetul de instalare pentru Kaspersky Endpoint Security este comun pentru toate versiunile de Windows și tipurile de arhitecturi acceptate.

2. Crearea activității *Install application remotely* a Serverului de administrare Kaspersky Security Center.



Implementarea Kaspersky Endpoint Security

Cum se execută Expertul de implementare a protecției în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectează **Advanced** → **Remote installation**.
3. Faceți clic pe linkul **Deploy installation package on managed devices (workstations)**.

Se va porni Expertul de implementare a protecției. Urmează instrucțiunile din expert.

Pe un computer client trebuie să fie deschise porturile TCP 139 și 445 și porturile UDP 137 și 138.

Pasul 1. Selectarea unui pachet de instalare

Selectați în listă pachetul de instalare pentru Kaspersky Endpoint Security. Dacă lista nu conține pachetul de instalare pentru Kaspersky Endpoint Security, puteți crea pachetul fîn Expert.

Poți configura setările pentru pachetul de instalare în Kaspersky Security Center. De exemplu, poți selecta componentele aplicației care vor fi instalate pe un computer.

Aplicația Agent de rețea va fi, de asemenea, instalată împreună cu Kaspersky Endpoint Security. *Agentul de rețea* facilitează interacțiunea dintre Serverul de administrare și un computer client. Dacă Agentul de rețea este deja instalat pe computer, acesta nu este instalat din nou.

Pasul 2. Selectarea sursei pachetului de instalare

Selectează sursa **Deploy Kaspersky Security Center package**.

Pasul 3. Selectarea dispozitivelor pentru instalare

Selectați computerele pentru instalarea aplicației Kaspersky Endpoint Security. Sunt disponibile următoarele opțiuni:

- Atribuirea activității unui grup de administrare. În acest caz, activitatea este atribuită computerelor incluse într-un grup de administrare creat anterior.
- Selectare computere detectate în rețea de Serverul de administrare: *dispozitive neatribuite*. Agentul de rețea nu este instalat pe dispozitive neatribuite. În acest caz, sarcina este atribuită unor dispozitive specifice. Dispozitivele specifice pot include dispozitive din grupuri de administrare, precum și dispozitive neatribuite.
- Specificarea manuală a adreselor computerelor sau importarea adreselor dintr-o listă. Poți specifica nume NetBIOS, adrese IP și subrețele IP ale dispozitivelor cărora dorești să le atribui activitatea.

Pasul 4. Definirea setărilor activității de instalare la distanță

Configurați următoarele setări suplimentare ale aplicației:

- **Force installation package download**. Selectați metoda de instalare a aplicației:
  - **Using Network Agent**. Agentul de rețea este responsabil pentru livrarea pachetului de instalare Kaspersky Endpoint Security către computerele client. Dacă nu este instalată componenta Agentul de rețea, activitatea se va termina cu o eroare. În acest caz, adaugă pachetul de instalare Agent de rețea la activitatea *Install application remotely* și activează livrarea fișierelor prin resursele sistemului de operare. Apoi, Agentul de rețea va fi instalat folosind resursele sistemului de operare. După aceea, Kaspersky Endpoint Security este instalat de instrumentele din Agentul de rețea.
  - **Using operating system resources through distribution points**. Pachetul de instalare se livrează computerelor client folosindu-se resursele sistemului de operare prin intermediul punctelor de distribuire. Poți selecta această opțiune dacă există cel puțin un punct de distribuire în rețea. Pentru mai multe detalii despre punctele de distribuție, consultați Ajutor pentru Kaspersky Security Center.
  - **Using operating system resources through Administration Server**. Fișierele vor fi livrate pe computerele client utilizându-se resursele sistemului de operare prin intermediul Serverului de administrare. Poți selecta această opțiune dacă Agentul de rețea nu este instalat pe computerul client, însă computerul client se află în aceeași rețea ca și Serverul de administrare.
- **Behavior for devices managed through other Administration Servers**. Selectați metoda de instalare pentru Kaspersky Endpoint Security. Dacă rețeaua are instalate mai multe Servere de administrare, aceste Servere de administrare pot vedea aceleași computere client. Acest lucru poate cauza, de exemplu, instalarea de mai multe ori la distanță a unei aplicații pe același computer client prin intermediul unor Servere de administrare diferite sau alte conflicte.
- **Do not re-install application if it is already installed**. Debifați această casetă de selectare dacă, de exemplu, dorești să instalezi o versiune anterioară a aplicației.
- **Assign Network Agent installation in Active Directory group policies**. Instalarea manuală a Agentului de rețea utilizând resursele Active Directory. Pentru a instala Agentul de rețea, activitatea de instalare la distanță trebuie executată cu privilegii de administrator de domeniu.

Pasul 5. Selectarea unei chei de licență

Adăugați la pachetul de instalare o cheie pentru activarea aplicației. Acest pas este opțional. Dacă Serverul de administrare conține o cheie de licență cu funcționalitate de distribuție automată, cheia va fi adăugată automat mai târziu. De asemenea, poți să activezi aplicația ulterior folosind activitatea *Add key*

Pasul 6. Selectarea setării de repornire a sistemului de operare

Selectați acțiunea care trebuie efectuată dacă este necesară o repornire a computerului. Repornirea nu este necesară atunci când instalezi Kaspersky Endpoint Security. Repornirea este necesară numai dacă trebuie să elimini aplicații incompatibile înainte de instalare. Repornirea poate fi necesară și atunci când actualizezi versiunea aplicației.

Pasul 7. Eliminarea aplicațiilor incompatibile înainte de instalarea aplicației

Citiți cu atenție lista de aplicații incompatibile și permiteți eliminarea acestor aplicații. Dacă pe computer sunt instalate aplicații incompatibile, instalarea aplicației Kaspersky Endpoint Security se termină cu o eroare.

Pasul 8. Selectarea unui cont pentru accesarea dispozitivelor

Selectați contul pentru instalarea Agentului de rețea folosind instrumentele din sistemul de operare. În acest caz, sunt necesare drepturi de administrator pentru accesul la computer. Poți adăuga mai multe conturi. Dacă un cont nu are drepturi suficiente, Expertul de instalare utilizează următorul cont. Dacă instalezi Kaspersky Endpoint Security utilizând instrumentele Agentului de rețea, nu este necesar să selectezi un cont.

Pasul 9. Pornirea instalării

Ieșiți din Expert. Dacă este necesar, bifați caseta de selectare **Run the task after the wizard finishes**. Puteți monitoriza progresul activității în proprietățile activității.

Cum se pornește Expertul de implementare a protecției în Web Console și Cloud Console

În fereastra principală a componentei Web Console, selectați **Discovery & deployment → Deployment & assignment → Protection deployment wizard**.

Se va porni Expertul de implementare a protecției. Urmează instrucțiunile din expert.

Pe un computer client trebuie să fie deschise porturile TCP 139 și 445 și porturile UDP 137 și 138.

Pasul 1. Selectarea unui pachet de instalare

Selectați în listă pachetul de instalare pentru Kaspersky Endpoint Security. Dacă lista nu conține pachetul de instalare pentru Kaspersky Endpoint Security, puteți crea pachetul fîn Expert. Pentru a crea pachetul de instalare, nu este necesar să căutați pachetul de distribuție și să îl salvați în memoria computerului. În Kaspersky Security Center, puteți vizualiza lista de pachete de distribuție care își are originea pe serverele Kaspersky, iar pachetul de instalare este creat automat. Kaspersky actualizează lista după lansarea de noi versiuni ale aplicației.

Poți configura setările pentru pachetul de instalare în Kaspersky Security Center. De exemplu, poți selecta componentele aplicației care vor fi instalate pe un computer.

Pasul 2. Selectarea unei chei de licență

Adăugați la pachetul de instalare o cheie pentru activarea aplicației. Acest pas este opțional. Dacă Serverul de administrare conține o cheie de licență cu funcționalitate de distribuție automată, cheia va fi adăugată automat mai târziu. De asemenea, poți să activezi aplicația ulterior folosind activitatea *Add key*

Pasul 3. Selectarea unui Agent de rețea

Selectați versiunea pentru Agent de rețea care va fi instalată împreună cu aplicația Kaspersky Endpoint Security. *Agentul de rețea* facilitează interacțiunea dintre Serverul de administrare și un computer client. Dacă Agentul de rețea este deja instalat pe computer, acesta nu este instalat din nou.

Pasul 4. Selectarea dispozitivelor pentru instalare

Selectați computerele pentru instalarea aplicației Kaspersky Endpoint Security. Sunt disponibile următoarele opțiuni:

- Atribuirea activității unui grup de administrare. În acest caz, activitatea este atribuită computerelor incluse într-un grup de administrare creat anterior.
- Selectare computere detectate în rețea de Serverul de administrare: *dispozitive neatribuite*. Agentul de rețea nu este instalat pe dispozitive neatribuite. În acest caz, sarcina este atribuită unor dispozitive specifice. Dispozitivele specifice pot include dispozitive din grupuri de administrare, precum și dispozitive neatribuite.
- Specificarea manuală a adreselor computerelor sau importarea adreselor dintr-o listă. Poți specifica nume NetBIOS, adrese IP și subrețele IP ale dispozitivelor cărora dorești să le atribui activitatea.

Pasul 5. Configurarea setărilor avansate

Configurați următoarele setări suplimentare ale aplicației:

- **Force installation package download**. Selectați metoda de instalare a aplicației:

  - **Using Network Agent**. Agentul de rețea este responsabil pentru livrarea pachetului de instalare Kaspersky Endpoint Security către computerele client. Dacă nu este instalată componenta Agentul de rețea, activitatea se va termina cu o eroare. În acest caz, adaugă pachetul de instalare Agent de rețea la activitatea *Install application remotely* și activează livrarea fișierelor prin resursele sistemului de operare. Apoi, Agentul de rețea va fi instalat folosind resursele sistemului de operare. După aceea, Kaspersky Endpoint Security este instalat de instrumentele din Agentul de rețea.

  - **Using operating system resources through distribution points**. Pachetul de instalare se livrează computerelor client folosindu-se resursele sistemului de operare prin intermediul punctelor de distribuire. Poți selecta această opțiune dacă există cel puțin un punct de distribuire în rețea. Pentru mai multe detalii despre punctele de distribuție, consultați Ajutor pentru Kaspersky Security Center.

  - **Using operating system resources through Administration Server**. Fișierele vor fi livrate pe computerele client utilizându-se resursele sistemului de operare prin intermediul Serverului de administrare. Poți selecta această opțiune dacă Agentul de rețea nu este instalat pe computerul client, însă computerul client se află în aceeași rețea ca și Serverul de administrare.

- **Do not re-install application if it is already installed**. Debifați această casetă de selectare dacă, de exemplu, dorești să instalezi o versiune anterioară a aplicației.

- **Assign package installation in Active Directory group policies**. Kaspersky Endpoint Security se instalează cu ajutorul Agentului de rețea sau, manual, prin intermediul Active Directory. Pentru a instala Agentul de rețea, activitatea de instalare la distanță trebuie executată cu privilegii de administrator de domeniu.

Pasul 6. Selectarea setării de repornire a sistemului de operare

Selectați acțiunea care trebuie efectuată dacă este necesară o repornire a computerului. Repornirea nu este necesară atunci când instalezi Kaspersky Endpoint Security. Repornirea este necesară numai dacă trebuie să elimini aplicații incompatibile înainte de instalare. Repornirea poate fi necesară și atunci când actualizezi versiunea aplicației.

Pasul 7. Eliminarea aplicațiilor incompatibile înainte de instalarea aplicației

Citiți cu atenție lista de aplicații incompatibile și permiteți eliminarea acestor aplicații. Dacă pe computer sunt instalate aplicații incompatibile, instalarea aplicației Kaspersky Endpoint Security se termină cu o eroare.

Pasul 8. Atribuirea la un grup de administrare

Selectați grupul de administrare în care vor fi mutate computerele după instalarea Agentului de rețea. Calculatoarele trebuie mutate într-un grup de administrare pentru a putea fi aplicate politicile și activitățile de grup. Dacă un computer este deja în orice grup de administrare, computerul nu va fi mutat. Dacă nu selectezi un grup de administrare, computerele vor fi adăugate la grupul **Unassigned devices**.

Pasul 9. Selectarea unui cont pentru accesarea dispozitivelor

Selectați contul pentru instalarea Agentului de rețea folosind instrumentele din sistemul de operare. În acest caz, sunt necesare drepturi de administrator pentru accesul la computer. Poți adăuga mai multe conturi. Dacă un cont nu are drepturi suficiente, Expertul de instalare utilizează următorul cont. Dacă instalezi Kaspersky Endpoint Security utilizând instrumentele Agentului de rețea, nu este necesar să selectezi un cont.

Pasul 10. Începerea instalării

Ieșiți din Expert. Dacă este necesar, bifați caseta de selectare **Run the task after the wizard finishes**. Puteți monitoriza progresul activității în proprietățile activității.

Crearea unui pachet de instalare

Un *pachet de instalare* este un set de fișiere create pentru instalarea la distanță a unei aplicații Kaspersky prin intermediul Kaspersky Security Center. Pachetul de instalare conține o serie de setări necesare pentru a instala aplicația și a o executa imediat după instalare. Pachetul de instalare este creat utilizându-se fișiere cu extensii .kpd și .kud incluse kitul de distribuție al aplicației. Pachetul de instalare pentru Kaspersky Endpoint Security este comun pentru toate versiunile de Windows și tipurile de arhitecturi acceptate.

Cum se creează un pachet de instalare în Consola de administrare (MMC)

1. În Consola de administrare, accesați directorul **Administration Server** → **Advanced** → **Remote installation** → **Installation packages**.

   Aceasta deschide o listă cu pachetele de instalare care au fost descărcate în Kaspersky Security Center.

2. Fă clic pe **Create installation package**.

Funcția Expert pentru pachet nou pornește. Urmează instrucțiunile din expert.

Pasul 1. Selectarea tipului pachetului de instalare

Selectați opțiunea **Create an installation package for a Kaspersky application**.

Pasul 2. Definirea numelui pachetului de instalare

Introduceți numele pachetului de instalare, de exemplu, *Kaspersky Endpoint Security for Windows 14.1*.

Pasul 3. Selectarea pachetului de distribuție pentru instalare

Faceți clic pe butonul **Răsfoire** și selectați fișierul `kes_win.kud` inclus în kitul de distribuție.

Dacă este necesar, actualizează bazele de date antivirus din pachetul de instalare utilizând caseta de selectare **Copy updates from repository to installation package**.

Pasul 4. Acordul de licență pentru utilizatorul final și Politica privind confidențialitatea

Citiți și acceptați termenii Acordului de licență pentru utilizatorul final și Politica privind confidențialitatea.

Pachetul de instalare va fi creat și adăugat în Kaspersky Security Center. Utilizând pachetul de instalare, poți să instalezi aplicația Kaspersky Endpoint Security pe computere din rețele de companie sau să actualizezi versiunea aplicației.

În setările pachetului de instalare, poți selecta componentele aplicației pentru diferite tipuri de sisteme de operare. Adică, pachetul de instalare include două seturi de componente: pentru stații de lucru și pentru servere. Înainte de a implementa pachetul de instalare, programul de instalare detectează tipul sistemului de operare și instalează numai acele componente ale aplicației pe care le-ai selectat pentru acel tip de sistem de operare. Astfel, poți utiliza același pachet de instalare pentru stațiile de lucru și servere.

Pachetul de instalare conține baze de date antivirus din depozitul Serverului de administrare. Puteți actualiza bazele de date din pachetul de instalare pentru a reduce consumul de trafic la actualizarea bazelor de date, după instalarea Kaspersky Endpoint Security.

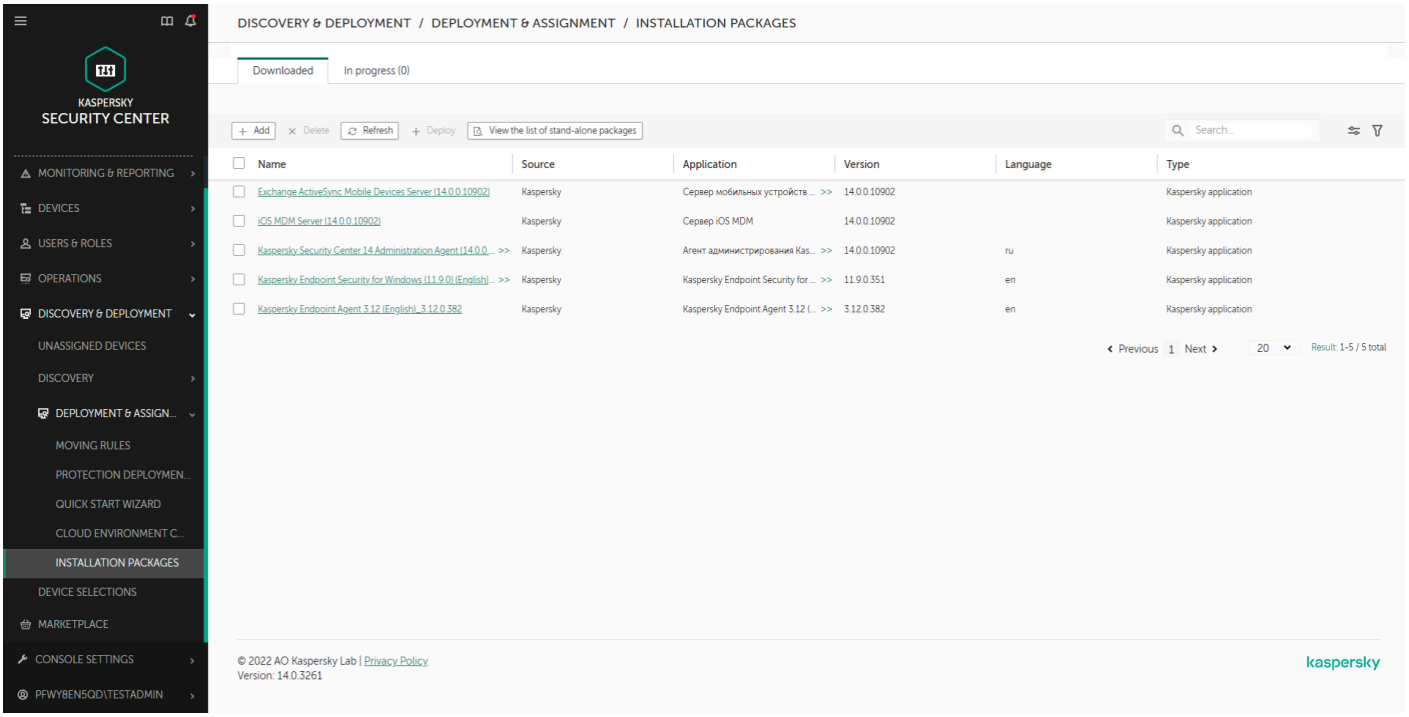
Cum se creează un pachet de instalare în Web Console și Cloud Console

1. În fereastra principală a componentei Web Console, selectați **Discovery & deployment → Deployment & assignment → Installation packages**.

   Aceasta deschide o listă cu pachetele de instalare care au fost descărcate în Kaspersky Security Center.

2. Fă clic pe **Add**.

Funcția Expert pentru pachet nou pornește. Urmează instrucțiunile din expert.



Lista pachetelor de instalare

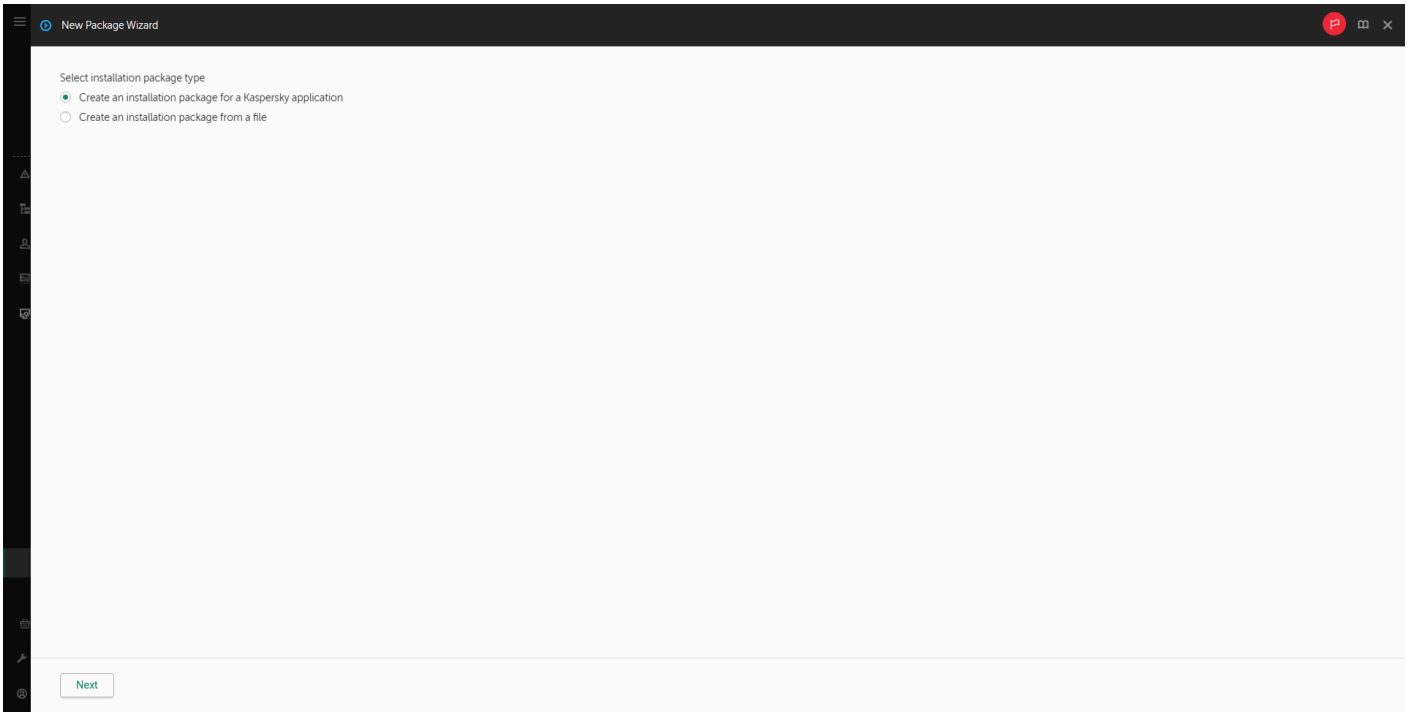
Pasul 1. Selectarea tipului pachetului de instalare

Selectați opțiunea **Create an installation package for a Kaspersky application**.

Expertul va crea un pachet de instalare din pachetul de distribuție care se află pe serverele Kaspersky. Lista este actualizată automat după lansarea noilor versiuni ale aplicațiilor Kaspersky. Se recomandă să selectați această opțiune pentru instalarea Kaspersky Endpoint Security.

De asemenea, puteți crea un pachet de instalare dintr-un fișier.

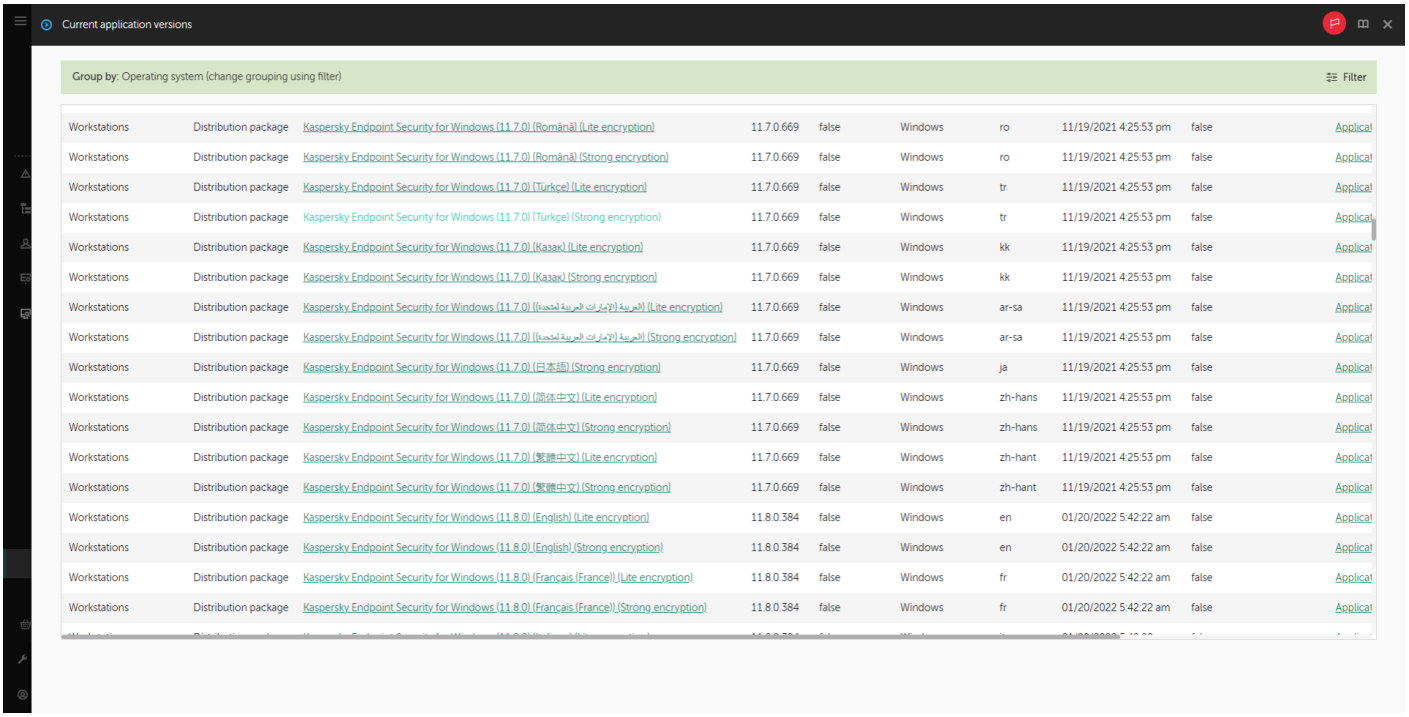
Crearea unui pachet de instalare pentru Kaspersky Endpoint Security dintr-un fișier este disponibilă numai în Kaspersky Security Center Web Console.



Tipuri de pachete de instalare

Pasul 2. Pachete de instalare

Selectați pachetul de instalare pentru Kaspersky Endpoint Security for Windows. Va începe procesul de creare a pachetului de instalare. În timpul creării pachetului de instalare, trebuie să acceptați termenii Acordului de licență pentru utilizatorul final și Politica privind confidențialitatea.

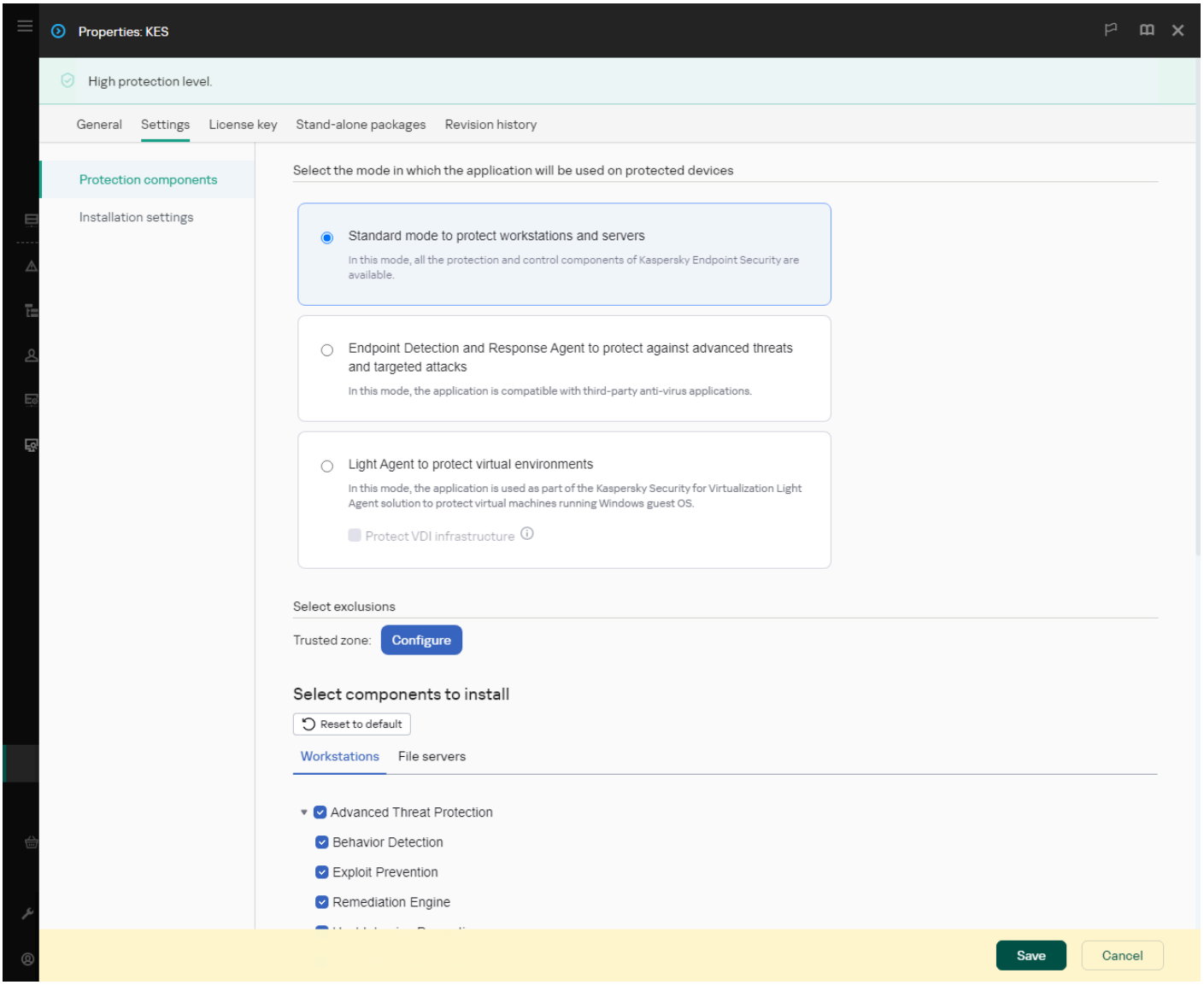


Lista pachetelor de instalare pe serverele Kaspersky

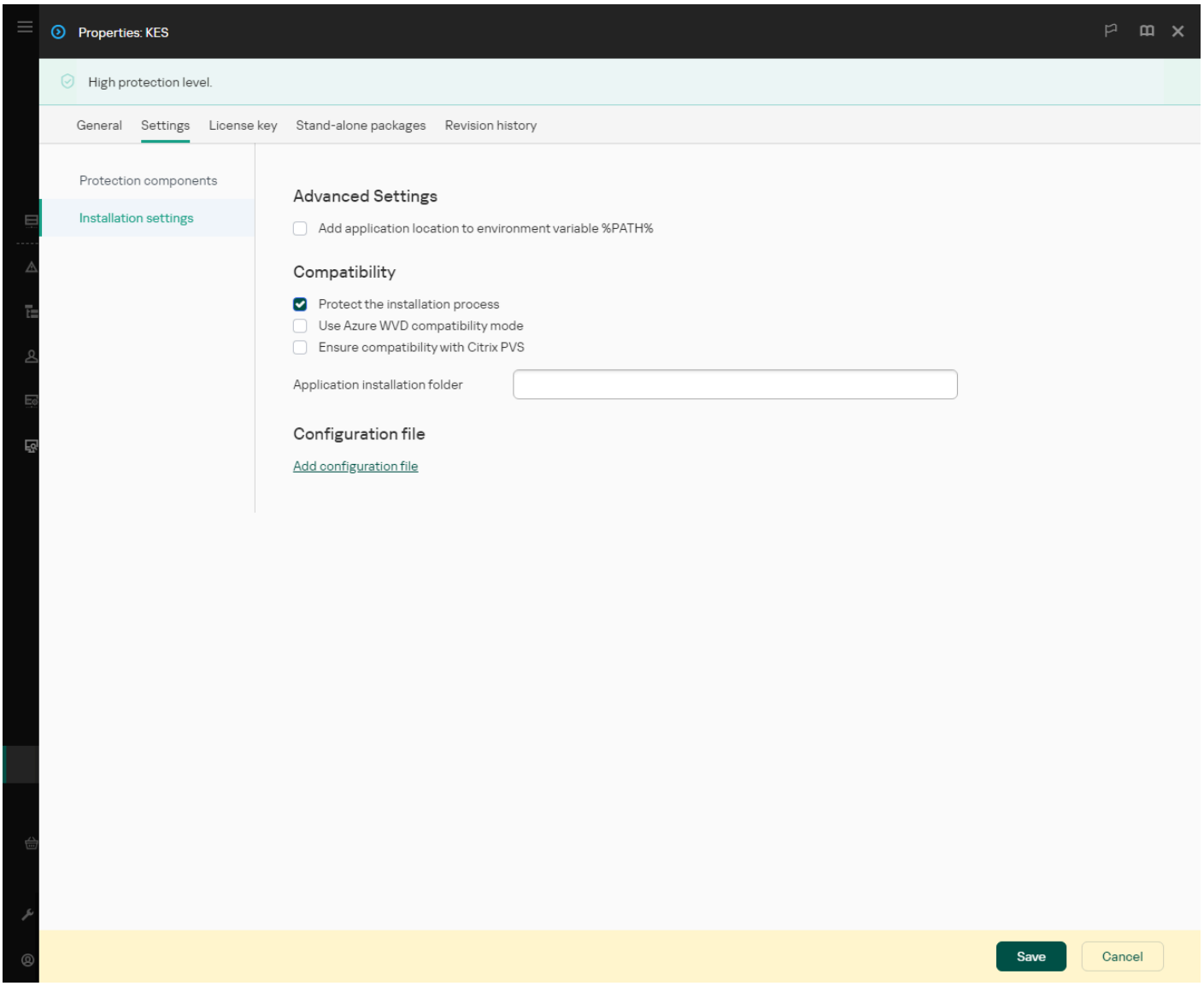
Pachetul de instalare va fi creat și adăugat în Kaspersky Security Center. Utilizând pachetul de instalare, poți să instalezi aplicația Kaspersky Endpoint Security pe computere din rețele de companie sau să actualizezi versiunea aplicației.

În setările pachetului de instalare, poți selecta componentele aplicației pentru diferite tipuri de sisteme de operare. Adică, pachetul de instalare include două seturi de componente: pentru stații de lucru și pentru servere. Înainte de a implementa pachetul de instalare, programul de instalare detectează tipul sistemului de operare și instalează numai acele componente ale aplicației pe care le-ai selectat pentru acel tip de sistem de operare. Astfel, poți utiliza același pachet de instalare pentru stațiile de lucru și servere.

Pachetul de instalare conține baze de date antivirus din depozitul Serverului de administrare. Puteți actualiza bazele de date din pachetul de instalare pentru a reduce consumul de trafic la actualizarea bazelor de date, după instalarea Kaspersky Endpoint Security.



Componente incluse în pachetul de instalare



Setările de instalare ale pachetului de instalare

Setări pentru pachetului de instalare

Secțiune	Descriere
Componente de protecție	**Modul Standard**. Configurația implicită. Această configurație vă permite să utilizați toate componentele aplicației, inclusiv componentele care oferă suport pentru soluțiile Detection and Response. Această configurație este utilizată pentru protecția completă a computerului împotriva unei varietăți de amenințări, atacuri de rețea și fraude. **Endpoint Detection and Response Agent**. În această configurație, puteți instala doar componentele care oferă suport pentru soluțiile Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), precum și KUMA. Această configurație este necesară dacă o platformă Endpoint Protection Platform (EPP) terță este implementată în organizație împreună cu soluția Kaspersky Detection and Response. Acest lucru face ca Kaspersky Endpoint Security în configurația Endpoint Detection and Response Agent să fie compatibil cu aplicațiile EPP terțe. **Light Agent pentru protejarea mediilor virtuale**. Această configurație este destinată aplicației care este utilizată ca parte a soluției Kaspersky Security for Virtualization Light Agent. Light Agent trebuie instalat pe fiecare mașină virtuală care trebuie protejată folosind soluția. În această configurație, nu puteți utiliza componentele Data Encryption sau Control adaptiv al anomaliilor. Dacă instalezi Light Agent pe un șablon de mașină virtuală care va fi folosit pentru a crea *mașini virtuale non-persistente*, bifează caseta de selectare **Protejează infrastructura VDI** (VDI înseamnă Virtual Desktop Infrastructure). Modul de protecție VDI ajută la optimizarea performanței Kaspersky Endpoint Security pe mașinile virtuale non-persistente. În acest mod, Light Agent refuză actualizările aplicației care necesită repornirea mașinii virtuale. Când se primesc actualizări ale aplicației care necesită o repornire, Light Agent generează un eveniment despre necesitatea actualizării șablonului mașinilor virtuale protejate.
Excluderi	Începând cu Kaspersky Endpoint Security 12.6 for Windows, excluderile de scanare și aplicații de încredere sunt adăugate la zona de încredere. Excluderile de la scanare și aplicațiile de încredere predefinite ajută la configurarea rapidă a Kaspersky Endpoint Security pe serverele SQL, serverele Microsoft Exchange și System Center Configuration Manager. Aceasta înseamnă că nu trebuie să configurați manual o zonă de încredere pentru aplicație pe servere. Începând cu Kaspersky Endpoint Security 12.8 for Windows, poți instala aplicația în modul Light Agent pentru a proteja mediile virtuale. Excluderile de la scanare predefinite și aplicațiile de încredere te pot ajuta să configurezi rapid Kaspersky Endpoint Security în mediile virtuale Citrix și VMware. De asemenea, poți configura zona de încredere mai târziu, în proprietățile politicii: excluderi de la scanare și aplicații de încredere.

Secțiune	Descriere
Selectează componentele de instalat	În această secțiune poți selecta componentele aplicației care vor fi disponibile. Poți să modifici ulterior setul de componente ale aplicației folosind activitatea *Modificare componente ale aplicației*. Poți crea seturi separate de componente pentru stații de lucru și servere. Înainte de a implementa pachetul de instalare, programul de instalare detectează tipul sistemului de operare și instalează numai acele componente ale aplicației pe care le-ai selectat pentru acel tip de sistem de operare. Astfel, poți utiliza același pachet de instalare pentru stațiile de lucru și servere. Setul de componente disponibile depinde de configurația aplicației: **Modul Standard** Componenta BadUSB Attack Prevention, componenta Detection and Response și componentele de criptare a datelor nu sunt instalate în mod implicit. Aceste componente se pot adăuga în setările pachetului de instalare. **Endpoint Detection and Response Agent** În această configurație, sunt disponibili numai agenți încorporați pentru soluțiile Kaspersky Detection and Response. **Light Agent pentru protejarea mediilor virtuale** În această configurație, poți utiliza aproape toate componentele aplicației care sunt disponibile în configurația **Modul Standard**, cu excepția componentelor de criptare a datelor și a componentei Control adaptiv al anomaliilor.
License key	În această secțiune puteți activa aplicația. Pentru a activa aplicația, trebuie să selectați o cheie de licență. Înainte de a face acest lucru, trebuie să adăugați cheia la Serverul de administrare. Pentru detalii suplimentare despre adăugarea cheilor pe Kaspersky Security Center Administration Server, consultați secțiunea Ajutor pentru Kaspersky Security Center.
Incompatible applications	Citiți cu atenție lista de aplicații incompatibile și permiteți eliminarea acestor aplicații. Dacă pe computer sunt instalate aplicații incompatibile, instalarea aplicației Kaspersky Endpoint Security se termină cu o eroare.
Installation settings	**Adaugă calea către fișierul avp.com la variabila de sistem %PATH%**. Poți adăuga calea de instalare la variabila %PATH% pentru utilizarea comodă a interfeței liniei de comandă. **Protect the installation process**. Protejarea instalării include protecția împotriva înlocuirii pachetului de distribuție cu aplicații rău intenționate, blocarea accesului la directorul de instalare al aplicației Kaspersky Endpoint Security și blocarea accesului la secțiunea de registre a sistemului care conține cheile aplicației. Cu toate acestea, dacă aplicația nu poate fi instalată (de exemplu, atunci când se execută o instalare la distanță cu ajutorul Windows Remote Desktop), te sfătuim să dezactivezi protecția procesului de instalare. **Asigură compatibilitatea cu Citrix PVS**. Poți activa suportul pentru Citrix Provisioning Services pentru a instala aplicația Kaspersky Endpoint Security pe o mașină virtuală. **Utilizează modul de compatibilitate Azure WVD**. Această funcție asigură afișarea corectă a stării mașinii virtuale Azure în consola Kaspersky Anti Targeted Attack Platform. Pentru a monitoriza performanța computerului, Kaspersky Endpoint Security trimite date de telemetrie către serverele KATA. Telemetria include un ID al computerului (Sensor ID). Modul de compatibilitate Azure WVD permite alocarea unui Sensor ID unic permanent către aceste mașini virtuale. Dacă modul de compatibilitate este dezactivat, Sensor ID se poate schimba după ce computerul este repornit din cauza modului în care funcționează mașinile virtuale Azure. Acest lucru poate face ca duplicate ale mașinilor virtuale să apară pe consolă. **Application installation folder**. Poți schimba calea de instalare a aplicației Kaspersky Endpoint Security pe un computer client. În mod implicit, aplicația este instalată în directorul `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.1`. **Configuration file**. Instalarea aplicației cu setări predefinite. Pentru aceasta, trebuie să încarci un fișier care definește setările pentru aplicația Kaspersky Endpoint Security. Poți crea un fișier de configurare în interfața locală a aplicației.

Actualizarea bazelor de date în pachetul de instalare

Pachetul de instalare conține baze de date antivirus din depozitul Serverului de administrare, care sunt actualizate la crearea pachetului de instalare. După crearea pachetului de instalare, puteți actualiza bazele de date antivirus din pachetul de instalare. Acest lucru vă permite să reduceți consumul de trafic la actualizarea bazelor de date antivirus după instalarea Kaspersky Endpoint Security.

Pentru a actualiza bazele de date antivirus din depozitul Serverului de administrare, utilizează activitatea *Download updates to the Administration Server repository* a Serverului de administrare. Pentru mai multe informații despre actualizarea bazelor de date antivirus din depozitul Administration Server, consultați Ajutor pentru Kaspersky Security Center.

Puteți actualiza bazele de date din pachetul de instalare numai în Consola de administrare și Kaspersky Security Center Web Console. Nu este posibil să actualizați bazele de date din pachetul de instalare în Kaspersky Security Center Cloud Console.

Cum se actualizează bazele de date antivirus din pachetul de instalare prin Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectează directorul **Advanced** → **Remote installation** → **Installation packages**.

   Aceasta deschide o listă cu pachetele de instalare care au fost descărcate în Kaspersky Security Center.
3. Deschideți proprietățile pachetului de instalare.
4. În secțiunea **General**, faceți clic pe **Update databases**.

Drept urmare, bazele de date antivirus din pachetul de instalare vor fi actualizate din depozitul Serverului de administrare. Fișierul `bases.cab` inclus în kitul de distribuție va fi înlocuit de directorul cu `bases`. Fișierele pachetului de actualizare se vor afla în director.

Cum se actualizează bazele de date antivirus din pachetul de instalare prin Web Console

1. În fereastra principală a componentei Web Console, selectați **Discovery & deployment** → **Deployment & assignment** → **Installation packages**.

   Se va deschide o listă de pachete de instalare descărcate pe Consola Web.
2. Faceți clic pe numele pachetului de instalare Kaspersky Endpoint Security în care doriți să actualizați bazele de date antivirus.

   Se deschide fereastra de proprietăți a pachetului de instalare.
3. În fila **General information**, faceți clic pe linkul **Update databases**.

Drept urmare, bazele de date antivirus din pachetul de instalare vor fi actualizate din depozitul Serverului de administrare. Fișierul `bases.cab` inclus în kitul de distribuție va fi înlocuit de directorul cu `bases`. Fișierele pachetului de actualizare se vor afla în director.

Crearea unui pachet de instalare la distanță

Activitatea *Install application remotely* este concepută pentru instalarea la distanță a Kaspersky Endpoint Security. Activitatea *Install application remotely* vă permite să implementați pachetul de instalare al aplicației pe toate computerele din organizație. Înainte de a implementa pachetul de instalare, puteți să actualizați bazele de date antivirus din pachet și să selectați componentele disponibile ale aplicației în proprietățile pachetului de instalare.

Cum se creează o activitate de instalare la distanță în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați **Tasks**.

   Lista activităților se deschide.
3. Fă clic pe **New task**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Selectarea tipului activității

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

Pasul 2. Selectarea unui pachet de instalare

Selectați în listă pachetul de instalare pentru Kaspersky Endpoint Security. Dacă lista nu conține pachetul de instalare pentru Kaspersky Endpoint Security, puteți crea pachetul fîn Expert.

Poți configura setările pentru pachetul de instalare în Kaspersky Security Center. De exemplu, poți selecta componentele aplicației care vor fi instalate pe un computer.

Aplicația Agent de rețea va fi, de asemenea, instalată împreună cu Kaspersky Endpoint Security. *Agentul de rețea* facilitează interacțiunea dintre Serverul de administrare și un computer client. Dacă Agentul de rețea este deja instalat pe computer, acesta nu este instalat din nou.

Pasul 3. Suplimentar

Selectează pachetul de instalare pentru Agentul de rețea. Versiunea selectată pentru Agentul de rețea va fi instalată împreună cu Kaspersky Endpoint Security.

Pasul 4. Setări

Configurați următoarele setări suplimentare ale aplicației:

- **Force installation package download**. Selectați metoda de instalare a aplicației:
  - **Using Network Agent**. Agentul de rețea este responsabil pentru livrarea pachetului de instalare Kaspersky Endpoint Security către computerele client. Dacă nu este instalată componenta Agentul de rețea, activitatea se va termina cu o eroare. În acest caz, adaugă pachetul de instalare Agent de rețea la activitatea *Install application remotely* și activează livrarea fișierelor prin resursele sistemului de operare. Apoi, Agentul de rețea va fi instalat folosind resursele sistemului de operare. După aceea, Kaspersky Endpoint Security este instalat de instrumentele din Agentul de rețea.
  - **Using operating system resources through distribution points**. Pachetul de instalare se livrează computerelor client folosindu-se resursele sistemului de operare prin intermediul punctelor de distribuire. Poți selecta această opțiune dacă există cel puțin un punct de distribuire în rețea. Pentru mai multe detalii despre punctele de distribuție, consultați Ajutor pentru Kaspersky Security Center.
  - **Using operating system resources through Administration Server**. Fișierele vor fi livrate pe computerele client utilizându-se resursele sistemului de operare prin intermediul Serverului de administrare. Poți selecta această opțiune dacă Agentul de rețea nu este instalat pe computerul client, însă computerul client se află în aceeași rețea ca și Serverul de administrare.

- **Behavior for devices managed through other Administration Servers**. Selectați metoda de instalare pentru Kaspersky Endpoint Security. Dacă rețeaua are instalate mai multe Servere de administrare, aceste Servere de administrare pot vedea aceleași computere client. Acest lucru poate cauza, de exemplu, instalarea de mai multe ori la distanță a unei aplicații pe același computer client prin intermediul unor Servere de administrare diferite sau alte conflicte.

- **Do not re-install application if it is already installed**. Debifați această casetă de selectare dacă, de exemplu, dorești să instalezi o versiune anterioară a aplicației.

Pasul 5. Selectarea setării de repornire a sistemului de operare

Selectați acțiunea care trebuie efectuată dacă este necesară o repornire a computerului. Repornirea nu este necesară atunci când instalezi Kaspersky Endpoint Security. Repornirea este necesară numai dacă trebuie să elimini aplicații incompatibile înainte de instalare. Repornirea poate fi necesară și atunci când actualizezi versiunea aplicației.

Pasul 6. Selectarea dispozitivelor cărora le va fi atribuită activitatea

Selectați computerele pentru instalarea aplicației Kaspersky Endpoint Security. Sunt disponibile următoarele opțiuni:

- Atribuirea activității unui grup de administrare. În acest caz, activitatea este atribuită computerelor incluse într-un grup de administrare creat anterior.

- Selectare computere detectate în rețea de Serverul de administrare: *dispozitive neatribuite*. Agentul de rețea nu este instalat pe dispozitive neatribuite. În acest caz, sarcina este atribuită unor dispozitive specifice. Dispozitivele specifice pot include dispozitive din grupuri de administrare, precum și dispozitive neatribuite.

- Specificarea manuală a adreselor computerelor sau importarea adreselor dintr-o listă. Poți specifica nume NetBIOS, adrese IP și subrețele IP ale dispozitivelor cărora dorești să le atribui activitatea.

Pasul 7. Selectarea contului pentru executarea activității

Selectați contul pentru instalarea Agentului de rețea folosind instrumentele din sistemul de operare. În acest caz, sunt necesare drepturi de administrator pentru accesul la computer. Poți adăuga mai multe conturi. Dacă un cont nu are drepturi suficiente, Expertul de instalare utilizează următorul cont. Dacă instalezi Kaspersky Endpoint Security utilizând instrumentele Agentului de rețea, nu este necesar să selectezi un cont.

Pasul 8. Configurarea unei planificări de pornire a activității

Configurați o planificare pentru începerea unei activități, de exemplu, manual sau atunci când computerul este inactiv.

Pasul 9. Definirea numelui activității

Introduceți un nume pentru activitate, de exemplu, *Instalează Kaspersky Endpoint Security for Windows 14.1*.

Pasul 10. Finalizarea creării activității

Ieșiți din Expert. Dacă este necesar, bifați caseta de selectare **Run the task after the wizard finishes**. Puteți monitoriza progresul activității în proprietățile activității. Aplicația va fi instalată în modul silențios. După instalare, pictograma va fi adăugată în zona de notificare a computerului utilizatorului. Dacă pictograma arată așa , asigurați-vă că ați activat aplicația.

Cum se creează o activitate de instalare la distanță în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **Add**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Configurarea setările generale ale activității

Configurați setările generale pentru activitate:

1. În lista verticală **Application**, selectează **Kaspersky Security Center**.
2. În lista verticală **Task type**, selectează **Install application remotely**.
3. În câmpul **Task name**, introdu o descriere succintă, de exemplu *Instalare Kaspersky Endpoint Security pentru manageri*.
4. În blocul **Devices to which the task will be assigned**, selectați domeniul activității.

Pasul 2. Selectarea computerelor pentru instalare

La acest pas, selectați computerele pe care va fi instalată aplicația Kaspersky Endpoint Security, în funcție de opțiunea selectată pentru domeniul activității.

Pasul 3. Configurarea unui pachet de instalare

La acest pas, configurați pachetul de instalare:

1. Selectați pachetul de instalare pentru Kaspersky Endpoint Security for Windows (14.1).

2. Selectează pachetul de instalare pentru Agentul de rețea.

   Versiunea selectată pentru Agentul de rețea va fi instalată împreună cu Kaspersky Endpoint Security. *Agentul de rețea* facilitează interacțiunea dintre Serverul de administrare și un computer client. Dacă Agentul de rețea este deja instalat pe computer, acesta nu este instalat din nou.

3. În blocul **Force installation package download**, selectați metoda de instalare a aplicației:

   - **Using Network Agent**. Agentul de rețea este responsabil pentru livrarea pachetului de instalare Kaspersky Endpoint Security către computerele client. Dacă nu este instalată componenta Agentul de rețea, activitatea se va termina cu o eroare. În acest caz, adaugă pachetul de instalare Agent de rețea la activitatea *Install application remotely* și activează livrarea fișierelor prin resursele sistemului de operare. Apoi, Agentul de rețea va fi instalat folosind resursele sistemului de operare. După aceea, Kaspersky Endpoint Security este instalat de instrumentele din Agentul de rețea.

   - **Using operating system resources through distribution points**. Pachetul de instalare se livrează computerelor client folosindu-se resursele sistemului de operare prin intermediul punctelor de distribuire. Poți selecta această opțiune dacă există cel puțin un punct de distribuire în rețea. Pentru mai multe detalii despre punctele de distribuție, consultați Ajutor pentru Kaspersky Security Center.

   - **Using operating system resources through Administration Server**. Fișierele vor fi livrate pe computerele client utilizându-se resursele sistemului de operare prin intermediul Serverului de administrare. Poți selecta această opțiune dacă Agentul de rețea nu este instalat pe computerul client, însă computerul client se află în aceeași rețea ca și Serverul de administrare.

4. În câmpul **Maximum number of concurrent downloads**, setează o limită pentru numărul de solicitări de descărcare a pachetului de instalare trimise către Administration Server. O limită pentru numărul de solicitări va ajuta la prevenirea supraîncărcării rețelei.

5. În câmpul **Maximum number of installation attempts**, setează o limită pentru numărul de încercări de instalare a aplicației. Dacă instalarea aplicației Kaspersky Endpoint Security se termină cu o eroare, activitatea va porni automat din nou instalarea.

6. Dacă este necesar, debifați caseta de selectare **Do not re-install application if it is already installed**. Acest lucru permite, de exemplu, instalarea uneia dintre versiunile anterioare ale aplicației.

7. Dacă este necesar, debifați caseta de selectare **Verify operating system type before downloading**. Acest lucru îți permite să eviți descărcarea unui pachet de distribuție a aplicației dacă sistemul de operare al computerului nu îndeplinește cerințele software. Dacă ești sigur că sistemul de operare al computerului îndeplinește cerințele software, poți ignora această verificare.

8. Dacă este necesar, bifați caseta de selectare **Assign package installation in Active Directory group policies**. Kaspersky Endpoint Security se instalează cu ajutorul Agentului de rețea sau, manual, prin intermediul Active Directory. Pentru a instala Agentul de rețea, activitatea de instalare la distanță trebuie executată cu privilegii de administrator de domeniu.

9. Dacă este necesar, bifați caseta de selectare **Prompt users to close running applications**. Instalarea aplicației Kaspersky Endpoint Security consumă resurse ale computerului. Pentru comoditatea utilizatorului, Expertul de instalare a aplicației îți solicită să închizi aplicațiile care se execută înainte de a începe instalarea. Acest lucru ajută la prevenirea perturbărilor în funcționarea altor aplicații și previne posibile funcționări defectuoase ale computerului.

10. În blocul **Behavior for devices managed through other Administration Servers**, selectați metoda de instalare a aplicației Kaspersky Endpoint Security. Dacă rețeaua are instalate mai multe Servere de administrare, aceste Servere de administrare pot vedea aceleași computere client. Acest lucru poate cauza, de exemplu, instalarea de mai multe ori la distanță a unei aplicații pe același computer client prin intermediul unor Servere de administrare diferite sau alte conflicte.

Pasul 4. Selectarea contului pentru executarea activității

Selectați contul pentru instalarea Agentului de rețea folosind instrumentele din sistemul de operare. În acest caz, sunt necesare drepturi de administrator pentru accesul la computer. Poți adăuga mai multe conturi. Dacă un cont nu are drepturi suficiente, Expertul de instalare utilizează următorul cont. Dacă instalezi Kaspersky Endpoint Security utilizând instrumentele Agentului de rețea, nu este necesar să selectezi un cont.

Pasul 5. Finalizarea creării activității

Termină expertul făcând clic pe butonul **Finish**. Se va afișa o activitate nouă în lista de activități. Pentru a executa o activitate, bifează caseta de selectare de lângă activitate și fă clic pe butonul **Start**. Aplicația va fi instalată în modul silențios. După instalare, pictograma va fi adăugată în zona de notificare a computerului utilizatorului. Dacă pictograma arată așa , asigurați-vă că ați activat aplicația.

Instalarea locală a aplicației folosind Expertul

Interfața aplicației Expert de configurare constă dintr-o secvență de ferestre corespunzătoare pașilor de instalare a aplicației. Asigură-te că contul de utilizator sub care execuți Expertul de configurare face parte din grupul de administratori.

Pentru a instala aplicația sau pentru a efectua un upgrade al aplicației de la o versiune anterioară folosind Expertul de instalare:

1. Copiați folderul kitului de distribuire pe computerul utilizatorului.

2. Rulați setup_kes.exe.

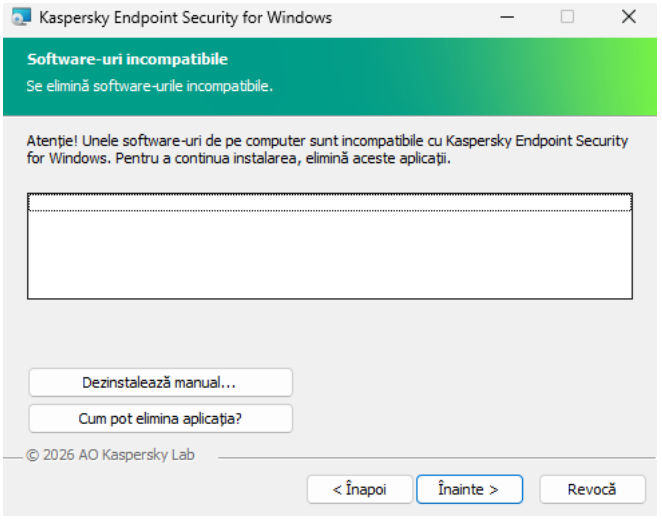
   Expertul de instalare pornește.

Pregătirea pentru instalare

Înainte de a instala Kaspersky Endpoint Security pe un computer sau de a face upgrade de la o versiune anterioară, trebuie verificate următoarele condiții:

- Dacă există vreun program instalat care ar putea avea probleme de compatibilitate cu Kaspersky Endpoint Security (lista programelor este disponibilă în fișierul incompatible.txt care este inclus în kitul de distribuție).
- Sunt sau nu îndeplinite cerințele hardware și software.
- Dacă Microsoft .NET Framework este instalat.
- Dacă utilizatorul are sau nu drepturile de a instala produsul software.

Dacă nu sunt îndeplinite toate cerințele anterioare, o notificare relevantă este afișată pe ecran. De exemplu, o notificare despre un software incompatibil (vezi figura de mai jos).



Eliminarea software-ului incompatibil

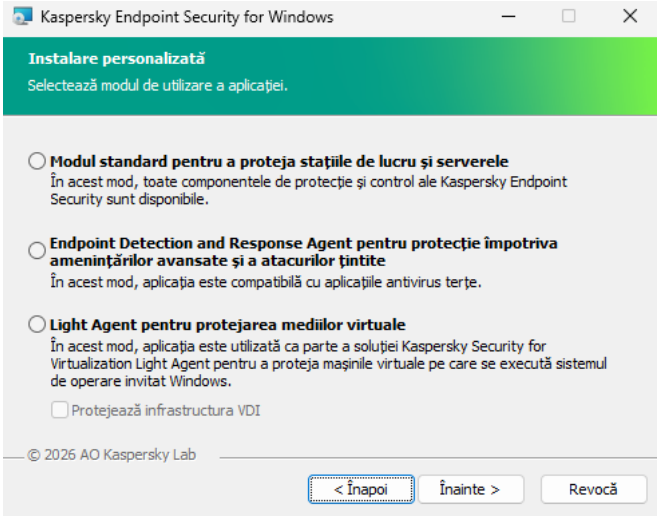
Dacă sunt îndeplinite condițiile prezentate, Expertul de instalare caută aplicații Kaspersky care ar putea conduce la conflicte atunci când sunt executate în același timp cu aplicația care este instalată. Dacă sunt găsite astfel de aplicații, ți se solicită eliminarea lor manuală.

Dacă aplicațiile detectate includ versiuni anterioare ale Kaspersky Endpoint Security, toate datele care pot fi migrate (cum ar fi datele de activare și setările pentru aplicații) sunt reținute și utilizate la instalarea Kaspersky Endpoint Security 14.1 for Windows, iar versiunea anterioară a aplicației este eliminată automat. Acest lucru este aplicabil pentru următoarele versiuni ale aplicației:

- Kaspersky Endpoint Security 12.1 for Windows (versiunea 12.1.0.506)
- Kaspersky Endpoint Security 12.2 for Windows (versiunea 12.2.0.462)
- Kaspersky Endpoint Security 12.3 for Windows (versiunea 12.3.0.493)
- Kaspersky Endpoint Security 12.4 for Windows (versiunea 12.4.0.467)
- Kaspersky Endpoint Security 12.5 for Windows (versiunea 12.5.0.539)
- Kaspersky Endpoint Security 12.6 for Windows (versiunea 12.6.0.438)

- Kaspersky Endpoint Security 12.7 for Windows (versiunea 12.7.0.533)
- Kaspersky Endpoint Security 12.8 for Windows (versiunea 12.8.0.505)
- Kaspersky Endpoint Security 12.9 for Windows (versiunea 12.9.0.384)
- Kaspersky Endpoint Security 12.10 for Windows (versiunea 12.10.0.466)
- Kaspersky Endpoint Security 12.11 for Windows (versiunea 12.11.0.637)
- Kaspersky Endpoint Security 12.12 for Windows (versiunea 12.12.0.522)
- Kaspersky Endpoint Security 14.0 for Windows (versiunea 14.0.0.504)

Configurarea Kaspersky Endpoint Security



Alegerea configurației aplicației

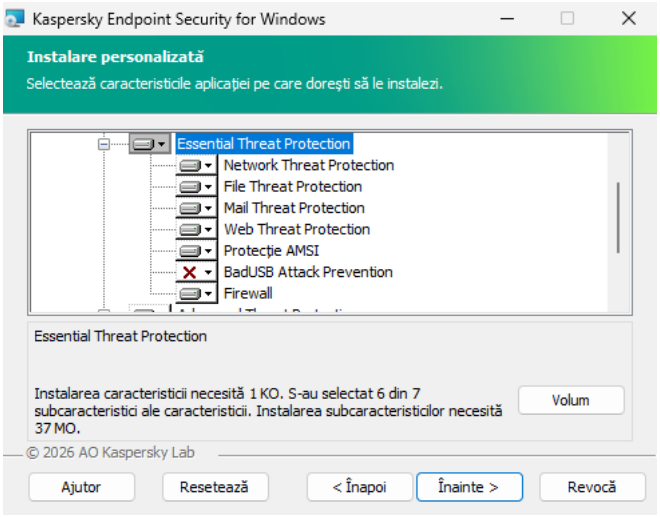
Modul Standard. Configurația implicită. Această configurație vă permite să utilizați toate componentele aplicației, inclusiv componentele care oferă suport pentru soluțiile Detection and Response. Această configurație este utilizată pentru protecția completă a computerului împotriva unei varietăți de amenințări, atacuri de rețea și fraude.

Endpoint Detection and Response Agent. În această configurație, puteți instala doar componentele care oferă suport pentru soluțiile Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), precum și KUMA. Această configurație este necesară dacă o platformă Endpoint Protection Platform (EPP) terță este implementată în organizație împreună cu soluția Kaspersky Detection and Response. Acest lucru face ca Kaspersky Endpoint Security în configurația Endpoint Detection and Response Agent să fie compatibil cu aplicațiile EPP terțe.

Light Agent pentru protejarea mediilor virtuale. Această configurație este destinată aplicației care este utilizată ca parte a soluției Kaspersky Security for Virtualization Light Agent. Light Agent trebuie instalat pe fiecare mașină virtuală care trebuie protejată folosind soluția. În această configurație, nu puteți utiliza componentele Data Encryption sau Control adaptiv al anomaliilor. Dacă instalezi Light Agent pe un șablon de mașină virtuală care va fi folosit pentru a crea *mașini virtuale non-persistente*, bifează caseta de selectare **Protejează infrastructura VDI** (VDI înseamnă Virtual Desktop Infrastructure). Modul de protecție VDI ajută la optimizarea performanței Kaspersky Endpoint Security pe mașinile virtuale non-persistente. În acest mod, Light Agent refuză actualizările aplicației care necesită repornirea mașinii virtuale. Când se primesc actualizări ale aplicației care necesită o repornire, Light Agent generează un eveniment despre necesitatea actualizării șablonului mașinilor virtuale protejate.

Componentele Kaspersky Endpoint Security

În timpul procesului de instalare poți selecta componentele Kaspersky Endpoint Security pe care vrei să le instalezi (vezi figura de mai jos). Componenta File Threat Protection trebuie să fie instalată în mod obligatoriu. Nu poți anula instalarea ei.



Selectarea componentelor aplicației de instalat

În mod implicit sunt selectate spre instalare toate componentele aplicației, cu excepția următoarelor:

- BadUSB Attack Prevention.
- Componente Data Encryption.
- Componente Detection and Response.

Puteți schimba componentele disponibile ale aplicației după instalarea aplicației. Pentru a face acest lucru, trebuie să executați din nou Expertul de configurare și să alegeți să schimbați componentele disponibile.

Dacă trebuie să instalați componentele Detection and Response, Kaspersky Endpoint Security acceptă următoarele configurări:

- Doar Endpoint Detection and Response Optimum
- Doar Endpoint Detection and Response Expert (cloud)
- Doar Endpoint Detection and Response Expert (on-premises)
- Doar Network Detection and Response (KATA)
- Doar Sandbox
- Endpoint Detection and Response Optimum și Sandbox
- Endpoint Detection and Response Expert (cloud) și Sandbox
- Endpoint Detection and Response Expert (on-premises) și Sandbox

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

Kaspersky Endpoint Security verifică selecția de componente înainte de instalarea aplicației. În cazul în care configurația selectată a componentelor Detection and Response cnu este acceptată, Kaspersky Endpoint Security nu poate fi instalat.

Selectarea directorului pentru instalarea aplicației

Poți schimba calea de instalare a aplicației Kaspersky Endpoint Security pe un computer client. În mod implicit, aplicația este instalată în directorul `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.1`.

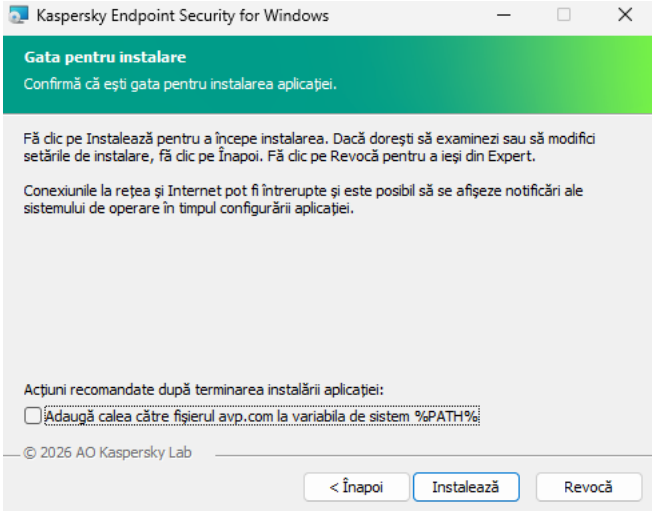
Configurarea zonei de încredere

Începând cu Kaspersky Endpoint Security 12.6 for Windows, excluderile de scanare și aplicații de încredere sunt adăugate la zona de încredere. Excluderile de la scanare și aplicațiile de încredere predefinite ajută la configurarea rapidă a Kaspersky Endpoint Security pe serverele SQL, serverele Microsoft Exchange și System Center Configuration Manager. Aceasta înseamnă că nu trebuie să configurați manual o zonă de încredere pentru aplicație pe servere.

Începând cu Kaspersky Endpoint Security 12.8 for Windows, poți instala aplicația în modul Light Agent pentru a proteja mediile virtuale. Excluderile de la scanare predefinite și aplicațiile de încredere te pot ajuta să configurezi rapid Kaspersky Endpoint Security în mediile virtuale Citrix și VMware.

De asemenea, poți configura zona de încredere mai târziu, în proprietățile politicii: excluderi de la scanare și aplicații de încredere.

Setări avansate



Setări avansate pentru instalarea aplicației

Protejează procesul de instalare a aplicației. Protejarea instalării include protecția împotriva înlocuirii pachetului de distribuție cu aplicații rău intenționate, blocarea accesului la directorul de instalare al aplicației Kaspersky Endpoint Security și blocarea accesului la secțiunea de registre a sistemului care conține cheile aplicației. Cu toate acestea, dacă aplicația nu poate fi instalată (de exemplu, atunci când se execută o instalare la distanță cu ajutorul Windows Remote Desktop), te sfătuim să dezactivezi protecția procesului de instalare.

Asigură compatibilitatea cu Citrix PVS. Poți activa suportul pentru Citrix Provisioning Services pentru a instala aplicația Kaspersky Endpoint Security pe o mașină virtuală.

Adaugă calea către fișierul avp.com la variabila de sistem %PATH%. Poți adăuga calea de instalare la variabila %PATH% pentru utilizarea comodă a interfeței liniei de comandă.

Instalarea la distanță a aplicației folosindu-se System Center Configuration Manager

Aceste instrucțiuni se aplică pentru System Center Configuration Manager 2012 R2.

Pentru a instala la distanță o aplicație folosind System Center Configuration Manager:

1. Deschide consola Configuration Manager.
2. În dreapta consolei, în blocul **App management**, selectați **Pachete**.
3. În partea de sus a consolei, în panoul de control, faceți clic pe butonul **Create package**.
   Este lansat *Expert pachet nou și aplicație*.
4. În Expert pachet nou și aplicație:
   a. În secțiunea **Package**:
      - În câmpul **Name**, introdu numele pachetului de instalare.
      - În câmpul **Source folder**, specificați o cale către directorul care conține pachetul de distribuție al Kaspersky Endpoint Security.
   b. În secțiunea **Application type**, selectați opțiunea **Standard program**.
   c. În secțiunea **Standard program**:
      - În câmpul **Name**, introdu numele unic pentru pachetul de instalare (de exemplu, numele aplicației, inclusiv versiunea).
      - În câmpul **Command line**, specifică opțiunile de instalare din linia de comandă pentru Kaspersky Endpoint Security.
      - Faceți clic pe butonul **Browse** pentru a introduce o cale către fișierul executabil al aplicației.
      - Asigură-te că în lista **Mod executare** este selectat elementul **Run with administrative rights**.

d. În secțiunea **Requirements**:

- Bifați caseta de selectare **Run another program first** dacă dorești ca o altă aplicație să fie pornită înainte de a instala Kaspersky Endpoint Security.

  Selectați aplicația din lista verticală **Application** sau specifică o cale către fișierul executabil al acestei aplicații făcând clic pe butonul **Browse**.

- Selectați opțiunea **This program can run only on specified platforms** în blocul **Platform requirements**, dacă doriți ca aplicația să fie instalată numai pe sistemele de operare specificate.

  În lista de mai jos, bifați casetele de selectare de lângă sistemele de operare pe care va fi instalat Kaspersky Endpoint Security.

Acest pas este opțional.

e. În secțiunea **Summary**, verifică toate valorile introduse pentru setări și faceți clic pe **Next**.

Pachetul de instalare creat va apărea în secțiunea **Packages**, în lista de pachete de instalare disponibile.

5. În meniul contextual al pachetului de instalare, selectați **Deploy**.

   Această acțiune pornește *Expertul de implementare*.

6. În Expertul de implementare:

   a. În secțiunea **General**:

   - În câmpul **Software**, introdu numele unic al pachetului de instalare sau selectați pachetul de instalare din listă făcând clic pe butonul **Browse**.

   - În câmpul **Collection**, introdu numele colecției de computere pe care va fi instalată aplicația sau selectați colecția făcând clic pe butonul **Browse**.

   b. În secțiunea **Contains**, adaugă puncte de distribuție (pentru informații mai detaliate, consultați documentația de ajutor pentru System Center Configuration Manager).

   c. Dacă este nevoie, specifică valorile pentru alte setări în Expertul de implementare. Aceste setări sunt opționale pentru instalarea la distanță a Kaspersky Endpoint Security.

   d. În secțiunea **Summary**, verifică toate valorile introduse pentru setări și faceți clic pe **Next**.

   După finalizarea Expertului de implementare, va fi creată o activitate pentru instalarea la distanță a Kaspersky Endpoint Security.

Descrierea setărilor fișierului setup.ini

Fișierul setup.ini este folosit atunci când se instalează aplicația din linia de comandă sau se folosește Editorul de politică de grup din Microsoft Windows. Pentru a aplica setări din fișierul setup.ini, plasează acest fișier în directorul care conține pachetul de distribuție Kaspersky Endpoint Security.

Utilizează fișierul setup.ini numai atunci când instalezi aplicația în modul silențios.

Nu poți adăuga o cale la fișierul de configurare install.cfg din fișierul setup.ini. Aplicația omite, de asemenea, fișierul de configurare install.cfg dacă este plasat în același director cu kitul de distribuție Kaspersky Endpoint Security. Pentru a aplica setările din fișierul de configurare install.cfg, trebuie să specifici calea către fișier în următoarea comandă de instalare a aplicației: `CONFIGPATH=<path to the configuration file>`.

DESCARCAȚI FIȘUL SETUP.INI

Fișierul setup.ini constă din următoarele secțiuni:

- `[Setup]` – setări generale ale instalării aplicației.
- `[Components]` – selectarea componentelor aplicației ce trebuie instalate în modul Standard. Dacă niciuna dintre componente nu este specificată, sunt instalate toate componentele disponibile pentru sistemul de operare. File Threat Protection este o componentă obligatorie și se instalează pe computer indiferent de setările indicate în această secțiune.
- `[Tasks]` – selecție a activităților care vor fi incluse în lista de activități Kaspersky Endpoint Security. Dacă nu este specificată nicio activitate, sunt incluse toate activitățile din lista de activități a Kaspersky Endpoint Security.

Alternativele la valoare `1` sunt valorile `yes`, `on`, `enable`, `enabled` și `true`. Alternativele la valoare `0` sunt valorile `no`, `off`, `disable`, `disabled` și `false`.

Setări ale fișierului setup.ini file

Secțiune	Parametru	Descriere
`[Setup]`	`InstallDir`	Calea către directorul de instalare a aplicației.
	`ActivationCode`	Codul de activare pentru Kaspersky Endpoint Security.
	`Eula`	Acceptarea termenilor Acordului de licență pentru utilizatorul final. Textul Acordului de licență este inclus în kitul de distribuire al Kaspersky Endpoint Security. Acceptarea termenilor Acordului de licență pentru utilizatorul final este necesară pentru instalarea aplicației sau pentru efectuarea unui upgrade la versiunea aplicației.

Secțiune	Parametru	Descriere
	`PrivacyPolicy`	Acceptarea Politicii de confidențialitate. Textul Politicii de confidențialitate este inclus în kitul de distribuire Kaspersky Endpoint Security. Pentru a instala aplicația sau pentru a face upgrade la versiunea aplicației, trebuie să acceptați Politica de confidențialitate.
	`KSN`	Acordul sau refuzul de a participa în Kaspersky Security Network (KSN). Dacă pentru acest parametru nu este setată nicio valoare, Kaspersky Endpoint Security vă va solicita să confirmați consimțământul sau refuzul de a participa la KSN la prima pornire a aplicației Kaspersky Endpoint Security. Valori disponibile: • `1` – acord de participare la KSN. • `0` – refuz de a participa la KSN (valoare implicită). Pachetul de distribuție Kaspersky Endpoint Security este optimizat pentru utilizare cu Kaspersky Security Network. Dacă ați optat să nu participați la Kaspersky Security Network, trebuie să actualizați Kaspersky Endpoint Security imediat după finalizarea instalării.
	`CLEANERSIGNCHECK`	Verificarea semnăturilor digitale ale fișierelor software detectate din lista incompatible.txt. Pentru a elimina software-ul, Kaspersky Endpoint Security rulează fișierul de instalare a software-ului. Dacă fișierul de instalare nu are o semnătură digitală, Kaspersky Endpoint Security consideră că fișierul nu este de încredere și oprește eliminarea software-ului pentru a evita executarea unui cod potențial rău intenționat. Dacă aplicația nu poate verifica semnătura digitală a fișierului software-ului detectat, instalarea Kaspersky Endpoint Security este oprită cu o eroare. Valoarea implicită este diferită, în funcție de metoda de instalare a software-ului: • `0` înseamnă că verificarea semnăturii digitale este dezactivată (valoarea implicită, dacă este implementată prin Kaspersky Security Center). • `1` înseamnă că verificarea semnăturii digitale este activată (valoarea implicită, dacă aplicația este instalată local).
	`Login`	Setează numele de utilizator pentru accesarea caracteristicilor și setărilor aplicației Kaspersky Endpoint Security (componenta Protecție prin parolă). Numele de utilizator se setează împreună cu setările `Password` și `PasswordArea`. În mod implicit este utilizat numele de utilizator KLAdmin.
	`Password`	Specifică o parolă pentru accesarea funcțiilor și setărilor Kaspersky Endpoint Security (parola este specificată împreună cu parametrii `Login` și `PasswordArea`). Dacă ai specificat o parolă, însă nu ai specificat un număr de utilizator cu parametrul `Login`, se utilizează în mod implicit numele de utilizator KLAdmin.
	`PasswordArea`	Specifică domeniul parolei pentru accesarea aplicației Kaspersky Endpoint Security. Atunci când un utilizator încearcă să efectueze o acțiune care este inclusă în acest domeniu, Kaspersky Endpoint Security solicită acreditările contului utilizatorului (parametrii `Login` și `Password`). Folosiți caracterul `;` pentru a specifica mai multe valori. Valori disponibile: • `SET` – modificare a setărilor aplicației. • `EXIT` – ieșire din aplicație. • `DISPROTECT` – dezactivare a componentelor protecției și oprire a activităților de scanare. • `DISPOLICY` – dezactivare a politicii Kaspersky Security Center. • `UNINST` – eliminare a aplicației de pe computer. • `DISCTRL` – dezactivare a componentelor de control. • `REMOVELIC` – eliminare a cheii. • `REPORTS` – vizualizare a rapoartelor. • `EXPORT` – exportarea setărilor aplicației. De exemplu, `PasswordArea=SET;PasswordArea=UNINST;PasswordArea=EXIT`.
	`SelfProtection`	Activează sau dezactivează mecanismul de protecție a instalării aplicației. Valori disponibile: • `1` – mecanismul de protecție a instalării aplicației este activat (valoare implicită). • `0` – mecanismul de protecție a instalării aplicației este dezactivat. Protejarea instalării include protecția împotriva înlocuirii pachetului de distribuție cu aplicații rău intenționate, blocarea accesului la directorul de instalare al aplicației Kaspersky Endpoint Security și blocarea accesului la secțiunea de registre a sistemului care conține cheile aplicației. Cu toate acestea, dacă aplicația nu poate fi instalată (de exemplu, atunci când se execută o instalare la distanță cu ajutorul Windows Remote Desktop), te sfătuim să dezactivezi protecția procesului de instalare.

Secțiune	Parametru	Descriere
	PROTECTOSSERVICES	Protecția funcționalității serviciilor sistemului de operare. Protecția serviciilor sistemului de operare împiedică aplicațiile terțe să interfereze cu funcționarea serviciilor sistemului de operare. Printre aceste servicii se numără, de exemplu, serviciul de pornire automată a aplicațiilor. • 1 înseamnă că protecția serviciilor sistemului de operare este activată (valoare implicită). • 0 înseamnă că protecția serviciilor sistemului de operare este dezactivată.
	EnableAzureSupport	Activarea sau dezactivarea modului de compatibilitate Azure WVD. Valori disponibile: • 1 – Modul de compatibilitate Azure WVD este activat. • 0 – Modul de compatibilitate Azure WVD este dezactivat (valoare implicită). Această funcție asigură afișarea corectă a stării mașinii virtuale Azure în consola Kaspersky Anti Targeted Attack Platform. Pentru a monitoriza performanța computerului, Kaspersky Endpoint Security trimite date de telemetrie către serverele KATA. Telemetria include un ID al computerului (Sensor ID). Modul de compatibilitate Azure WVD permite alocarea unui Sensor ID unic permanent către aceste mașini virtuale. Dacă modul de compatibilitate este dezactivat, Sensor ID se poate schimba după ce computerul este repornit din cauza modului în care funcționează mașinile virtuale Azure. Acest lucru poate face ca duplicate ale mașinilor virtuale să apară pe consolă.
	Reboot	Se repornește automat computerul, dacă este necesar, după instalarea sau upgrade-ul aplicației. Dacă nu este setată nicio valoare pentru acest parametru, repornirea automată a computerului este blocată. Repornirea nu este necesară atunci când instalezi Kaspersky Endpoint Security. Repornirea este necesară numai dacă trebuie să elimini aplicații incompatibile înainte de instalare. Repornirea poate fi necesară și atunci când actualizezi versiunea aplicației.
	AddEnvironment	Se adaugă la variabila de sistem %PATH% calea către fișierele executabile localizate în directorul de instalare pentru Kaspersky Endpoint Security. Valori disponibile: • 1 – la variabila de sistem %PATH% se adaugă calea către fișierele executabile localizate în directorul de instalare pentru Kaspersky Endpoint Security. • 0 – la variabila de sistem %PATH% nu se adaugă calea către fișierele executabile localizate în directorul de instalare pentru Kaspersky Endpoint Security.
	AMPPL	Activează sau dezactivează protecția proceselor aplicației Kaspersky Endpoint Security folosind tehnologia AM-PPL (Antimalware Protected Process Light). Pentru mai multe detalii despre tehnologia AM-PPL, vizitați site-ul web Microsoft. Tehnologia AM-PPL este disponibilă pentru Windows 10 versiunea 1703 (RS2) sau ulterioară și pentru sistemele de operare Windows Server 2019. Valori disponibile: • 1 – protecția proceselor aplicației Kaspersky Endpoint Security folosindu-se tehnologia AM-PPL este activată. • 0 – protecția proceselor aplicației Kaspersky Endpoint Security folosindu-se tehnologia AM-PPL este dezactivată.
	UPGRADEMODE	Mod upgrade aplicație: • Seamless înseamnă efectuarea upgrade-ului aplicației cu repornirea computerului (valoare implicită) • Force înseamnă efectuarea upgrade-ului aplicației fără repornire. Poți efectua upgrade-ul aplicației fără repornire începând cu versiunea 11.10.0. Pentru a efectua upgrade-ul unei versiuni anterioare a aplicației, trebuie să repornești computerul. De asemenea, poți instala corecții fără repornire începând cu versiunea 11.11.0. Repornirea nu este necesară atunci când instalezi Kaspersky Endpoint Security. Așadar, modul de actualizare a aplicației va fi specificat în setările aplicației. Poți modifica acest parametru în setările aplicației sau în politică. Când upgrade-ul a instalat deja aplicația, prioritatea parametrului specificat în fișierul setup.ini este mai mare decât cea a parametrului specificat în setările aplicației sau în linia de comandă. De exemplu, dacă modul de upgrade Force este specificat în fișierul setup.ini și modul Seamless este specificat în setările aplicației, upgrade-ul va fi instalat fără repornirea computerului (Force). Dacă folosești fișierul setup.ini, atunci când parametrul UPGRADEMODE nu este specificat, programul de instalare va utiliza o valoare implicită (Seamless) și va instala upgrade-ul fără repornirea computerului.
	SetupReg	Activează scrierea de chei de registru din fișierul setup.reg în registru. Valoarea parametrului SetupReg: setup.reg.
	EnableTraces	Activarea sau dezactivarea urmăririi aplicațiilor. După ce pornește Kaspersky Endpoint Security, acesta salvează fișierele de urmărire în directorul %ProgramData%\Kaspersky Lab\KES.14.1\Traces. Valori disponibile: • 1 – urmărirea este activată. • 0 – urmărirea este dezactivată (valoare implicită).

Secțiune	Parametru	Descriere
	`TracesLevel`	Nivelul de detaliere a urmăririi. Valori disponibile: • `100` (critic). Numai mesaje despre erorile fatale. • `200` (ridicat). Mesaje despre toate erorile, inclusiv erorile fatale. • `300` (diagnosticare). Mesaje despre toate erorile, precum și avertismente. • `400` (important). Toate mesajele de eroare, avertismentele și informațiile suplimentare. • `500` (normal). Mesaje despre toate erorile și avertismentele, precum și informații detaliate despre funcționarea aplicației în modul normal (implicit). • `600` (scăzut). Toate mesajele.
	`RESTAPI`	Gestionarea aplicației prin API REST. Pentru a gestiona aplicația prin API REST, trebuie să specificați numele de utilizator (parametrul `RESTAPI_User`). Valori disponibile: • `1` - gestionarea prin API REST este permisă. • `0` - gestionarea prin API REST este blocată (valoarea implicită). Pentru a gestiona aplicația prin API REST, trebuie să fie permisă gestionarea folosind sisteme administrative. Pentru a face acest lucru, setați parametrul `AdminKitConnector=1`. Dacă gestionați aplicația prin API REST, este imposibil să gestionați aplicația folosind sistemele de administrare ale Kaspersky.
	`RESTAPI_User`	Numele de utilizator al contului domeniului Windows utilizat pentru gestionarea aplicației prin API REST. Gestionarea aplicației prin API REST este disponibilă numai pentru acest utilizator. Introduceți numele de utilizator în formatul `<DOMAIN>\<UserName>` (de exemplu, `RESTAPI_User=COMPANY\Administrator`). Puteți selecta un singur utilizator pentru a lucra cu API REST. Adăugarea unui nume de utilizator este o condiție necesară pentru gestionarea aplicației prin API REST.
	`RESTAPI_Port`	Port utilizat pentru gestionarea aplicației prin API REST. Portul 6782 este folosit în mod implicit. Asigurați-vă că portul este liber.
	`RESTAPI_Certificate`	Certificat pentru identificarea solicitărilor (de exemplu, `RESTAPI_Certificate=C:\cert.pem`). Interacțiunea sigură a Kaspersky Endpoint Security cu clientul REST necesită configurarea identificării solicitării. Pentru aceasta, trebuie să instalați un certificat și ulterior să semnați sarcina fiecărei solicitări.
	`StandaloneMode`	Instalarea aplicației în modul Endpoint Detection and Response Agent (EDR Agent). *Endpoint Detection and Response Agent* este o aplicație care este instalată pe stațiile de lucru și pe serverele individuale din infrastructura IT a organizației pentru a susține soluțiile Kaspersky Managed Detection and Response și Kaspersky Anti Targeted Attack Platform. EDR Agent este compatibil cu aplicațiile EPP terțe. Acest lucru vă permite să utilizați instrumente de securitate ale infrastructurii terțe alături de Detection and Response de la Kaspersky. Pentru a instala EDR Agent, în secțiunea `[Components]`, selectează componentele `StandaloneKATA`, `StandaloneNDR` sau `StandaloneMDR`. EDR Agent nu acceptă alte componente altei aplicații. Valori disponibile: • `1` pentru a instala aplicația în modul EDR Agent. • `0` pentru a instala aplicația în modul Standard (implicit).
	`KSVLAMode`	Instalarea aplicației în modul Light Agent. Această configurație este destinată aplicației care este utilizată ca parte a soluției Kaspersky Security for Virtualization Light Agent. Light Agent trebuie instalat pe fiecare mașină virtuală care trebuie protejată folosind soluția. Valori disponibile: • `1` pentru a instala aplicația în modul Light Agent. • `0` pentru a instala aplicația în modul Standard (implicit).
	`InstallOnVDI`	Activarea modului de protecție VDI la instalarea aplicației în modul Light Agent (`KSVLAMode=1`). Modul de protecție VDI ajută la optimizarea performanței Kaspersky Endpoint Security pe mașinile virtuale non-persistente. În acest mod, Light Agent refuză actualizările aplicației care necesită repornirea mașinii virtuale. Când se primesc actualizări ale aplicației care necesită o repornire, Light Agent generează un eveniment despre necesitatea actualizării șablonului mașinilor virtuale protejate. Valori disponibile: • `1` pentru a activa modul de protecție VDI. • `0` pentru a dezactiva modul de protecție VDI (implicit).

Secțiune	Parametru	Descriere
	`KESExclusions`	Adăugarea excluderilor de la scanare predefinite și a aplicațiilor de încredere la instalarea aplicației pe server. Excluderile de la scanare și aplicațiile de încredere predefinite ajută la configurarea rapidă a Kaspersky Endpoint Security pe serverele SQL, serverele Microsoft Exchange și System Center Configuration Manager. De exemplu, excluderile de scanare predefinite pentru serverele SQL includ fișiere de baze de date MDF și LDF. Aceasta înseamnă că nu trebuie să configurați manual o zonă de încredere pentru aplicație pe servere. Valori disponibile: • `1` activează excluderile de la scanare predefinite și aplicațiile de încredere. • `0` dezactivează excluderile de la scanare predefinite și aplicațiile de încredere (implicit).
	`LAExclusions`	Adăugarea excluderilor de la scanare și a aplicațiilor de încredere la instalarea aplicației pe o mașină virtuală (modul Light Agent). Excluderile de la scanare predefinite și aplicațiile de încredere te pot ajuta să configurezi rapid Kaspersky Endpoint Security în mediile virtuale Citrix și VMware. Valori disponibile: • `1` activează excluderile de la scanare predefinite și aplicațiile de încredere. • `0` dezactivează excluderile de la scanare predefinite și aplicațiile de încredere (implicit).
	`EnableUniqueSensorID`	Crearea unui identificator unic de computer (Sensor ID) în timpul instalării sau actualizării aplicației. Sensor ID este utilizat în soluția Kaspersky Anti Targeted Attack Platform pentru a identifica computerele care trimit telemetrie către server. La crearea unui Sensor ID, aplicația folosește un algoritm care ține cont de configurația computerului, cum ar fi numărul de serie al plăcii de bază. În unele cazuri, de exemplu, când se utilizează aplicația într-un mediu virtual, Sensor ID poate fi duplicat. Ca urmare, Kaspersky Anti Targeted Attack Platform nu poate identifica computerul de pe care este trimisă telemetria. Pentru a crea un Sensor ID unic, trebuie să setezi parametrul `EnableUniqueSensorID=1`. Ca urmare, aplicația va folosi un alt algoritm pentru a crea Sensor ID, care ia în considerare și alte date despre computer. Acest lucru asigură un identificator Sensor ID unic. În mod implicit, parametrul nu este setat. Aplicația moștenește identificatorul Sensor ID în următoarele cazuri: • actualizarea versiunii aplicației; • migrarea configurării [KES+KEA] la [KES+built-in agent]. Ca parte a procesului de reparare a aplicației, programul de instalare încearcă să moștenească Sensor ID. Dacă Sensor ID nu poate fi restaurat, aplicația creează un nou Sensor ID.
	`CitrixCompatibility`	Activarea suportului pentru Citrix Provisioning Services pentru a instala aplicația Kaspersky Endpoint Security pe o mașină virtuală.
`[Components]`	`ALL`	Instalare a tuturor componentelor. Dacă este specificată valoarea `1` pentru acest parametru, vor fi instalate toate componentele, indiferent de setările de instalare ale componentelor individuale. Având în vedere modul în care sunt acceptate soluțiile Detection and Response, componentele Endpoint Detection and Response Optimum și Sandbox sunt instalate pe computer. Componenta Endpoint Detection and Response Expert (cloud) nu este compatibilă cu această configurație.
	`MailThreatProtection`	Mail Threat Protection.
	`WebThreatProtection`	Web Threat Protection.
	`AMSI`	Protecție AMSI.
	`HostIntrusionPrevention`	Host Intrusion Prevention.
	`BehaviorDetection`	Behavior Detection.
	`ExploitPrevention`	Exploit Prevention.
	`RemediationEngine`	Remediation Engine.
	`Firewall`	Firewall.
	`NetworkThreatProtection`	Network Threat Protection.
	`WebControl`	Control Web.
	`DeviceControl`	Control dispozitive.

Secțiune	Parametru	Descriere
	`ApplicationControl`	Application Control.
	`AdaptiveAnomaliesControl`	Control adaptiv al anomaliilor.
	`CloudDiscovery`	Cloud Discovery.
	`LogInspector`	Inspecție jurnal
	`AntiCryptor`	Anti-Cryptor
	`FileThreatProtection`	File Threat Protection.
	`SystemIntegrityMonitor`	Monitorizare integritate sistem.
	`FileEncryption`	Biblioteci File Level Encryption.
	`DiskEncryption`	Biblioteci Full Disk Encryption.
	`MSBitLocker`	Biblioteci de gestionare a criptării BitLocker.
	`BadUSBAttackPrevention`	BadUSB Attack Prevention.
	`EDR`	Endpoint Detection and Response Optimum Componenta nu este compatibilă cu componentele Endpoint Detection and Response Expert (cloud) (`EDRCloud`) și Endpoint Detection and Response Expert (on-premises) (`AntiAPT`).
	`EDRCloud`	Endpoint Detection and Response Expert (cloud) Componenta nu este compatibilă cu componentele Endpoint Detection and Response Optimum (`EDR`) și Endpoint Detection and Response Expert (on-premises) (`AntiAPT`).
	`AntiAPT`	Endpoint Detection and Response Expert (on-premises) Componenta nu este compatibilă cu componentele Endpoint Detection and Response Expert (cloud) (`EDRCloud`) și Endpoint Detection and Response Optimum (`EDR`).
	`SB`	Kaspersky Sandbox sau KATA Sandbox. *Kaspersky Sandbox* este o soluție autonomă Detection and Response de la Kaspersky. *KATA Sandbox* este o componentă a soluției Kaspersky Anti Targeted Attack Platform.
	`MDR`	Managed Detection and Response
	`NDR`	Network Detection and Response (KATA) Componenta nu este compatibilă cu componentele Endpoint Detection and Response Expert (cloud) (`EDRCloud`) și Endpoint Detection and Response Optimum (`EDR`).
	`AdminKitConnector`	Gestionarea aplicațiilor folosind sisteme de administrare. Sistemele de administrare includ, de exemplu, Kaspersky Security Center. Pe lângă sistemele de administrare Kaspersky, puteți utiliza soluții terțe. Kaspersky Endpoint Security oferă o API în acest scop. Valori disponibile: • `1` - gestionarea aplicațiilor cu ajutorul sistemelor de administrare este permisă (valoare implicită). • `0` - gestionarea aplicațiilor este permisă doar prin interfața locală.
	`KUMAIntegration`	Integrare cu KUMA
	`StandaloneKATA`	Instalarea aplicației în modul Endpoint Detection and Response Agent (EDR Agent) pentru integrarea cu soluția Kaspersky Anti Targeted Attack Platform (EDR).

Secțiune	Parametru	Descriere
	`StandaloneMDR`	Instalarea aplicației în modul Endpoint Detection and Response Agent (EDR Agent) pentru integrarea cu Kaspersky Managed Detection and Response.
	`StandaloneNDR`	Instalarea aplicației în modul Endpoint Detection and Response Agent (EDR Agent) pentru integrarea cu soluția Kaspersky Anti Targeted Attack Platform (NDR).
	`StandaloneSiemTelemetry`	Instalarea aplicației în modul Endpoint Detection and Response Agent (EDR Agent) pentru integrarea cu soluția KUMA.
`[Tasks]`	`ScanMyComputer`	Activitate de scanare completă. Valori disponibile: • `1` – activitatea este inclusă în lista de activități Kaspersky Endpoint Security. • `0` – activitatea nu este inclusă în lista de activități Kaspersky Endpoint Security.
	`ScanCritical`	Activitate de scanare a zonelor critice. Valori disponibile: • `1` – activitatea este inclusă în lista de activități Kaspersky Endpoint Security. • `0` – activitatea nu este inclusă în lista de activități Kaspersky Endpoint Security.
	`Updater`	Activitate de actualizare. Valori disponibile: • `1` – activitatea este inclusă în lista de activități Kaspersky Endpoint Security. • `0` – activitatea nu este inclusă în lista de activități Kaspersky Endpoint Security.

Modificare componente ale aplicației

În timpul instalării aplicației, puteți selecta componentele care vor fi disponibile. Puteți modifica componentele disponibile ale aplicației în următoarele moduri:

- Local, folosind Expertul de configurare.

  Componentele aplicațiilor sunt modificate folosind metoda normală pentru un sistem de operare Windows, care se face prin Control Panel. Executați Expertul de configurare a aplicațiilor și selectați opțiunea pentru a schimba componentele aplicației care sunt disponibile. Urmați instrucțiunile de pe ecran.

  > Această metodă nu este disponibilă dacă aplicația a fost instalată prin Kaspersky Security Center. Poți modifica selecția componentelor aplicației în Panoul de control numai după instalarea aplicației la nivel local.

- De la distanță, folosind Kaspersky Security Center.

  Activitatea *Modificare componente ale aplicației* permite modificarea componentelor aplicației Kaspersky Endpoint Security după instalarea acesteia.

Vă rugăm să țineți cont de următoarele considerente speciale atunci când schimbați componentele aplicației:

- Pe computerele pe care se execută Windows Server, nu puteți instala toate componentele Kaspersky Endpoint Security (de exemplu, componenta Control adaptiv al anomaliilor nu este disponibilă).
- Dacă unitățile hard disk de pe computer sunt protejate de Full Disk Encryption (FDE), nu puteți elimina componenta Full Disk Encryption. Pentru a elimina componenta Full Disk Encryption, decriptați toate unitățile hard disk ale computerului.
- În cazul în care computerul are fișiere criptate (FLE) sau utilizatorul folosește unități amovibile criptate (FDE sau FLE), va fi imposibil să accesați fișierele și unitățile amovibile după ce componentele funcției Data Encryption sunt eliminate. Puteți accesa fișierele și unitățile amovibile reinstalând componentele funcției Data Encryption.
- Dacă aplicația este instalată în modul Light Agent într-o infrastructură VDI, schimbarea componentelor setate nu este acceptată.

Cum se adăugă sau se elimină componentele aplicației în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **New task**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Selectarea tipului activității

Selectați **Kaspersky Endpoint Security for Windows (14.1)** → **Selectează componentele de instalat**.

Pasul 2. Setările activităților pentru modificarea componentelor aplicației

Selectați configurației aplicației:

- **Mod standard pentru a proteja gazdele**. Configurația implicită. Această configurație vă permite să utilizați toate componentele aplicației, inclusiv componentele care oferă suport pentru soluțiile Detection and Response. Această configurație este utilizată pentru protecția completă a computerului împotriva unei varietăți de amenințări, atacuri de rețea și fraude.

- **Endpoint Detection and Response Agent pentru protecție împotriva amenințărilor avansate și a atacurilor țintite**. În această configurație, puteți instala doar componentele care oferă suport pentru soluțiile Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), precum și KUMA. Această configurație este necesară dacă o platformă Endpoint Protection Platform (EPP) terță este implementată în organizație împreună cu soluția Kaspersky Detection and Response. Acest lucru face ca Kaspersky Endpoint Security în configurația Endpoint Detection and Response Agent să fie compatibil cu aplicațiile EPP terțe.

  Când modifici configurația aplicației pentru ca EDR Agent să funcționeze cu MDR, asigură-te că componentele responsabile de recepționarea telemetriei sunt activate.

- **Light Agent pentru protejarea mediilor virtuale**. Această configurație este destinată aplicației care este utilizată ca parte a soluției Kaspersky Security for Virtualization Light Agent. Light Agent trebuie instalat pe fiecare mașină virtuală care trebuie protejată folosind soluția. În această configurație, nu puteți utiliza componentele Data Encryption sau Control adaptiv al anomaliilor. Dacă instalezi Light Agent pe un șablon de mașină virtuală care va fi folosit pentru a crea *mașini virtuale non-persistente*, bifează caseta de selectare **Protejează infrastructura VDI** (VDI înseamnă Virtual Desktop Infrastructure). Modul de protecție VDI ajută la optimizarea performanței Kaspersky Endpoint Security pe mașinile virtuale non-persistente. În acest mod, Light Agent refuză actualizările aplicației care necesită repornirea mașinii virtuale. Când se primesc actualizări ale aplicației care necesită o repornire, Light Agent generează un eveniment despre necesitatea actualizării șablonului mașinilor virtuale protejate.

Selectați componentele aplicației care vor fi disponibile pe computerul utilizatorului.

Pasul 3. Setări avansate

Configurați setările avansate pentru activitate (consultați tabelul de mai jos).

Pasul 4. Selectarea dispozitivelor cărora le va fi atribuită activitatea

Selectați computerele pe care se va efectua activitatea. Sunt disponibile următoarele opțiuni:

- Atribuirea activității unui grup de administrare. În acest caz, activitatea este atribuită computerelor incluse într-un grup de administrare creat anterior.
- Selectare computere detectate în rețea de Serverul de administrare: *dispozitive neatribuite*. Dispozitivele specifice pot include dispozitive din grupuri de administrare, precum și dispozitive neatribuite.
- Specificarea manuală a adreselor computerelor sau importarea adreselor dintr-o listă. Poți specifica nume NetBIOS, adrese IP și subrețele IP ale dispozitivelor cărora dorești să le atribui activitatea.

Pasul 5. Configurarea unei planificări de pornire a activității

Configurați o planificare pentru începerea unei activități, de exemplu, manual sau atunci când computerul este inactiv.

Pasul 6. Definirea numelui activității

Introduceți un nume pentru activitate, de exemplu, *Adăugați componenta Application Control*.

Pasul 7. Finalizarea creării activității

Ieșiți din Expert. Dacă este necesar, bifați caseta de selectare **Run the task after the wizard finishes**. Puteți monitoriza progresul activității în proprietățile activității.

Cum se adaugă sau se elimină componentele aplicației în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **Add**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Configurarea setările generale ale activității

Configurați setările generale pentru activitate:

1. În lista verticală **Application**, selectează **Kaspersky Endpoint Security for Windows 14.1.0**.
2. În lista verticală **Task type**, selectează **Change application components**.
3. În câmpul **Task name**, introdu o descriere succintă, de exemplu *Adăugare componentă Application Control*.
4. În blocul **Devices to which the task will be assigned**, selectați domeniul activității.

Pasul 2. Selectarea dispozitivelor cărora le va fi atribuită activitatea

Selectați computerele pe care se va efectua activitatea. De exemplu, selectați un grup de administrare separat sau construiți o selecție.

Pasul 3. Finalizarea creării activității

Bifează caseta de selectare **Open task details when creation is complete** și finalizează expertul.

În proprietățile activității, selectați fila **Application settings**. Apoi, selectați configurația aplicației:

- **Standard mode to protect workstations and servers**. Configurația implicită. Această configurație vă permite să utilizați toate componentele aplicației, inclusiv componentele care oferă suport pentru soluțiile Detection and Response. Această configurație este utilizată pentru protecția completă a computerului împotriva unei varietăți de amenințări, atacuri de rețea și fraude.

- **Endpoint Detection and Response Agent to protect against advanced threats and targeted attacks**. În această configurație, puteți instala doar componentele care oferă suport pentru soluțiile Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), precum și KUMA. Această configurație este necesară dacă o platformă Endpoint Protection Platform (EPP) terță este implementată în organizație împreună cu soluția Kaspersky Detection and Response. Acest lucru face ca Kaspersky Endpoint Security în configurația Endpoint Detection and Response Agent să fie compatibil cu aplicațiile EPP terțe.

  Când modifici configurația aplicației pentru ca EDR Agent să funcționeze cu MDR, asigură-te că componentele responsabile de recepționarea telemetriei sunt activate.

- **Light Agent to protect virtual environments**. Această configurație este destinată aplicației care este utilizată ca parte a soluției Kaspersky Security for Virtualization Light Agent. Light Agent trebuie instalat pe fiecare mașină virtuală care trebuie protejată folosind soluția. În această configurație, nu puteți utiliza componentele Data Encryption sau Control adaptiv al anomaliilor. Dacă instalezi Light Agent pe un șablon de mașină virtuală care va fi folosit pentru a crea *mașini virtuale non-persistente*, bifează caseta de selectare **Protect VDI infrastructure** (VDI înseamnă Virtual Desktop Infrastructure). Modul de protecție VDI ajută la optimizarea performanței Kaspersky Endpoint Security pe mașinile virtuale non-persistente. În acest mod, Light Agent refuză actualizările aplicației care necesită repornirea mașinii virtuale. Când se primesc actualizări ale aplicației care necesită o repornire, Light Agent generează un eveniment despre necesitatea actualizării șablonului mașinilor virtuale protejate.

Selectați componentele aplicației care vor fi disponibile pe computerul utilizatorului. Configurați setările avansate pentru activitate (consultați tabelul de mai jos).

Ca rezultat, setul de componente ale aplicației Kaspersky Endpoint Security de pe computerele utilizatorilor va fi modificat în modul Silențios. Setările componentelor disponibile vor fi afișate în interfața locală a aplicației. Componentele care nu au fost incluse în aplicație sunt dezactivate, iar setările acestor componente nu sunt disponibile.

La instalarea, actualizarea sau dezinstalarea Kaspersky Endpoint Security, pot apărea erori. Pentru mai multe informații despre rezolvarea acestor erori, vă rugăm să consultați Baza de cunoștințe pentru suport tehnic.

Setări avansate ale activității

Parametru	Descriere
Setări activități	**Verifică aplicațiile terțe incompatibile**. În mod implicit, Kaspersky Endpoint Security verifică compatibilitatea aplicațiilor instalate. Lista programelor software care pot cauza probleme de compatibilitate este disponibilă în fișierul incompatible.txt. Fișierul este inclus în kitul de distribuție. Dacă scanarea software-urilor instalate este activată, atunci când este detectată o aplicație din listă, Kaspersky Endpoint Security oprește activitatea. Poți dezactiva scanarea software-urilor instalate dacă documentația producătorului software-ului terț prevede compatibilitatea cu Endpoint Protection Platform (EPP). **Elimină aplicațiile terțe incompatibile**. Eliminarea automată a aplicațiilor listate în fișierul incompatible.txt înainte de a modifica setul de componente. Dacă această funcționalitate este activată, Kaspersky Endpoint Security încearcă să elimine aplicațiile care pot cauza probleme de compatibilitate pentru a continua activitatea. **Utilizează modul de compatibilitate Azure WVD**. Această funcție asigură afișarea corectă a stării mașinii virtuale Azure în consola Kaspersky Anti Targeted Attack Platform. Pentru a monitoriza performanța computerului, Kaspersky Endpoint Security trimite date de telemetrie către serverele KATA. Telemetria include un ID al computerului (Sensor ID). Modul de compatibilitate Azure WVD permite alocarea unui Sensor ID unic permanent către aceste mașini virtuale. Dacă modul de compatibilitate este dezactivat, Sensor ID se poate schimba după ce computerul este repornit din cauza modului în care funcționează mașinile virtuale Azure. Acest lucru poate face ca duplicate ale mașinilor virtuale să apară pe consolă.

Parametru	Descriere
Excluderi	Începând cu Kaspersky Endpoint Security 12.6 for Windows, excluderile de scanare și aplicații de încredere sunt adăugate la zona de încredere. Excluderile de la scanare și aplicațiile de încredere predefinite ajută la configurarea rapidă a Kaspersky Endpoint Security pe serverele SQL, serverele Microsoft Exchange și System Center Configuration Manager. Aceasta înseamnă că nu trebuie să configurați manual o zonă de încredere pentru aplicație pe servere. Începând cu Kaspersky Endpoint Security 12.8 for Windows, poți instala aplicația în modul Light Agent pentru a proteja mediile virtuale. Excluderile de la scanare predefinite și aplicațiile de încredere te pot ajuta să configurezi rapid Kaspersky Endpoint Security în mediile virtuale Citrix și VMware. De asemenea, poți configura zona de încredere mai târziu, în proprietățile politicii: excluderi de la scanare și aplicații de încredere.
Mod separat / Mod combinat	Poți crea seturi separate de componente pentru stații de lucru și servere – **Mod separat**. Înainte de a implementa pachetul de instalare, programul de instalare detectează tipul sistemului de operare și instalează numai acele componente ale aplicației pe care le-ai selectat pentru acel tip de sistem de operare. Astfel, poți utiliza același pachet de instalare pentru stațiile de lucru și servere. **Mod combinat** oferă o listă obișnuită de componente pentru stația de lucru și servere. Disponibilitatea componentelor individuale depinde de tipul sistemului de operare. În acest mod, recomandăm crearea unui pachet de instalare separat pentru stațiile de lucru și un pachet de instalare separat pentru servere. Poți configura lista obișnuită de componente din pachetul de instalare numai în modul Standard.
Utilizare parolă pentru modificarea setului componentelor aplicației	De obicei, administratorii activează Protecție prin parolă pentru a restricționa accesul la Kaspersky Endpoint Security. Aceasta înseamnă că, pentru a modifica selecția componentelor aplicației, trebuie să introduceți acreditările unui utilizator care are permisiunea **Elimină/modifică/restaurează aplicația**. De exemplu, puteți utiliza contul KLAdmin.
Utilizează parola pentru a dezinstala Kaspersky Endpoint Agent și Kaspersky Security for Windows Server	Administratorii activează, de obicei, Protecție prin parolă în setările acestor activități pentru a restricționa accesul la Kaspersky Endpoint Agent (KEA) și Kaspersky Security for Windows Server (KSWS). Aceasta înseamnă că, dacă migrați de la configurația [KES+KEA] la [agent încorporat+ KES] sau dacă migrați de la KSWS la KES, trebuie să introduceți o parolă pentru a elimina aceste aplicații.

Upgradarea unei versiuni anterioare a aplicației

Când actualizați o versiune anterioară a aplicației la o versiune mai nouă, luați în considerare următoarele:

- Localizarea noii versiuni a Kaspersky Endpoint Security trebuie să corespundă cu localizarea versiunii instalate a aplicației. Dacă localizările aplicațiilor nu se potrivesc, upgrade-ul aplicației se va finaliza cu o eroare.
- Vă recomandăm să închideți toate aplicațiile active înainte de a începe actualizarea.
- Înainte de actualizare, Kaspersky Endpoint Security blochează funcționalitatea Full Disk Encrytion. Dacă nu poate fi blocată componenta Full Disk Encryption, nu va porni instalarea upgrade-ului. După actualizarea aplicației, funcționalitatea Full Disk Encryption va fi restabilită.

Kaspersky Endpoint Security acceptă actualizări pentru următoarele versiuni ale aplicației:

- Kaspersky Endpoint Security 12.1 for Windows (versiunea 12.1.0.506)
- Kaspersky Endpoint Security 12.2 for Windows (versiunea 12.2.0.462)
- Kaspersky Endpoint Security 12.3 for Windows (versiunea 12.3.0.493)
- Kaspersky Endpoint Security 12.4 for Windows (versiunea 12.4.0.467)
- Kaspersky Endpoint Security 12.5 for Windows (versiunea 12.5.0.539)
- Kaspersky Endpoint Security 12.6 for Windows (versiunea 12.6.0.438)
- Kaspersky Endpoint Security 12.7 for Windows (versiunea 12.7.0.533)

- Kaspersky Endpoint Security 12.8 for Windows (versiunea 12.8.0.505)
- Kaspersky Endpoint Security 12.9 for Windows (versiunea 12.9.0.384)
- Kaspersky Endpoint Security 12.10 for Windows (versiunea 12.10.0.466)
- Kaspersky Endpoint Security 12.11 for Windows (versiunea 12.11.0.637)
- Kaspersky Endpoint Security 12.12 for Windows (versiunea 12.12.0.522)
- Kaspersky Endpoint Security 14.0 for Windows (versiunea 14.0.0.504)

La instalarea, actualizarea sau dezinstalarea Kaspersky Endpoint Security, pot apărea erori. Pentru mai multe informații despre rezolvarea acestor erori, vă rugăm să consultați Baza de cunoștințe pentru suport tehnic.

Metode de efectuare a upgrade-ului aplicației:

Aplicația Kaspersky Endpoint Security poate fi actualizată pe computer în următoarele moduri:

- Utilizând serviciul de actualizare Kaspersky (Seamless Update – SMU).
- local, folosind Expertul de configurare.
- local, din linia de comandă.
- de la distanță, folosind Kaspersky Security Center.
- la distanță, prin intermediul editorului de gestionare a politicilor de grup pentru Microsoft Windows (pentru mai multe detalii, vizitați site-ul web de suport tehnic Microsoft).
- la distanță, folosind System Center Configuration Manager.

Dacă aplicația care este instalată în rețeaua corporativă prezintă un set de componente, altele decât setul implicit, actualizarea aplicației prin Consola de administrare (MMC) este diferită de actualizarea aplicației prin Web Console și Cloud Console. Când actualizați Kaspersky Endpoint Security, luați în considerare următoarele:

- Kaspersky Security Center Web Console sau Kaspersky Security Center Cloud Console.

  Dacă ați creat un pachet de instalare pentru noua versiune a aplicației cu setul de componente implicit, atunci setul de componente de pe computerul unui utilizator nu va fi modificat. Pentru a utiliza Kaspersky Endpoint Security cu setul implicit de componente, trebuie să deschideți proprietățile pachetului de instalare, să schimbați setul de componente, apoi să reveniți la setul original de componente și să salvați modificările.

- Consola de administrare Kaspersky Security Center.

  Setul de componente al aplicației după actualizare se va potrivi cu setul de componente din pachetul de instalare. Adică, dacă noua versiune a aplicației are setul implicit de componente, atunci, de exemplu, BadUSB Attack Prevention va fi eliminată de pe computer, deoarece această componentă este exclusă din setul implicit. Pentru a continua să utilizați aplicația cu același set de componente ca înainte de actualizare, selectați componentele necesare în setările pachetului de instalare.

Efectuarea upgrade-ului aplicației fără repornire

Actualizarea aplicației fără repornire asigură funcționarea neîntreruptă a serverului atunci când versiunea aplicației este actualizată.

Efectuarea upgrade-ului aplicației fără repornire are următoarele limitări:

- Poți efectua upgrade-ul aplicației fără repornire începând cu versiunea 11.10.0. Pentru a efectua upgrade-ul unei versiuni anterioare a aplicației, trebuie să repornești computerul.
- Poți instala corecții fără repornire începând cu versiunea 11.11.0. Pentru a instala corecții pentru versiunile anterioare ale aplicației, poate fi necesară o repornire a computerului.
- Efectuarea upgrade-ului aplicației fără repornire nu este disponibilă pe computerele pe care este activată criptarea datelor (criptare Kaspersky (FDE), BitLocker, File Level Encryption (FLE)). Pentru efectuarea upgrade-ului aplicației pe computere pe care este activată criptarea datelor, computerul trebuie repornit.
- Aplicația nu poate fi actualizată pe o mașină virtuală fără repornire. Pentru a actualiza aplicația pe o mașină virtuală, trebuie să repornești mașina virtuală.

După efectuarea unui upgrade al aplicației, instalarea unei corecții, modificarea setului de componente ale aplicației sau restaurare, Kaspersky Endpoint Security repornește pentru a începe să utilizeze noua versiune. Repornirea Kaspersky Endpoint Security poate dura până la un minut. În acest interval, nivelul de protecție a computerului este redus. După repornirea aplicației, nivelul de protecție al computerului va fi restabilit.

Cum se selectează modul de efectuare a upgrade-ului aplicației în Consola de administrare (MMC)

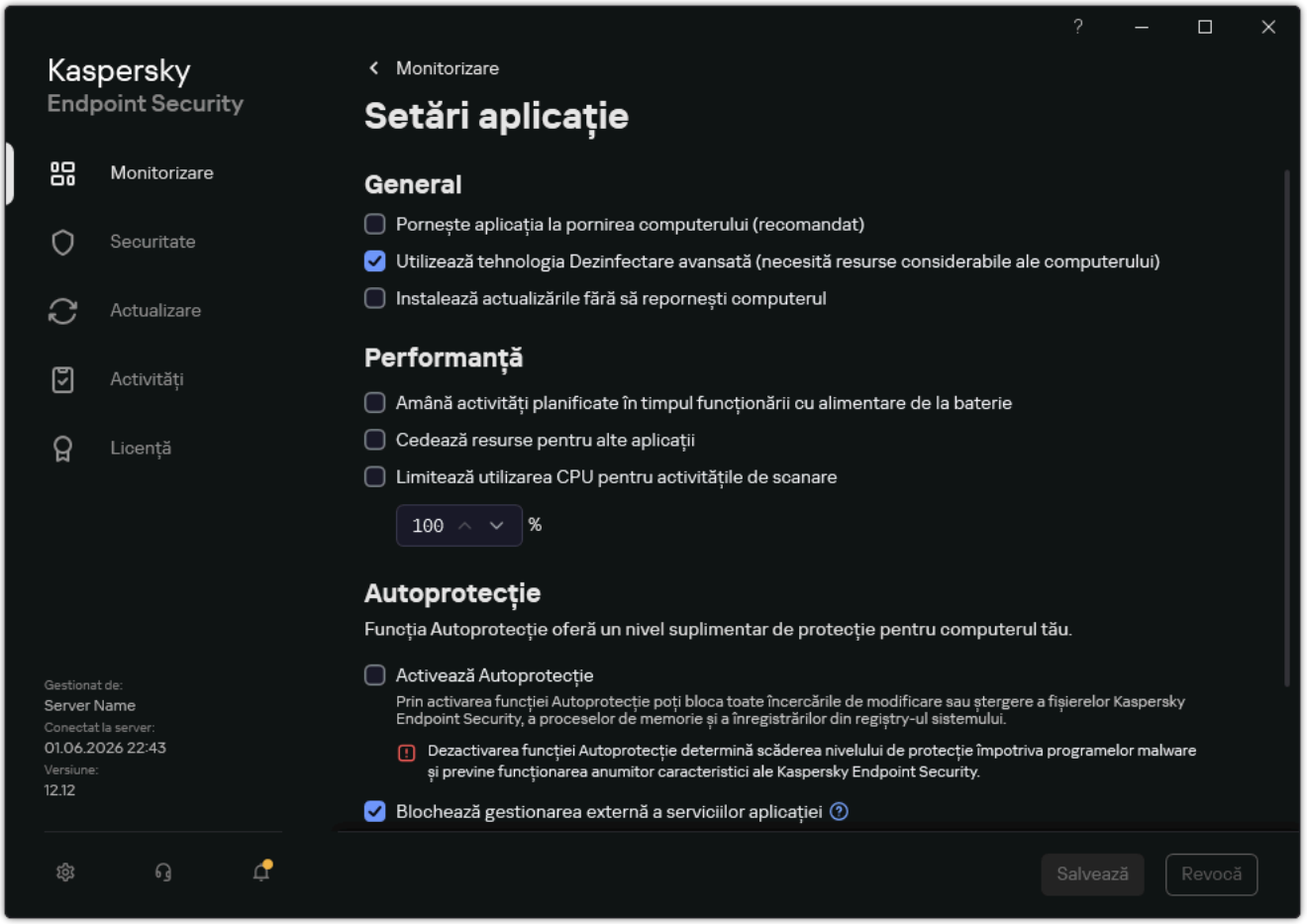
1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **General Settings** → **User Interaction**.
5. În blocul **Application update settings**, bifează sau debifează caseta de selectare **Install application updates without restart** pentru a configura modul de efectuare a upgrade-ului aplicației.
6. Salvați-vă modificările.

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Setări generale** → **Setări aplicație**.
4. În blocul **Setări avansate**, bifează sau debifează caseta de selectare **Instalează actualizările aplicației fără repornire** pentru a configura modul de efectuare a upgrade-ului aplicației.
5. Salvați-vă modificările.

Cum se selectează modul de efectuare a upgrade-ului aplicației în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Setări generale** → **Setări aplicație**.



Setări Kaspersky Endpoint Security for Windows

3. În blocul **General**, bifează sau debifează caseta de selectare **Instalează actualizările fără să repornești computerul** pentru a configura modul de efectuare a upgrade-ului aplicației.
4. Salvați-vă modificările.

După finalizarea procedurii de actualizare a aplicației fără repornire, noua versiune a Kaspersky Endpoint Security va fi instalată pe computer. Versiunea anterioară a aplicației este ștearsă automat.

Nu puteți iniția o actualizare a aplicației înainte ca actualizarea anterioară să se fi finalizat complet.

Puteți verifica starea actualizării Kaspersky Endpoint Security folosind raportul privind versiunea aplicației Kaspersky din consola Kaspersky Security Center.

Actualizarea SMU a aplicației

Pentru a actualiza aplicația utilizând serviciul de actualizare Kaspersky (Seamless Update; SMU), nu trebuie să rulezi programul de instalare, spre deosebire de alte metode de actualizare. Kaspersky Endpoint Security primește noua versiune a aplicației împreună cu bazele de date antivirus din aceeași sursă.

O actualizare SMU permite actualizarea aplicației pe toate computerele organizației tale la cea mai recentă versiune. Înainte de a aplica o actualizare SMU, recomandăm testarea noii versiuni a aplicației pe câteva computere. Pentru aceasta, trebuie să actualizezi manual aplicația pe aceste computere (de exemplu, local, folosind Expertul de configurare). Nu poți selecta computere individuale atunci când efectuezi o actualizare SMU.

Programul de actualizare a aplicației este stabilit de personalul Kaspersky. Pentru a te asigura că noua versiune a aplicației funcționează fără probleme, Kaspersky pune la dispoziție actualizările pas cu pas. Aceasta înseamnă că poți obține actualizarea SMU cu până la două luni mai târziu fa'[de data lansării unei noi versiuni.

Poți gestiona actualizarea SMU a aplicației folosind activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor*. Pentru a avea noua versiune a aplicației inclusă în același pachet cu bazele de date antivirus, trebuie să permiți actualizarea *modulelor aplicației* în setările activității *Actualizarea modulelor bazelor de date și ale aplicațiilor*. De asemenea, în setările activității *Actualizarea modulelor bazelor de date și ale aplicațiilor*, poți permite actualizarea aplicației fără repornire.

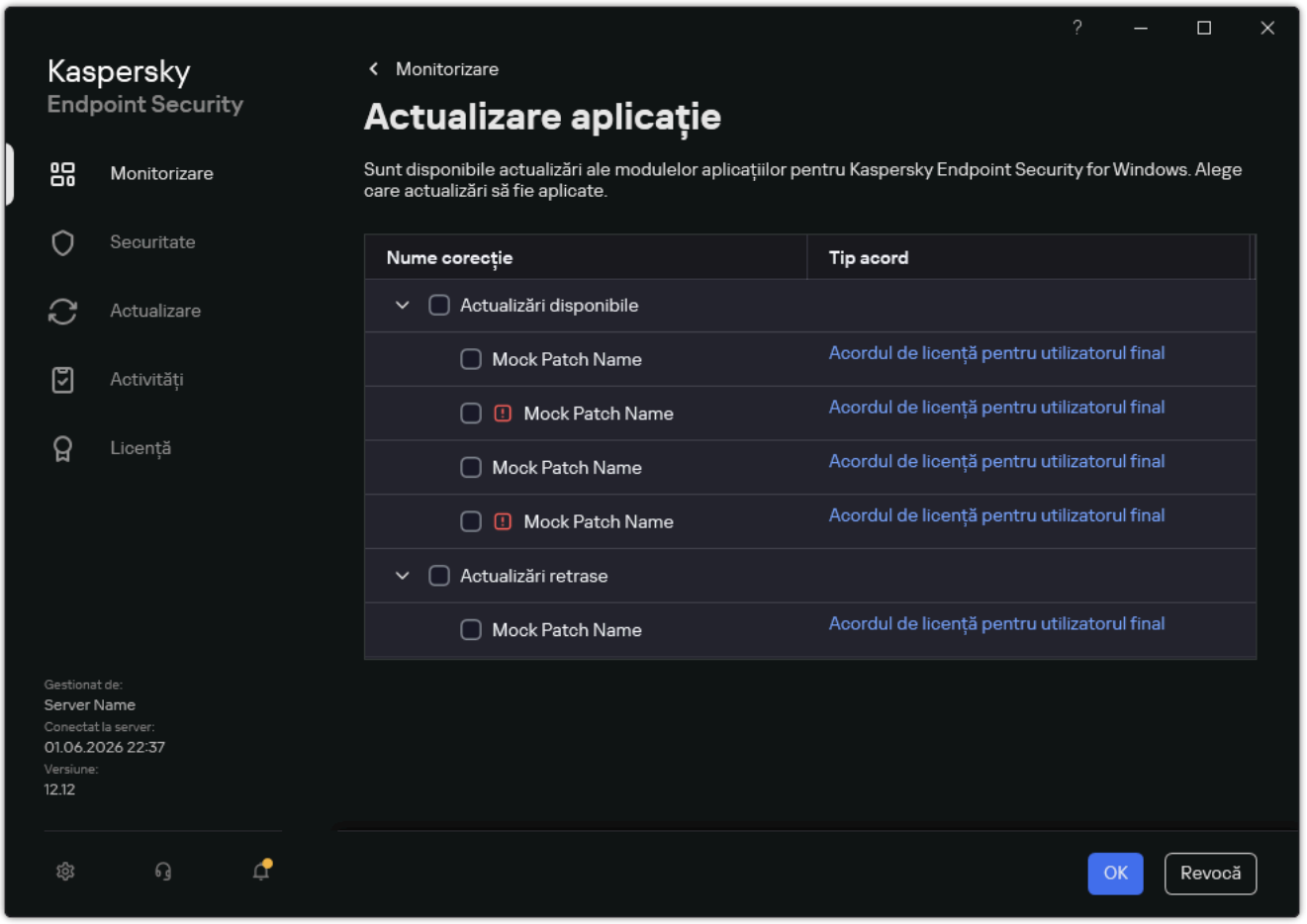
Etapele unei actualizări SMU a aplicației

1. **După lansarea unei noi versiuni a aplicației, Kaspersky distribuie actualizarea.**
2. **Utilizatorul aprobă actualizarea aplicației.**

   Dacă computerul este conectat la Kaspersky Security Center, actualizarea este disponibilă în Kaspersky Security Center, în secțiunea **Update of Kaspersky databases and application modules**. Pentru mai multe detalii despre aprobarea actualizărilor, consultă Ajutor pentru Kaspersky Security Center.

   Dacă computerul nu este conectat la Kaspersky Security Center, actualizarea este disponibilă în secțiunea de notificări a interfeței aplicației: . Pentru a aproba actualizarea, selectează o versiune a aplicației și acceptă termenii și condițiile acordurilor (vezi figura de mai jos).
3. **Kaspersky Endpoint Security execută activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* în conformitate cu programul configurat.**

Drept urmare, Kaspersky Endpoint Security actualizează aplicația în modul „silențios”.



Actualizări disponibile pentru aplicații

Eliminarea aplicației

Eliminarea aplicației Kaspersky Endpoint Security lasă computerul și datele utilizatorului neprotejate împotriva amenințărilor.

La instalarea, actualizarea sau dezinstalarea Kaspersky Endpoint Security, pot apărea erori. Pentru mai multe informații despre rezolvarea acestor erori, vă rugăm să consultați Baza de cunoștințe pentru suport tehnic.

Eliminarea aplicației de la distanță, folosind Kaspersky Security Center

Puteți dezinstala aplicația de la distanță folosind activitatea *Uninstall application remotely*. La efectuarea activității, Kaspersky Endpoint Security descarcă utilitarul de dezinstalare a aplicației pe computerul utilizatorului. După finalizarea dezinstalării aplicației, utilitarul va fi eliminat automat.

Cum se elimină aplicația prin Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați **Tasks**.
   Lista activităților se deschide.
3. Fă clic pe **New task**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Selectarea tipului activității

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

Pasul 2. Selectarea aplicației care trebuie eliminată

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

Pasul 3. Setările activității pentru dezinstalarea aplicației

Selectați **Kaspersky Endpoint Security for Windows (14.1)**.

Pasul 4. Dezinstalarea setărilor utilitare

Configurați următoarele setări suplimentare ale aplicației:

- **Force download of the uninstallation utility**. Selectați metoda de livrare a utilitarului:
  - **Using Network Agent**. Dacă Agentul de rețea nu a fost instalat pe computer, primul Agent de rețea va fi instalat utilizându-se instrumentele din sistemul de operare. Apoi, Kaspersky Endpoint Security este dezinstalat de instrumentele funcției Agent de rețea.
  - **Using operating system resources through Administration Server**. Utilitarul va fi livrat pe computerele client utilizându-se resursele sistemului de operare, prin intermediul Serverului de administrare. Poți selecta această opțiune dacă Agentul de rețea nu este instalat pe computerul client, însă computerul client se află în aceeași rețea ca și Serverul de administrare.
  - **Using operating system resources through distribution points**. Utilitarul este livrat pe computerele client utilizându-se folosindu-se resursele sistemului de operare prin intermediul punctelor de distribuire. Poți selecta această opțiune dacă există cel puțin un punct de distribuire în rețea. Pentru mai multe detalii despre punctele de distribuție, consultați Ajutor pentru Kaspersky Security Center.
- **Verify operating system type before downloading**. Dacă este necesar, debifați această casetă de selectare. Acest lucru vă permite să evitați descărcarea utilitarului de dezinstalare dacă sistemul de operare al computerului nu îndeplinește cerințele software. Dacă ești sigur că sistemul de operare al computerului îndeplinește cerințele software, poți ignora această verificare.

Dacă operațiunea de dezinstalare a aplicației este protejată prin parolă, procedați după cum urmează:

1. Bifați caseta de selectare **Use uninstallation password**.
2. Faceți clic pe butonul **Edit**.
3. Introduceți parola contului KLAdmin.

Pasul 5. Selectarea setării de repornire a sistemului de operare

După dezinstalarea aplicației, este necesară o repornire. Selectați acțiunea care va fi efectuată pentru a reporni computerul.

Pasul 6. Selectarea dispozitivelor cărora le va fi atribuită activitatea

Selectați computerele pe care se va efectua activitatea. Sunt disponibile următoarele opțiuni:

- Atribuirea activității unui grup de administrare. În acest caz, activitatea este atribuită computerelor incluse într-un grup de administrare creat anterior.
- Selectare computere detectate în rețea de Serverul de administrare: *dispozitive neatribuite*. Dispozitivele specifice pot include dispozitive din grupuri de administrare, precum și dispozitive neatribuite.
- Specificarea manuală a adreselor computerelor sau importarea adreselor dintr-o listă. Poți specifica nume NetBIOS, adrese IP și subrețele IP ale dispozitivelor cărora dorești să le atribui activitatea.

Pasul 7. Selectarea contului pentru executarea activității

Selectați contul pentru instalarea Agentului de rețea folosind instrumentele din sistemul de operare. În acest caz, sunt necesare drepturi de administrator pentru accesul la computer. Poți adăuga mai multe conturi. Dacă un cont nu are drepturi suficiente, Expertul de instalare utilizează următorul cont. Dacă dezinstalezi Kaspersky Endpoint Security utilizând instrumentele Agentului de rețea, nu este necesar să selectezi un cont.

Pasul 8. Configurarea unei planificări de pornire a activității

Configurați o planificare pentru începerea unei activități, de exemplu, manual sau atunci când computerul este inactiv.

Pasul 9. Definirea numelui activității

Introduceți un nume pentru activitate, de ex. *Elimină Kaspersky Endpoint Security 14.1*.

Pasul 10. Finalizarea creării activității

Ieșiți din Expert. Dacă este necesar, bifați caseta de selectare **Run the task after the wizard finishes**. Puteți monitoriza progresul activității în proprietățile activității.

Aplicația va fi dezinstalată în modul silențios.

Cum se elimină aplicația prin Web Console și Cloud Console

1. În fereastra principală a Web Console, selectează **Tasks**.
   Lista activităților se deschide.
2. Fă clic pe **Add**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Configurarea setările generale ale activității

Configurați setările generale pentru activitate:

1. În lista verticală **Application**, selectează **Kaspersky Security Center**.
2. În lista verticală **Task type**, selectează **Uninstall application remotely**.
3. În câmpul **Task name**, introduceți o descriere succintă, de exemplu *Dezinstalare Kaspersky Endpoint Security de pe computerele Suportului tehnic*.
4. În blocul **Devices to which the task will be assigned**, selectați domeniul activității.

Pasul 2. Selectarea dispozitivelor cărora le va fi atribuită activitatea

Selectați computerele pe care se va efectua activitatea. De exemplu, selectați un grup de administrare separat sau construiți o selecție.

Pasul 3. Configurarea setărilor de dezinstalare a aplicației

În acest pas, configurați setările de dezinstalare a aplicației:

1. Selectați **Uninstall managed application**.
2. Selectați **Kaspersky Endpoint Security for Windows**.

3. **Force download of the uninstallation utility**. Selectați metoda de livrare a utilitarului:

   - **Using Network Agent**. Dacă Agentul de rețea nu a fost instalat pe computer, primul Agent de rețea va fi instalat utilizându-se instrumentele din sistemul de operare. Apoi, Kaspersky Endpoint Security este dezinstalat de instrumentele funcției Agent de rețea.

   - **Using operating system resources through Administration Server**. Utilitarul va fi livrat pe computerele client utilizându-se resursele sistemului de operare, prin intermediul Serverului de administrare. Poți selecta această opțiune dacă Agentul de rețea nu este instalat pe computerul client, însă computerul client se află în aceeași rețea ca și Serverul de administrare.

   - **Using operating system resources through distribution points**. Utilitarul este livrat pe computerele client utilizându-se folosindu-se resursele sistemului de operare prin intermediul punctelor de distribuire. Poți selecta această opțiune dacă există cel puțin un punct de distribuire în rețea. Pentru mai multe detalii despre punctele de distribuție, consultați Ajutor pentru Kaspersky Security Center.

4. În câmpul **Maximum number of concurrent downloads**, setați o limită pentru numărul de solicitări trimise către Administration Server pentru a descărca utilitarul de dezinstalare a aplicației. O limită pentru numărul de solicitări va ajuta la prevenirea supraîncărcării rețelei.

5. În câmpul **Maximum number of uninstallation attempts**, setați o limită pentru numărul de încercări de dezinstalare a aplicației. Dacă dezinstalarea aplicației Kaspersky Endpoint Security se termină cu o eroare, activitatea va porni automat din nou dezinstalarea.

6. Dacă este necesar, debifați caseta de selectare **Verify operating system type before downloading**. Acest lucru vă permite să evitați descărcarea utilitarului de dezinstalare dacă sistemul de operare al computerului nu îndeplinește cerințele software. Dacă ești sigur că sistemul de operare al computerului îndeplinește cerințele software, poți ignora această verificare.

Pasul 4. Selectarea contului pentru executarea activității

Selectați contul pentru instalarea Agentului de rețea folosind instrumentele din sistemul de operare. În acest caz, sunt necesare drepturi de administrator pentru accesul la computer. Poți adăuga mai multe conturi. Dacă un cont nu are drepturi suficiente, Expertul de instalare utilizează următorul cont. Dacă dezinstalezi Kaspersky Endpoint Security utilizând instrumentele Agentului de rețea, nu este necesar să selectezi un cont.

Pasul 5. Finalizarea creării activității

Termină expertul făcând clic pe butonul **Finish**. Se va afișa o activitate nouă în lista de activități.

Pentru a executa o activitate, bifează caseta de selectare de lângă activitate și fă clic pe butonul **Start**. Aplicația va fi dezinstalată în modul silențios. După finalizarea dezinstalării, Kaspersky Endpoint Security afișează o solicitare pentru a reporni computerul.

Dacă operațiunea de dezinstalare a aplicației este protejată prin parolă, introdu parola contului KL Admin în proprietățile activității *Uninstall application remotely*. Fără parolă, activitatea nu va fi executată.

Pentru a utiliza parola contului KLAdmin în activitatea Uninstall application remotely:

1. În fereastra principală a Web Console, selectați **Asset management** → **Tasks**.

   Lista activităților se deschide.

2. Apasă pe activitatea **Uninstall application remotely** a Kaspersky Security Center.

   Se va deschide fereastra de proprietăți a activității.

3. Selectați fila **Application settings**.

4. Bifați caseta de selectare **Use uninstallation password**.

5. Introduceți parola contului KLAdmin.

6. Salvați-vă modificările.

Repornește aplicația pentru a finaliza dezinstalarea. Pentru a face acest lucru, Agentul de rețea afișează o fereastră pop-up.

Eliminarea aplicației de la distanță folosind Active Directory

Puteți dezinstala aplicația de la distanță utilizând o politică de grup Microsoft Windows. Pentru a dezinstala aplicația, trebuie să deschideți Consola de management al politicii de grup (gpmc.msc) și să utilizați Editorul politicii de grup pentru a crea o activitate de eliminare a aplicației (pentru mai multe detalii, vă rugăm să vizitați site-ul web Suport tehnic Microsoft).

Dacă operațiunea de dezinstalare a aplicației este protejată prin parolă, trebuie să procedați după cum urmează:

1. Creați un fișier BAT cu următorul conținut:

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

   `<GUID>` este ID-ul unic al aplicației. Puteți afla codul GUID al aplicației în Baza de cunoștințe pentru suport tehnic sau folosind următoarea comandă:

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

   Exemplu

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

2. Creați o nouă politică Microsoft Windows pentru computerele din Consola de gestionare a politicilor de grup (gpmc.msc).

3. Utilizați noua politică pentru a executa fișierul BAT creat pe computere.

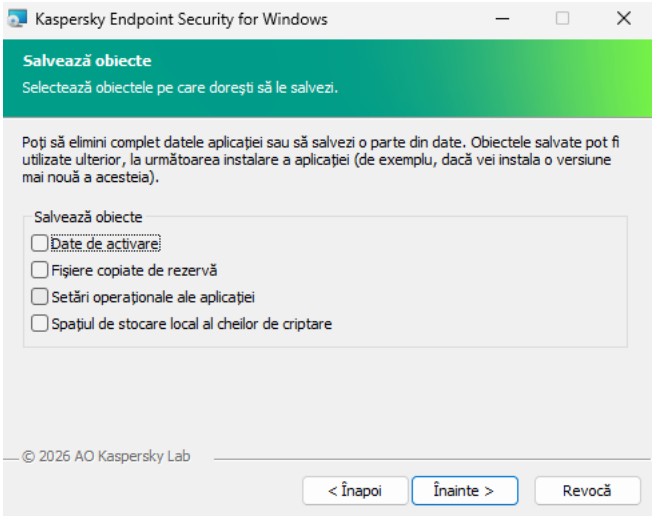
Eliminarea aplicației local

Poți elimina aplicația local, folosind Expertul de configurare. Kaspersky Endpoint Security este eliminat folosind metoda normală pentru un sistem de operare Windows, care se face prin Control Panel. Expertul de instalare pornește. Urmați instrucțiunile de pe ecran.



Selectarea operației de eliminare a aplicației

Poți specifica datele folosite de aplicație pe care dorește să le salvezi pentru utilizare ulterioare, la următoarea instalare a aplicației (de exemplu când se face upgrade la o versiune mai nou a aplicației). Dacă nu specifici niciun fel de date, aplicația va fi complet eliminată (vezi figura de mai jos).



Salvarea datelor după eliminare

Puteți salva următoarele date:

- **Date de activare**, care vă permit să evitați să activați din nou aplicația. Kaspersky Endpoint Security adaugă automat o cheie de licență dacă termenul licenței nu a expirat înainte de instalare.
- **Fișiere copiate de rezervă** – fișiere care sunt scanate de aplicație și sunt plasate în Copie de rezervă.

  Fișierele din Copie de rezervă care sunt salvate după eliminarea aplicației pot fi accesate numai din aceeași versiune a aplicației care a fost folosită pentru salvarea acelor fișiere.

Dacă intenționați să folosiți obiectele din Copie de rezervă după eliminarea aplicației, trebuie să restaurați acele obiecte înainte de a elimina aplicația. Cu toate acestea, experții Kaspersky nu recomandă restaurarea obiectelor din Copie de rezervă, deoarece aceasta ar putea dăuna computerului.

- **Setări operaționale ale aplicației** – valori ale setărilor aplicației care sunt selectate în timpul configurării aplicației.

- **Spațiul de stocare local al cheilor de criptare** – date care oferă acces la fișierele și unitățile care au fost criptate înainte de eliminarea aplicației. Pentru a asigura accesul la fișierele și unitățile criptate, asigurați-vă că ați selectat funcționalitatea de criptare a datelor când reinstalați Kaspersky Endpoint Security. Nu este necesară nicio acțiune suplimentară pentru accesul la fișierele și unitățile criptate anterior.

Kaspersky Endpoint Security salvează datele în directorul `C:\ProgramData\Kaspersky Lab\KES.14.1\QB`.

De asemenea, poți șterge aplicația local folosind linia de comanda.

Licența aplicației

Această secțiune oferă informații despre conceptele generale legate de licențierea Kaspersky Endpoint Security.

Despre Acordul de licență pentru utilizatorul final

Acordul de licență pentru utilizatorul final este un acord obligatoriu între tine și AO Kaspersky Lab, care stipulează condițiile în care poți folosi aplicația.

Recomandăm citirea cu atenție a termenilor din Acordul de licență pentru utilizatorul final înainte de utilizarea aplicației.

Poți vedea termenii din Acordul de licență în următoarele moduri:

- La instalarea aplicației Kaspersky Endpoint Security în modul interactiv.
- Citind fișierul license.txt. Acest document este inclus în kitul de distribuție al aplicației și se găsește, de asemenea, în directorul de instalare a aplicației `%ProgramFiles(x86)%\Kaspersky Lab\KES\Doc\<locale>\KES`.

Confirmând acceptarea Acordului de licență pentru utilizatorul final, indici acceptare termenilor Acordului de licență pentru utilizatorul final. Dacă nu accepți termenii din Acordul de licență pentru utilizatorul final, trebuie să abandonezi instalarea.

Despre licență

O *licență* este un drept pe durată limitată de utilizare a aplicației acordat în baza Acordului de licență pentru utilizatorul final.

Licența îți permite să utilizezi aplicația în conformitate cu termenii Acordului de licență pentru utilizatorul final și să beneficiezi de suport tehnic. Lista funcțiilor disponibile și perioada de utilizare a aplicației depind de tipul de licență cu care a fost activată aplicația.

Există două tipuri de licență:

- *Trial* – o licență gratuită destinată încercării aplicației.

  O licență trial are, de obicei, un termen scurt. După expirarea licenței trial, toate caracteristicile aplicației Kaspersky Endpoint Security sunt dezactivate. Pentru a continua utilizarea aplicației, trebuie să achiziționezi o licență comercială.

  Puteți activa aplicația sub licență pentru versiune trial o singură dată. Aplicația nu poate fi activată în baza unei licențe trial după ce a fost activată cu o licență comercială.

- *Comercială* – o licență plătită furnizată atunci când achiziționezi Kaspersky Endpoint Security.

  Funcționalitatea aplicației disponibilă în baza licenței comerciale depinde de alegerea produsului. Produsul selectat este indicat în Certificat licență. Informații despre produsele disponibile pot fi găsite pe site-ul web Kaspersky.

Când licența comercială expiră, caracteristicile cheie ale aplicației sunt dezactivate. Pentru a continua utilizarea aplicației, trebuie să-ți reînnoiești licența comercială. Dacă nu intenționați să vă reînnoiți licența, trebuie să eliminați aplicația de pe computer.

Despre certificatul de licență

Un *certificat de licență* este un document transferat utilizatorului împreună cu un fișier cheie sau un cod de activare.

Certificatul de licență conține următoarele informații despre licență:

- ID-ul licenței sau numărul comenzii.
- Detalii despre utilizatorul căruia îi este acordată licența.
- Detalii despre aplicația care poate fi activată utilizându-se licența.
- Limitarea numărului de unități licențiate (de exemplu, numărul de dispozitive pe care poate fi utilizată aplicația în baza licenței).
- Data de început a valabilității licenței.
- Data expirării licenței sau valabilitatea licenței.
- Tip licență.

Despre abonament

Un *abonament pentru Kaspersky Endpoint Security* este o comandă de achiziție pentru aplicație, cu anumiți parametri (cum ar fi data de expirare a abonamentului și număr de dispozitive protejate). Poți comanda un abonament pentru Kaspersky Endpoint Security de la furnizorul tău de servicii (de exemplu, un ISP). Un abonament poate fi reînnoit manual sau automat și poate fi anulat. Vă puteți administra abonamentul pe site-ul Web al furnizorului de servicii.

Abonamentul poate fi limitat (pentru un an de zile, de exemplu) sau nelimitat (fără o dată de expirare). Pentru ca aplicația Kaspersky Endpoint Security să funcționeze după expirarea termenului unui abonament limitat, trebuie să vă reînnoiti abonamentul. Abonamentul nelimitat este reînnoit automat dacă serviciile furnizorului au fost plătite anticipat în timp util.

Când expiră un abonament limitat, poți beneficia de o perioadă de grație pentru reînnoirea abonamentului, timp în care aplicația funcționează în continuare. Disponibilitatea și durata acestei perioade de grație sunt decise de furnizorul de servicii.

Pentru a folosi Kaspersky Endpoint Security în baza unui abonament, trebuie să aplicați codul de activare primit de la furnizorul de servicii. După aplicarea codului de activare, cheia activă este adăugată. Cheia activă determină licența pentru utilizarea aplicației în baza abonamentului. Nu poți activa aplicația în baza abonamentului utilizând un fișier cheie. Furnizorul de servicii poate furniza doar un cod de activare. Nu se poate adăuga o cheie de rezervă în baza unui abonament.

Codurile de activare achiziționate în baza unui abonament nu pot fi folosite pentru a activa versiuni anterioare ale Kaspersky Endpoint Security.

Despre cheia de licență

O *cheie de licență* este o secvență de biți pe care o puteți utiliza pentru a activa și apoi utiliza aplicația în conformitate cu termenii Acordului de licență pentru utilizatorul final.

Un certificat de licență nu este furnizat pentru o cheie adăugată în baza unui abonament.

Poți adăuga o cheie de licență pentru aplicație fie aplicând un fișier cheie, fie introducând un cod de activare.

Cheia poate fi blocată de către Kaspersky dacă au fost încălcați termenii din Acordul de licență pentru utilizatorul final. Dacă o cheie a fost blocată, trebuie să adaugați o altă cheie pentru a continua să folosiți aplicația.

Există două tipuri de chei: active și de rezervă.

O *cheie activă* este o cheie care este utilizată în mod curent de aplicație. O cheie trial sau o cheie pentru licență pentru versiune comercială poate fi adăugată drept cheie activă. Aplicația nu poate avea mai mult de o singură cheie activă.

O *cheie de rezervă* este o cheie care dă dreptul utilizatorului să folosească aplicația, dar care nu este în prezent în uz. La expirarea cheii active, o cheie de rezervă devine activă în mod automat. O cheie de rezervă poate fi adăugată numai dacă este disponibilă o cheie activă.

O cheie pentru o licență trial poate fi adăugată numai drept cheie activă. Aceasta nu poate fi adăugată drept cheie de rezervă. O cheie pentru licență trial nu poate înlocui cheia activă pentru o licență pentru versiune comercială.

Dacă se adaugă o cheie la lista de chei interzise, funcționalitatea aplicației definită de licența utilizată pentru activarea aplicației rămâne disponibilă timp de opt zile. Aplicația notifică utilizatorul că cheia a fost adăugată la lista de chei interzise. După opt zile, funcționarea aplicației devine limitată la nivelul de funcționare care este disponibil după expirarea licenței. Poți să utilizezi componentele de protecție și control și să execuți o scanare utilizând bazele de date ale aplicației instalate înainte de expirarea licenței. De asemenea, aplicația continuă să cripteze fișiere care au fost modificate și criptate înainte de expirarea licenței, dar nu criptează fișiere noi. Utilizarea Kaspersky Security Network nu este disponibilă.

Despre codul de activare

Un *cod de activare* este o secvență unică de 20 de caractere alfanumerice. Introduceți un cod de activare pentru a adăuga o cheie de licență care activează Kaspersky Endpoint Security. Primiți un cod de activare pe adresa de e-mail pe care ați specificat-o după achiziționarea Kaspersky Endpoint Security.

Pentru a activa aplicația folosind un cod de activare, este necesar acces la Internet pentru conectarea la serverele de activare Kaspersky.

Atunci când aplicația este activată folosind un cod de activare, este adăugată cheia activă. O cheie de rezervă poate fi adăugată numai folosind un cod de activare și nu poate fi adăugată folosind un fișier cheie.

Dacă se pierde un cod de activare după activarea aplicație, îl poți restaura. Este posibil să ai nevoie de un cod de activare, de exemplu, pentru a înregistra un cont Kaspersky CompanyAccount. În cazul în care ați pierdut codul de activare după activarea aplicației, contactați partenerul Kaspersky de la care ați cumpărat licența.

Despre fișierul cheie

Un *fișier cheie* este un fișier cu extensia .key pe care-l primești de la Kaspersky. Scopul unui fișier cheie este acela de a adăuga o cheie de licență care activează aplicația.

Primiți un fișier cheie la adresa de e-mail pe care ați furnizat-o atunci când ați achiziționat Kaspersky Endpoint Security sau ați comandat versiunea trial a Kaspersky Endpoint Security.

Nu trebuie să te conectezi la serverele de activare Kaspersky pentru a activa aplicația cu un fișier cheie.

Poți recupera un fișier cheie dacă acesta a fost șters în mod accidental. Vei avea nevoie de un fișier cheie pentru a înregistra un cont Kaspersky CompanyAccount, de exemplu.

Pentru a recupera un fișier cheie, procedează într-unul din modurile următoare:

- Contactează vânzătorul licenței.
- Obține un fișier cheie de pe site-ul Web Kaspersky, pe baza codului de activare existent.
- Obține un fișier cheie de la alt Server de administrare.

Atunci când aplicația este activată folosind un fișier cheie, este adăugată o cheie activă. O cheie de rezervă poate fi adăugată numai folosind un fișier cheie și nu poate fi adăugată folosind un cod de activare.

Comparația funcționalității aplicației în funcție de tipul licenței pentru stații de lucru

Setul de funcționalități Kaspersky Endpoint Security disponibil pe stațiile de lucru depinde de tipul licenței (consultați tabelul de mai jos).

[Consultați, de asemenea, comparația funcționalității aplicației pentru servere]

Pentru o comparație între funcționalitățile aplicației în funcție de tipul de licență Kaspersky Next, consultați Ajutor Kaspersky Next.

Comparație a caracteristicilor aplicației Kaspersky Endpoint Security

Caracteristică	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	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Advanced Threat Protection								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
Behavior Detection	✓	✓	✓	✓	✓	✓	✓	✓
Anti-Cryptor	✓	✓	✓	✓	✓	✓	✓	✓
Exploit Prevention	✓	✓	✓	✓	✓	✓	✓	✓
Host Intrusion Prevention	✓	✓	✓	✓	✓	✓	✓	✓
Remediation Engine	✓	✓	✓	✓	✓	✓	✓	✓
Essential Threat Protection								
File Threat Protection	✓	✓	✓	✓	✓	✓	✓	✓
Web Threat Protection	✓	✓	✓	✓	✓	✓	✓	✓
Mail Threat Protection	✓	✓	✓	✓	✓	✓	✓	✓
Firewall	✓	✓	✓	✓	✓	✓	✓	✓
Network Threat Protection	✓	✓	✓	✓	✓	✓	✓	✓
BadUSB Attack Prevention	✓	✓	✓	✓	✓	✓	✓	✓
Protecție AMSI	✓	✓	✓	✓	✓	✓	✓	✓
Security Controls								
Inspecție jurnal	–	–	–	–	–	–	–	–
Application Control	✓	✓	✓	✓	✓	✓	✓	✓
Control dispozitive	✓	✓	✓	✓	✓	✓	✓	✓
Control Web	✓	✓	✓	✓	✓	✓	✓	✓
Control adaptiv al anomaliilor	–	✓	✓	✓	✓	✓	–	✓
Monitorizare integritate sistem	–	–	–	–	–	–	–	–
Data Encryption								
Kaspersky Disk Encryption	–	✓	✓	✓	✓	✓	–	✓
BitLocker Drive Encryption	–	✓	✓	✓	✓	✓	–	✓

Caracteristică	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	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
File Level Encryption	–	✓	✓	✓	✓	✓	–	✓
Criptare unități amovibile	–	✓	✓	✓	✓	✓	–	✓
Detection and Response								
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓	–	–
Kaspersky Sandbox *(licența Kaspersky Sandbox trebuie achiziționată separat)*	✓	✓	✓	✓	✓	✓	✓	✓
Integrare cu KUMA *(licența pentru integrarea KUMA trebuie achiziționată separat)*	✓	✓	✓	✓	✓	✓	✓	✓
Modul Light Agent *(pentru a activa aplicația, trebuie să adaugi o cheie de licență la SVM-ul la care este conectat Light Agent)*	–	–	–	–	–	–	✓	✓

Compararea funcționalității aplicației în funcție de tipul licenței pentru servere

Setul de funcționalități Kaspersky Endpoint Security disponibil pe servere depinde de tipul licenței (consultați tabelul de mai jos).

Consultați, de asemenea, comparația funcționalității aplicației pentru stații de lucru

Pentru o comparație între funcționalitățile aplicației în funcție de tipul de licență Kaspersky Next, consultați Ajutor Kaspersky Next.

Caracteristică	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	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Advanced Threat Protection								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
Behavior Detection	✓	✓	✓	✓	✓	✓	✓	✓
Anti-Cryptor	✓	✓	✓	✓	✓	✓	✓	✓
Exploit Prevention	✓	✓	✓	✓	✓	✓	✓	✓
Host Intrusion Prevention	–	–	–	–	–	–	–	–
Remediation Engine	✓	✓	✓	✓	✓	✓	✓	✓
Essential Threat Protection								
File Threat Protection	✓	✓	✓	✓	✓	✓	✓	✓
Web Threat Protection	–	✓	✓	✓	✓	✓	✓	✓
Mail Threat Protection	–	✓	✓	✓	✓	✓	✓	✓
Firewall	✓	✓	✓	✓	✓	✓	✓	✓
Network Threat Protection	✓	✓	✓	✓	✓	✓	✓	✓
BadUSB Attack Prevention	✓	✓	✓	✓	✓	✓	✓	✓
Protecție AMSI	✓	✓	✓	✓	✓	✓	✓	✓
Security Controls								
Inspecție jurnal	–	–	–	–	–	–	–	✓
Application Control	–	✓	✓	✓	✓	✓	–	✓
Control dispozitive	–	✓	✓	✓	✓	✓	✓	✓
Control Web	–	✓	✓	✓	✓	✓	✓	✓
Control adaptiv al anomaliilor	–	–	–	–	–	–	–	–
Monitorizare integritate sistem	–	–	–	–	–	–	–	✓
Data Encryption								
Kaspersky Disk Encryption	–	–	–	–	–	–	–	–
BitLocker Drive Encryption	–	✓	✓	✓	✓	✓	–	✓
File Level Encryption	–	–	–	–	–	–	–	–
Criptare unități amovibile	–	–	–	–	–	–	–	–
Detection and Response								

Caracteristică	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	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓	–	–
Kaspersky Sandbox *(licența Kaspersky Sandbox trebuie achiziționată separat)*	✓	✓	✓	✓	✓	✓	✓	✓
Integrare cu KUMA *(licența pentru integrarea KUMA trebuie achiziționată separat)*	✓	✓	✓	✓	✓	✓	✓	✓
Modul Light Agent *(pentru a activa aplicația, trebuie să adaugi o cheie de licență la SVM-ul la care este conectat Light Agent)*	–	–	–	–	–	–	✓	✓

Activarea aplicației

Activarea este procesul de activare a unei licențe care îți permite să folosești o versiune complet funcțională a aplicației, până când licența expiră. Procesul de activare a aplicației implică adăugarea unei chei de licență.

Poți activa aplicația folosind unul din următoarele moduri:

- Local, din interfața aplicației, utilizând Expertul de activare. În acest mod puteți adăuga atât cheia activă, cât și o cheie de rezervă.
- La distanță, utilizând suita programului Kaspersky Security Center.
  - Utilizarea activității *Adaugă cheie*.

    Această metodă îți permite să adaugi o cheie unui anumit computer sau unor computere care fac parte dintr-un grup de administrare. În acest mod puteți adăuga atât cheia activă, cât și o cheie de rezervă.
  - Prin distribuirea unei chei, care este stocată pe Serverul de administrare Kaspersky Security Center, către computere.

    Această metodă îți permite să adaugi automat o cheie la computerele deja conectate la Kaspersky Security Center și la computere noi. Pentru a utiliza această metodă, mai întâi trebuie să adăugați cheia pe Serverul de administrare Kaspersky Security Center. Pentru detalii suplimentare despre adăugarea cheilor pe Kaspersky Security Center Administration Server, consultați secțiunea Ajutor pentru Kaspersky Security Center.

    Codul de activare achiziționat în baza abonamentului este distribuit primul.

- Prin adăugarea cheii la pachetul de instalare Kaspersky Endpoint Security.

  Această metodă vă permite să adăugați cheia în Proprietăți pachet de instalare în timpul implementării Kaspersky Endpoint Security. Aplicația se activează automat după instalare.

- Folosind linia de comandă.

Poate dura ceva timp până când aplicația este activată folosind un cod de activare (indiferent că este vorba despre o instalare la distanță sau neinteractivă), din cauza distribuirii încărcării între serverele de activare ale Kaspersky. Dacă trebuie să activezi aplicația imediat, poți întrerupe procesul de activare în curs și poți începe activarea folosind Expertul de activare.

Dacă Kaspersky Endpoint Security este utilizat în modul Light Agent pentru a proteja mediile virtuale, nu este necesar să activezi aplicația separat.

Activarea aplicației

Cum să activați aplicația în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **New task**.

   Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Selectarea tipului activității

Selectați **Kaspersky Endpoint Security for Windows (14.1)** → **Adaugă cheie**.

Pasul 2. Adăugarea unei chei

Introduceți un cod de activare sau selectați un fișier cheie.

Pentru detalii suplimentare despre adăugarea cheilor în depozitul Kaspersky Security Center, consultați secțiunea Ajutor pentru Kaspersky Security Center.

Pasul 3. Selectarea dispozitivelor cărora le va fi atribuită activitatea

Selectați computerele pe care se va efectua activitatea. Sunt disponibile următoarele opțiuni:

- Atribuirea activității unui grup de administrare. În acest caz, activitatea este atribuită computerelor incluse într-un grup de administrare creat anterior.
- Selectare computere detectate în rețea de Serverul de administrare: *dispozitive neatribuite*. Dispozitivele specifice pot include dispozitive din grupuri de administrare, precum și dispozitive neatribuite.
- Specificarea manuală a adreselor computerelor sau importarea adreselor dintr-o listă. Poți specifica nume NetBIOS, adrese IP și subrețele IP ale dispozitivelor cărora dorești să le atribui activitatea.

Pasul 4. Configurarea unei planificări de pornire a activității

Configurați o planificare pentru începerea unei activități, de exemplu, manual sau atunci când computerul este inactiv.

Pasul 5. Definirea numelui activității

Introduceți un nume pentru activitate, cum ar fi *Activare Kaspersky Endpoint Security for Windows*.

Pasul 6. Finalizarea creării activității

Ieșiți din Expert. Dacă este necesar, bifați caseta de selectare **Run the task after the wizard finishes**. Puteți monitoriza progresul activității în proprietățile activității. Ca rezultat, aplicația Kaspersky Endpoint Security va fi activată pe computerele utilizatorilor în modul silențios.

Cum se activează aplicația în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **Add**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Configurarea setările generale ale activității

Configurați setările generale pentru activitate:

1. În lista verticală **Application**, selectează **Kaspersky Endpoint Security for Windows 14.1.0**.
2. În lista verticală **Task type**, selectează **Add key**.
3. În câmpul **Task name**, introdu o descriere succintă, de exemplu *Activare Kaspersky Endpoint Security for Windows*.
4. În blocul **Devices to which the task will be assigned**, selectați domeniul activității. Mergeți la pasul următor.

Pasul 2. Selectarea dispozitivelor cărora le va fi atribuită activitatea

Selectați computerele pe care se va efectua activitatea. Sunt disponibile următoarele opțiuni:

- Atribuirea activității unui grup de administrare. În acest caz, activitatea este atribuită computerelor incluse într-un grup de administrare creat anterior.
- Selectare computere detectate în rețea de Serverul de administrare: *dispozitive neatribuite*. Dispozitivele specifice pot include dispozitive din grupuri de administrare, precum și dispozitive neatribuite.
- Specificarea manuală a adreselor computerelor sau importarea adreselor dintr-o listă. Poți specifica nume NetBIOS, adrese IP și subrețele IP ale dispozitivelor cărora dorești să le atribui activitatea.

Pasul 3. Selectarea unei licențe

Selectați licența pe care doriți să o utilizați pentru a activa aplicația. Mergeți la pasul următor.

Puteți adăuga chei la Consola Web (**Operations** → **Licensing**).

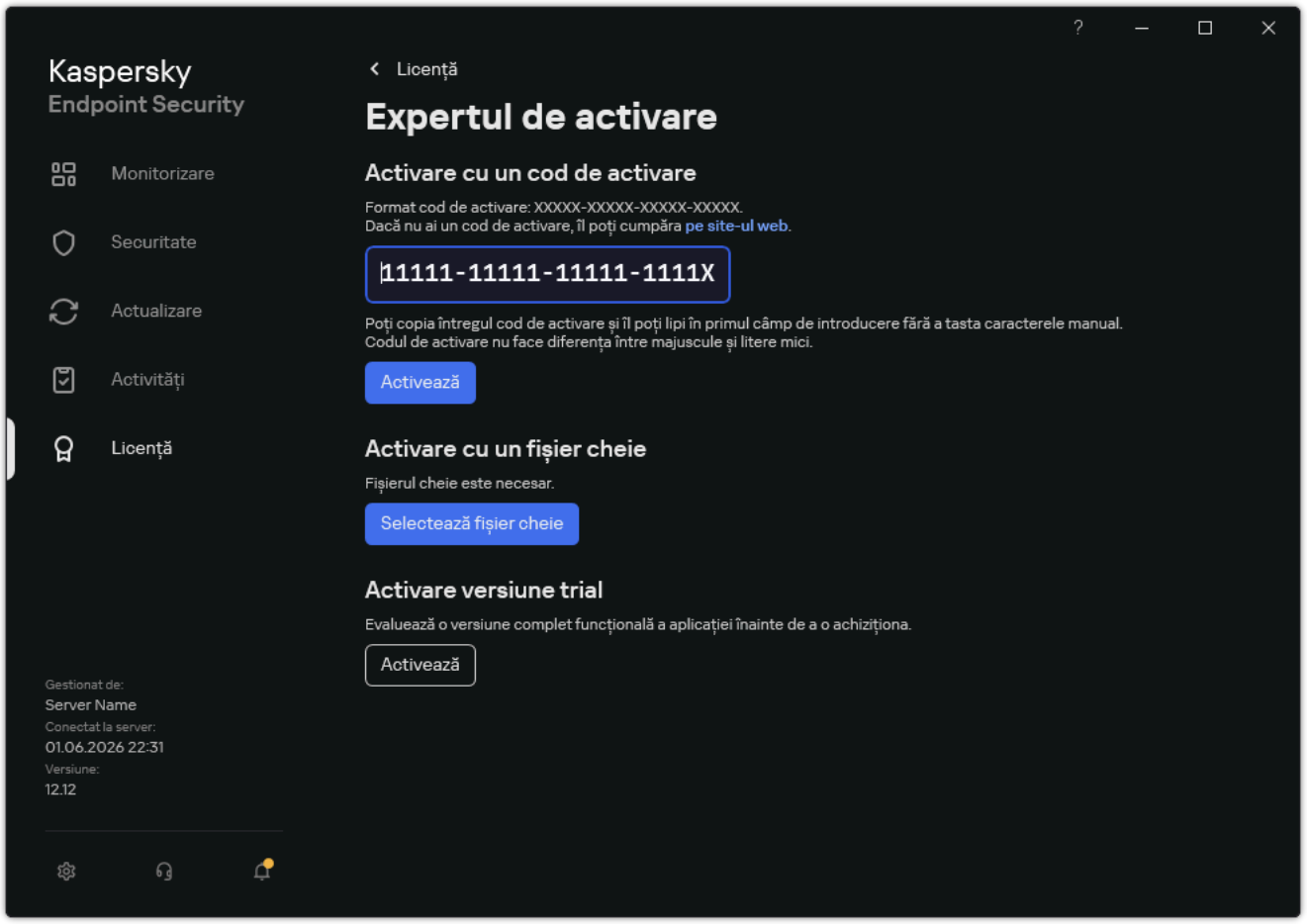
Pasul 4. Finalizarea creării activității

Termină expertul făcând clic pe butonul **Finish**. Se va afișa o activitate nouă în lista de activități. Pentru a executa o activitate, bifează caseta de selectare de lângă activitate și fă clic pe butonul **Start**. Ca rezultat, aplicația Kaspersky Endpoint Security va fi activată pe computerele utilizatorilor în modul silențios.

Cum se activează aplicația în interfața aplicației

1. În fereastra principală a aplicației, accesați secțiunea **Licență**.
2. Fă clic pe **Activează aplicația utilizând o licență nouă**.

Expertul de activare a aplicației pornește. Urmează instrucțiunile din Expertul de activare.



Activarea aplicației

În proprietățile activității *Adaugă cheie*, puteți adăuga o cheie de rezervă computerului. O *cheie de rezervă* devine activă atunci când cheia activă expiră. Disponibilitatea unei chei de rezervă vă permite să evitați limitările pentru funcționalitatea aplicației atunci când o licență expiră.

Cum se adaugă automat o cheie de licență pe computere prin Consola de administrare (MMC)

1. În Consola de administrare, accesează directorul **Kaspersky Licenses**.

   Se deschide o listă de chei de licență.

2. Deschideți proprietățile cheii de licență.

3. În secțiunea **General**, bifați caseta de selectare **Automatically distribute license key to managed devices**.

4. Salvați-vă modificările.

   Ca rezultat, cheia va fi distribuită automat către computerele corespunzătoare. În timpul distribuirii automate a unei chei drept cheie activă sau cheie de rezervă, este luată în considerare limita de licențiere privind numărul de computere (setată în proprietățile cheii). Dacă se atinge limita de licențiere, distribuirea acestei chei către computere încetează automat. Puteți vizualiza numărul de computere la care a fost adăugată cheia și alte date din proprietățile cheii în secțiunea **Devices**.

Cum se adaugă automat o cheie de licență pe computere prin Web Console și Cloud Console

1. În fereastra principală a componentei Web Console, selectați **Operations → Licensing → Licenses**.

   Se deschide o listă de chei de licență.

2. Deschideți proprietățile cheii de licență.

3. În fila **General**, activează comutatorul **Automatically distribute license key to managed devices**.

4. Salvați-vă modificările.

Ca rezultat, cheia va fi distribuită automat către computerele corespunzătoare. În timpul distribuirii automate a unei chei drept cheie activă sau cheie de rezervă, este luată în considerare limita de licențiere privind numărul de computere (setată în proprietățile cheii). Dacă se atinge limita de licențiere, distribuirea acestei chei către computere încetează automat. Poți vizualiza numărul de computere la care a fost adăugată cheia și alte date din proprietățile cheii din fila **Devices**.

Dacă activezi aplicația folosind un *cod de activare*, ai nevoie de acces la Internet pentru conectarea la serverele de activare Kaspersky. Dacă activezi aplicația cu a *fișier cheie*, accesul la internet nu este necesar. În cazul în care computerele se află într-un segment de rețea izolat, fără acces la internet, pentru a activa aplicația cu un cod, trebuie să permiți utilizarea serverului de administrare Kaspersky Security Center ca server proxy. Adică, aplicația poate obține acces la serverele de activare prin serverul de administrare care are acces la internet.

Cum se permite utilizarea serverului de administrare ca server proxy pentru activarea aplicației în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.

2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

3. În fereastra politicii, selectați **Setări generale** → **Setări aplicație**.

4. Bifați caseta de selectare **Utilizează Kaspersky Security Center ca server proxy pentru activare**.

5. Salvați-vă modificările.

Cum se permite utilizarea serverului de administrare ca server proxy pentru activarea aplicației în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **General Settings** → **KSC Integration**.

5. Bifați caseta de selectare **Use Kaspersky Security Center as proxy server for activation**.

6. Salvați-vă modificările.

Dacă nu poți activa aplicația cu un *cod de activare*, poți încerca să obții un *fișier cheie* folosind soluția Kaspersky și încercând să activezi din nou aplicația folosind o altă metodă.

Monitorizarea utilizării licenței

Poți monitoriza utilizarea licențelor în următoarele moduri:

- Vizualizează *Report on usage of license keys* pentru infrastructura organizației (**Monitoring** → **Reports**).
- Vizualizează stările computerelor în fila **Managed devices** → **Devices**. Dacă aplicația nu este activată, computerul va avea starea ⚠ *Aplicația nu este activată*.
- Vizualizează informațiile despre licență în proprietățile computerului.
- Vizualizează proprietățile cheii (**Operations** → **Licensing**).

Specificații privind activarea aplicației ca parte a Kaspersky Security Center Cloud Console

O versiune trial este furnizată pentru Kaspersky Security Center Cloud Console. *Versiunea trial* este o versiune specială a Kaspersky Security Center Cloud Console, concepută pentru a familiariza un utilizator cu caracteristicile aplicației. În această versiune, puteți efectua acțiuni într-un spațiu de lucru pentru o perioadă de 30 de zile. Toate aplicațiile gestionate sunt executate în mod automat sub o licență pentru versiunea trial pentru Kaspersky Security Center Cloud Console, inclusiv Kaspersky Endpoint Security. Cu toate acestea, nu puteți activa Kaspersky Endpoint Security utilizând propria sa licență pentru versiunea trial când licența pentru versiunea trial pentru Kaspersky Security Center Cloud Console expiră. Pentru informații detaliate despre licențierea aplicației Kaspersky Security Center, consultați Ajutor pentru Kaspersky Security Center Cloud Console.

> Versiunea trial a Kaspersky Security Center Cloud Console nu vă permite să treceți ulterior la o versiune comercială. Orice spațiu de lucru în versiune trial va fi șters automat cu tot conținutul său după expirarea perioadei de 30 de zile.

Eliminarea unei chei de licență

Pentru a elimina o cheie de licență, trebuie să executi o activitate specială pe computerele tale. Poți elimina o cheie de licență, de exemplu, pentru a rearanja unitățile de licențiere. De asemenea, când licența expiră, Kaspersky Endpoint Security te notifică. Dacă ai adăugat o cheie de licență cu un termen scurt pentru a încerca aplicația (de exemplu, suplimentul EDR Optimum), poți elimina această cheie de licență pentru a scăpa de notificări și pentru a remedia starea computerului.

Activitatea *Elimină cheia* permite eliminarea oricăror chei de licență de pe computer. Poți elimina cheile de licență active, precum și cheile de licență de rezervă. Pe lângă cheia de licență de activare a Kaspersky Endpoint Security, poți elimina cheile de licență individuale ale soluțiilor Kaspersky Detection and Response (de exemplu, suplimentul EDR Optimum).

Cum se elimină o cheie de licență în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **New task**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Selectarea tipului activității

Selectați **Kaspersky Endpoint Security for Windows (14.1)** → **Elimină cheia**.

Pasul 2. Selectarea unei licențe

Selectează cheia de licență pe care dorești să o ștergi. Poți selecta o cheie de licență din depozitul de chei Kaspersky Security Center sau puteți selecta un fișier cheie.

Pasul 3. Selectarea dispozitivelor cărora le va fi atribuită activitatea

Selectați computerele pe care se va efectua activitatea. Sunt disponibile următoarele opțiuni:

- Atribuirea activității unui grup de administrare. În acest caz, activitatea este atribuită computerelor incluse într-un grup de administrare creat anterior.
- Selectare computere detectate în rețea de Serverul de administrare: *dispozitive neatribuite*. Dispozitivele specifice pot include dispozitive din grupuri de administrare, precum și dispozitive neatribuite.
- Specificarea manuală a adreselor computerelor sau importarea adreselor dintr-o listă. Poți specifica nume NetBIOS, adrese IP și subrețele IP ale dispozitivelor cărora dorești să le atribui activitatea.

Pasul 4. Configurarea unei planificări de pornire a activității

Configurați o planificare pentru începerea unei activități, de exemplu, manual sau atunci când computerul este inactiv.

Pasul 5. Definirea numelui activității

Introdu un nume pentru activitate, de exemplu, *Elimină cheia pentru versiunea beta*.

Pasul 6. Finalizarea creării activității

Ieșiți din Expert. Dacă este necesar, bifați caseta de selectare **Run the task after the wizard finishes**. Puteți monitoriza progresul activității în proprietățile activității.

Cum se elimină o cheie de licență din Web Console

1. În fereastra principală a Web Console, selectează **Tasks**.
   Lista activităților se deschide.
2. Fă clic pe **Add**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Configurarea setările generale ale activității

Configurați setările generale pentru activitate:

1. În lista verticală **Application**, selectează **Kaspersky Endpoint Security for Windows 14.1.0**.
2. În lista verticală **Task type**, selectează **Remove key**.
3. În câmpul **Task name**, introdu o descriere succintă, de exemplu *Elimină cheia pentru versiunea beta*.
4. În blocul **Devices to which the task will be assigned**, selectați domeniul activității. Mergeți la pasul următor.

Pasul 2. Selectarea dispozitivelor cărora le va fi atribuită activitatea

Selectați computerele pe care se va efectua activitatea. Sunt disponibile următoarele opțiuni:

- Atribuirea activității unui grup de administrare. În acest caz, activitatea este atribuită computerelor incluse într-un grup de administrare creat anterior.
- Selectare computere detectate în rețea de Serverul de administrare: *dispozitive neatribuite*. Dispozitivele specifice pot include dispozitive din grupuri de administrare, precum și dispozitive neatribuite.
- Specificarea manuală a adreselor computerelor sau importarea adreselor dintr-o listă. Poți specifica nume NetBIOS, adrese IP și subrețele IP ale dispozitivelor cărora dorești să le atribui activitatea.

Pasul 3. Selectarea unei licențe

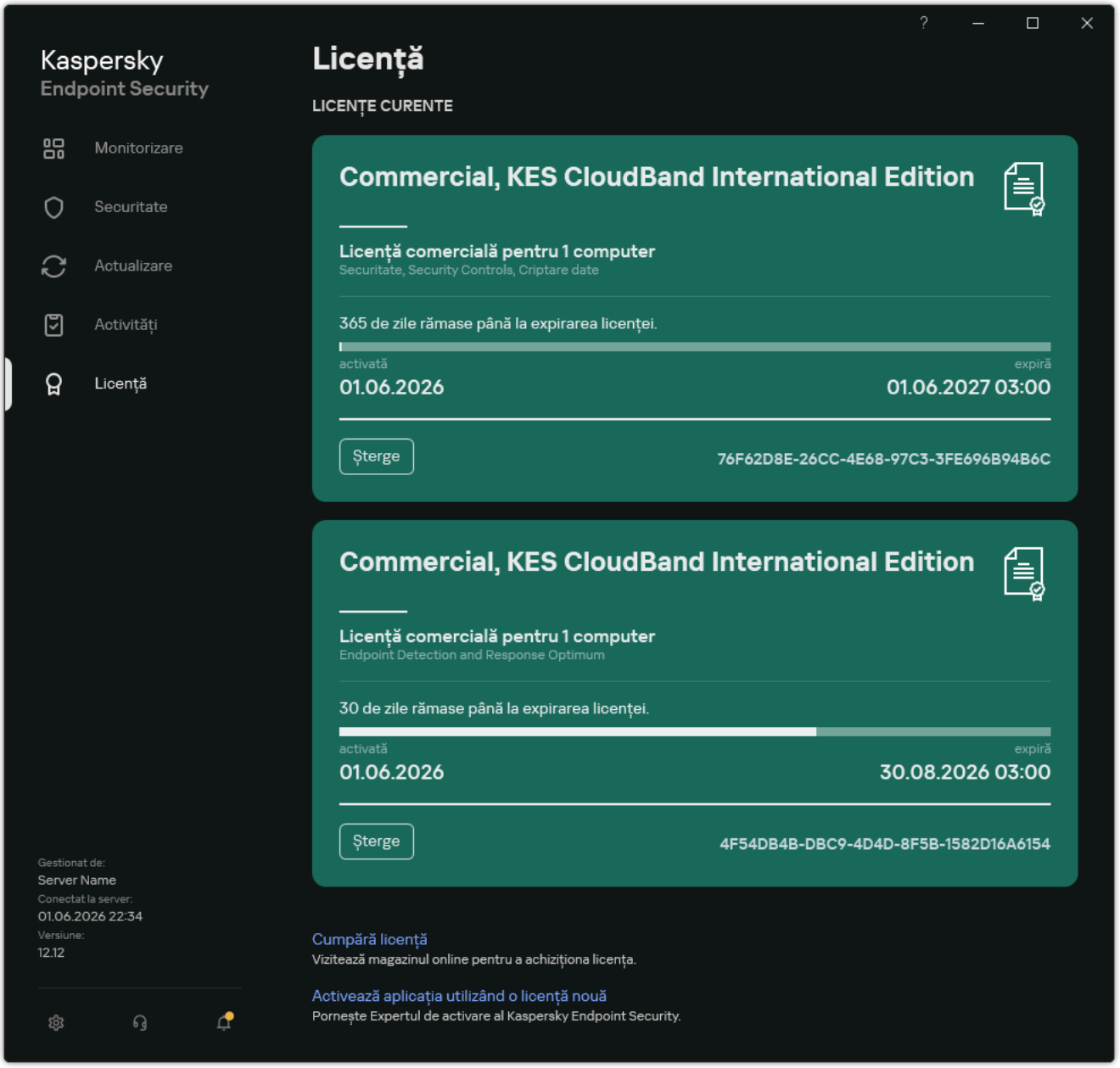
Selectează cheia de licență pe care dorești să o ștergi. Poți selecta o cheie de licență din depozitul de chei Kaspersky Security Center sau puteți selecta un fișier cheie. Mergeți la pasul următor.

Pasul 4. Finalizarea creării activității

Termină expertul făcând clic pe butonul **Finish**. Se va afișa o activitate nouă în lista de activități. Pentru a executa o activitate, bifează caseta de selectare de lângă activitate și fă clic pe butonul **Start**.

Cum se elimină o cheie de licență în interfața aplicației

1. În fereastra principală a aplicației, accesați secțiunea **Licență**.
2. Selectează cheia pe care dorești să o ștergi și fă clic pe **Șterge**.



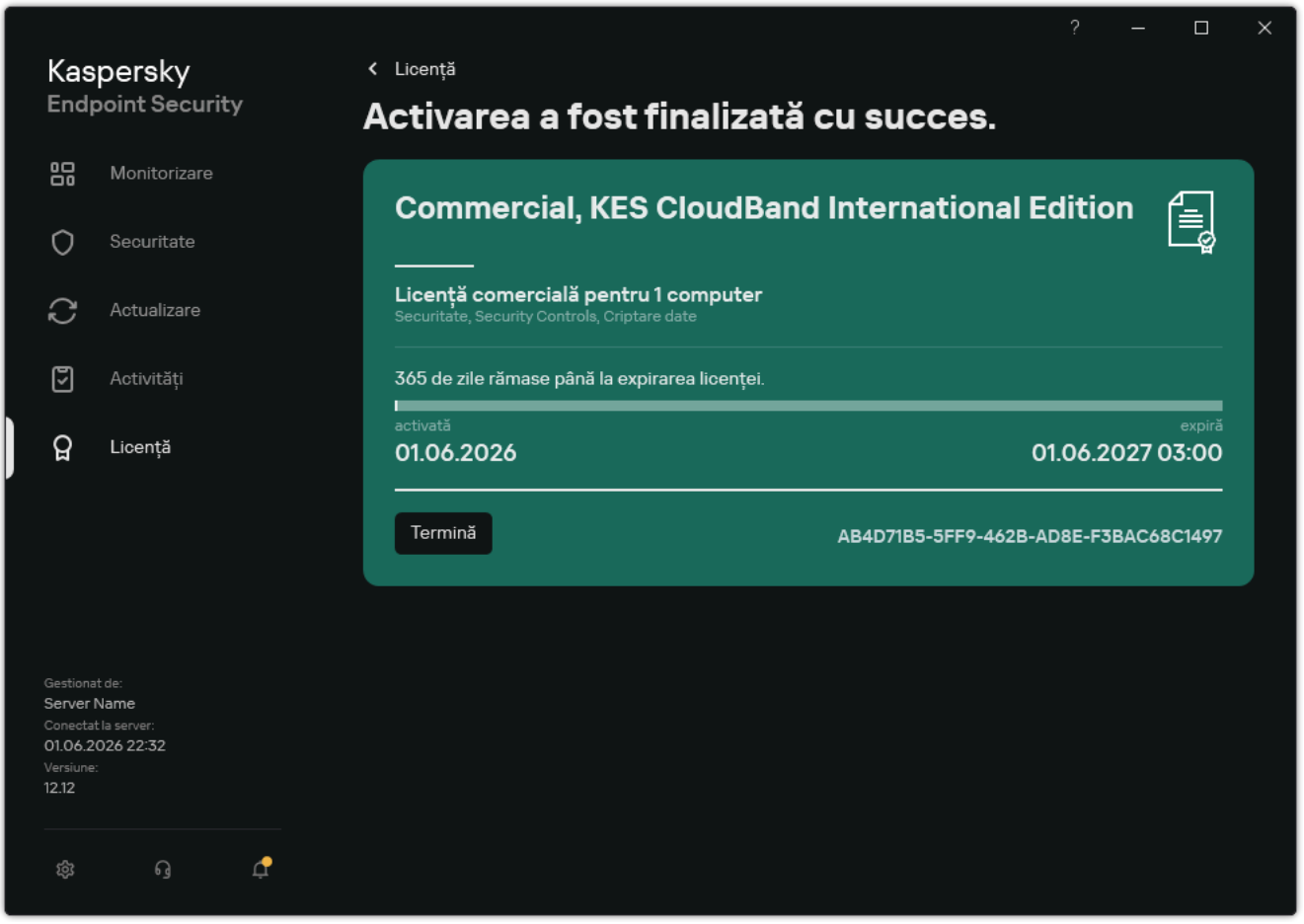
Fereastra Licențiere

De asemenea, poți elimina o cheie de licență în linia de comandă.

Vizualizarea informațiilor despre licență

Pentru a vizualiza informații despre o licență:

În fereastra principală a aplicației, accesați secțiunea **Licență** (consultați figura de mai jos).



Fereastra Licențiere

Sectiunea afișează următoarele detalii:

- *Stare cheie*. Pe un computer pot fi stocate mai multe chei. Există două tipuri de chei: active și de rezervă. Aplicația nu poate avea mai mult de o singură cheie activă. O cheie de rezervă poate deveni activă numai după ce expiră cheia activă sau după ce aceasta a fost ștearsă utilizând butonul **Șterge**.
- *Nume aplicație*. Numele complet al aplicației Kaspersky achiziționată.
- *Tip licență*. Sunt disponibile următoarele tipuri de licențe: trial și comercială.
- *Funcționalitate*. Caracteristicile aplicației care sunt disponibile cu licența dvs. Caracteristicile pot include Protecție, Security Controls, Data Encryption și altele. Lista funcțiilor disponibile este, de asemenea, furnizată în Certificatul de licență.

- *Informații suplimentare despre licență*. Data de începere și data de încheiere a termenului licenței (numai pentru cheia activă), durata rămasă a termenului licenței.

  Ora expirării licenței se afișează în funcție de fusul orar configurat în sistemul de operare.

- *Cheie*. O cheie este o secvență alfanumerică unică care este generată dintr-un cod de activare sau un fișier cheie.

În fereastra Licențiere, poți efectua, de asemenea, una dintre următoarele acțiuni:

- **Cumpără licență** / **Reînnoiește licența**. Deschide site-ul Web al magazinului Kaspersky, unde poți să achiziționezi sau să reînnoiești o licență. Pentru a face acest lucru, introdu informațiile despre companie și plătește pentru comandă.

- **Activează aplicația utilizând o licență nouă**. Pornește Expertul de activare a aplicației. În acest expert poți adăuga o cheie utilizând un cod de activare sau un fișier cheie. Expertul de activare a aplicației vă permite să adaugați o cheie activă și numai o singură cheie de rezervă.

Achiziționarea unei licențe

Poți achiziționa o licență după instalarea aplicației. După achiziționarea unei licențe, veți primi un cod de activare sau un fișier cheie pentru activarea aplicației.

Pentru a achiziționa o licență:

1. În fereastra principală a aplicației, accesați secțiunea **Licență**.

2. Efectuează una dintre următoarele acțiuni:

   - Dacă nu au fost adăugate chei sau a fost adăugată o cheie pentru o licență trial, faceți clic pe butonul **Cumpără licență**.

   - Dacă este adăugată cheia pentru o licență pentru versiune comercială, faceți clic pe butonul **Reînnoiește licența**.

   Se va deschide o fereastră cu magazinul online Kaspersky, unde poți achiziționa o licență.

Reînnoirea abonamentului

Atunci când folosești aplicația în baza unui abonament, Kaspersky Endpoint Security contactează în mod automat serverul de activare la intervale specificate, până când abonamentul tău expiră.

Dacă folosești aplicația în baza unui abonament nelimitat, Kaspersky Endpoint Security verifică în fundal serverul de activare pentru a găsi eventuale chei reînnoite. Dacă pe serverul de activare este disponibilă o cheie, aplicația o adaugă, înlocuind cheia anterioară. Astfel, abonamentul nelimitat pentru Kaspersky Endpoint Security este reînnoit fără implicarea utilizatorului.

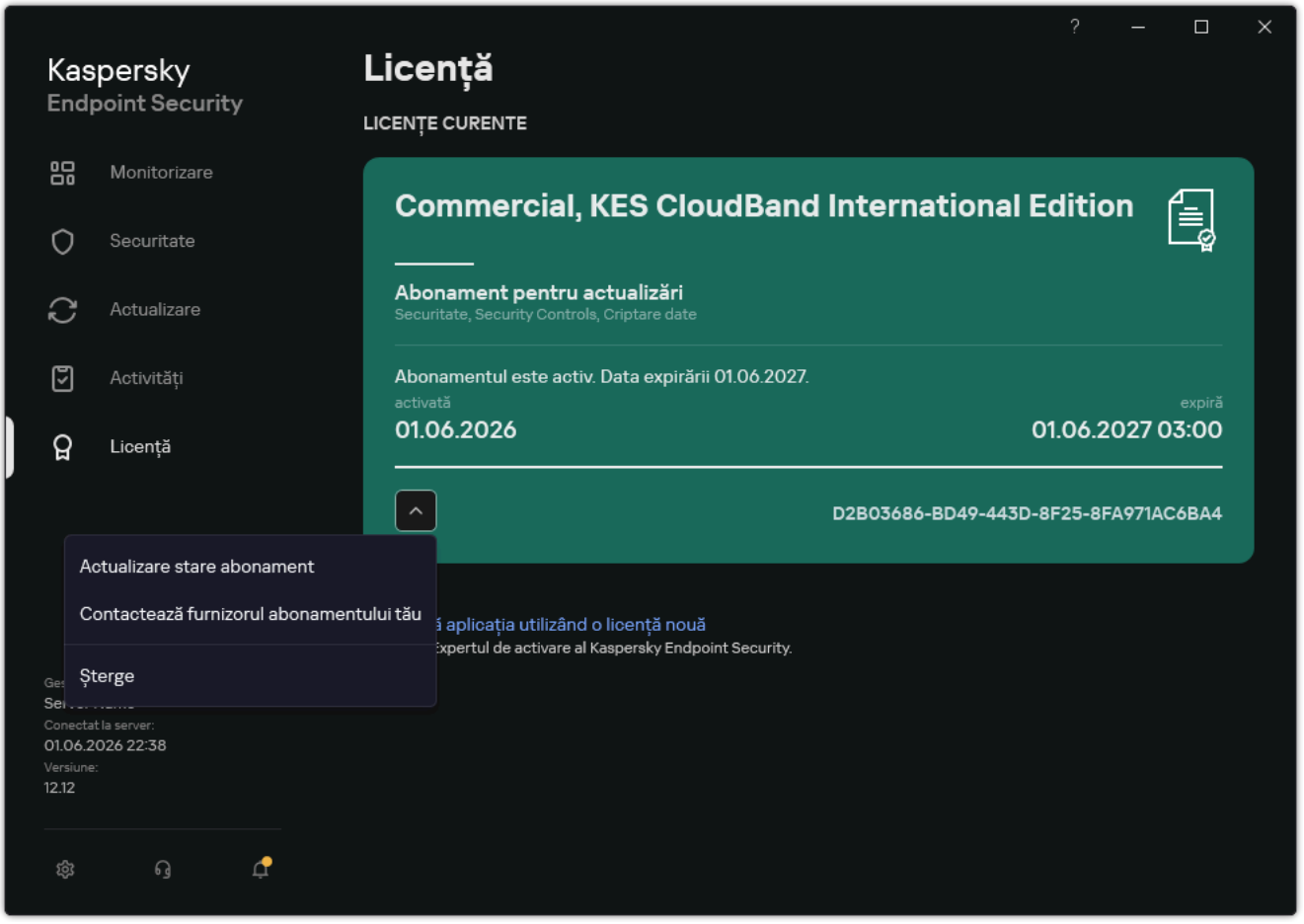
Dacă folosești aplicația cu abonament limitat, la data expirării abonamentului (sau la data expirării perioadei de grație pentru reînnoirea abonamentului), Kaspersky Endpoint Security te anunță despre acest lucru și oprește încercarea de reînnoire automată a abonamentului. În acest caz, Kaspersky Endpoint Security se comportă la fel ca atunci când expiră o licență pentru versiune comercială pentru aplicație: aplicația operează fără actualizări, iar Kaspersky Security Network nu este disponibil.

Vă puteți reînnoi abonamentul pe site-ul Web al furnizorului de servicii.

Pentru a vizita site-ul Web al furnizorului de servicii din interfața aplicației:

1. În fereastra principală a aplicației, accesați secțiunea **Licență**.
2. Fă clic pe **Contactează furnizorul abonamentului tău**.

Puteți actualiza manual starea abonamentului. Acest lucru poate fi necesar dacă abonamentul a fost reînnoit după perioada de grație și aplicația nu a actualizat automat starea abonamentului.



Reînnoirea abonamentului

Noțiuni de bază

După instalarea Kaspersky Endpoint Security, puteți gestiona aplicația folosind următoarele interfețe:

- Interfața aplicației locale.
- Consola de administrare Kaspersky Security Center.
- Kaspersky Security Center Web Console.
- Kaspersky Security Center Cloud Console.

Consola de administrare Kaspersky Security Center

De la distanță, Kaspersky Security Center îți permite să instalezi și să dezinstalezi, să pornești și să oprești Kaspersky Endpoint Security, să configurezi setările aplicației, să modifici setul de componente ale aplicației disponibile, să adaugi chei și să pornești și să oprești activități de actualizare și scanare.

Aplicația poate fi gestionată prin Kaspersky Security Center folosind Plug-inul de gestionare Kaspersky Endpoint Security.

Pentru mai multe detalii despre gestionarea aplicației prin intermediul Kaspersky Security Center, consultați Ajutor pentru Kaspersky Security Center.

Kaspersky Security Center Web Console și Kaspersky Security Center Cloud Console

Kaspersky Security Center Web Console (denumită în continuare *Web Console*) este o aplicație web destinată efectuării centralizate a activităților principale de gestionare și întreținere a sistemului de securitate al rețelei unei organizații. Web Console este o componentă a Kaspersky Security Center care furnizează interfață cu utilizatorul. Pentru informații detaliate despre Kaspersky Security Center Web Console, consultați Ajutor pentru Kaspersky Security Center.

Kaspersky Security Center Cloud Console (denumită în continuare „*Cloud Console*") este o soluție bazată pe cloud pentru protejarea și gestionarea rețelei unei organizații. Pentru informații detaliate despre Kaspersky Security Center Cloud Console, consultați Ajutor pentru Kaspersky Security Center Cloud Console.

Web Console și Cloud Console vă permit să faceți următoarele:

- Monitorizează starea sistemului de securitate a organizației.
- Instalează aplicații Kaspersky pe dispozitive din rețea.
- Gestionează aplicații instalate.
- Vizualizează rapoarte despre starea sistemului de securitate.

Gestionarea Kaspersky Endpoint Security prin Web Console, Cloud Console și Consola de Administrare Kaspersky Security Center oferă toate capacități de gestionare diferite. Componentele și activitățile disponibile diferă, de asemenea, pentru diferitele console.

Despre upgrade-ul Plug-inului de gestionare al Kaspersky Endpoint Security for Windows

Plug-in-ul de gestionare Kaspersky Endpoint Security for Windows permite interacțiunea dintre Kaspersky Endpoint Security și Kaspersky Security Center. Plug-in-ul de gestionare îți permite să gestionezi aplicația Kaspersky Endpoint Security utilizând politici, activități și setări pentru aplicațiile locale. Interacțiunea cu Kaspersky Security Center Web Console este asigurată de plug-inul web.

Versiunea Plug-inului de gestionare poate fi diferită de versiunea aplicației Kaspersky Endpoint Security instalată pe computerul client. Dacă versiunea Plug-inului de gestionare instalată are mai puține funcționalități decât versiunea instalată a aplicației Kaspersky Endpoint Security, setările pentru funcțiile care lipsesc nu sunt reglementate de Plug-inul de gestionare. Aceste setări pot fi modificate de utilizator în interfața locală a Kaspersky Endpoint Security.

Plug-inul web nu este instalat în mod implicit în Kaspersky Security Center Web Console. Plug-in-ul web trebuie să fie instalat pe un computer pe care este instalată Consola web Kaspersky Security Center. Funcționalitatea plug-inului web este disponibilă pentru toți administratorii care au acces la Consola Web într-un browser. Poți să vizualizezi lista de plug-inuri web instalate în interfața componentei Web Console (**Console settings** → **Web plug-ins**). Pentru mai multe detalii despre compatibilitatea versiunilor plug-inurilor web și Web Console, consultați Ajutor pentru Kaspersky Security Center.

Dacă utilizezi Kaspersky Endpoint Security ca parte a soluției Kaspersky Endpoint Detection and Response Optimum, trebuie să instalezi plug-in-ul de gestionare Kaspersky Endpoint Detection and Response. Plug-in-ul de gestionare este necesar pentru a afișa detaliile alertelor. *Detalii detecție* este un instrument pentru vizualizarea tuturor informațiilor colectate despre o amenințare detectată. Detaliile detecției includ, de exemplu, istoricul fișierelor care apar pe computer. Astfel, pentru a crea activități de răspuns la amenințări, ai nevoie de plug-in-ul de gestionare Kaspersky Endpoint Security, iar pentru a vizualiza detaliile alertelor, ai nevoie de plug-in-ul de gestionare EDR.

Instalarea plug-inului Web

Poți instala plug-inul Web după cum urmează:

- Instalează plug-inul Web folosind Quick Start Wizard al Kaspersky Security Center Web Console.

  Web Console îți solicită automat să execuți Quick Start Wizard atunci când conectezi prima oară componenta Web Console la Administration Server. Poți, de asemenea, să execuți Quick Start Wizard în interfața Web Console (**Discovery & deployment** → **Deployment & assignment** → **Quick start wizard**). Quick Start Wizard poate, de asemenea, să verifice dacă plug-inurile web instalate sunt actualizate și să descarce actualizările necesare. Pentru mai multe detalii despre Quick Start Wizard pentru Kaspersky Security Center Web Console, consultați Ajutor pentru Kaspersky Security Center.

- Instalarea plug-inului Web din lista de pachete de distribuire disponibile în Web Console.

  Pentru a instala plug-inul web, selectează pachetul de distribuție al plug-inului web Kaspersky Endpoint Security în interfața componentei Web Console (**Console settings** → **Web plug-ins**). Lista pachetelor de distribuție disponibile este actualizată automat după lansarea noilor versiuni ale aplicațiilor Kaspersky.

- Descarcă pachetul de distribuție în Consola Web dintr-o sursă externă.

  Pentru a instala plug-inul web, adaugă arhiva ZIP a pachetului de distribuție pentru plug-inul web Kaspersky Endpoint Security în interfața componentei Web Console (**Console settings** → **Web plug-ins**). Pachetul de distribuție al plug-inului Web poate fi descărcat, de exemplu, de pe site-ul Web Kaspersky.

Începând cu Kaspersky Endpoint Security 12.11 for Windows, procedura de instalare a plug-in-ului web s-a modificat. Pachetul de distribuție include acum două plug-in-uri web: *Kaspersky Endpoint Security for Windows 14.1.0* și *Unified Protection and Management Plug-in*. Acest lucru se datorează trecerii la un singur plug-in web unificat pentru gestionarea aplicațiilor Kaspersky. Plug-in-ul web unificat permite crearea unei singure politici pentru gestionarea mai multor aplicații Kaspersky (de exemplu, Kaspersky Endpoint Security for Windows, macOS și Linux). Tranziția la pluginul web unificat poate dura câteva versiuni. După finalizarea tranziției, pachetul de distribuție va include numai *Unified Protection and Management Plug-in*.

Actualizarea Plug-inului de gestionare

Pentru a actualiza Plug-inul de gestionare Kaspersky Endpoint Security for Windows, descărcați cea mai recentă versiune a plug-inului (inclus în kit-ul de distribuție) și executați expertul de instalare a plug-inului.

Dacă devine disponibilă o versiune nouă a plug-inului Web, Consola Web va afișa notificarea *Updates are available for utilized plug-ins*. Poți continua să actualizezi versiunea plug-inului Web din această notificare a Consolei Web. De asemenea, poți să verifici manual dacă există actualizări noi ale plug-inului web în interfața componentei Web Console (**Console settings** → **Web plug-ins**). Versiunea anterioară a plug-inului Web va fi eliminată automat în timpul actualizării.

> Atunci când se actualizează plug-inul web, se salvează elementele deja existente (de exemplu, politici sau activități). Setările noi ale elementelor care implementează funcții noi ale Kaspersky Endpoint Security vor apărea în elementele existente și vor avea valorile implicite.

Poți actualiza plug-inul Web după cum urmează:

- Actualizează plug-inul Web din lista de plug-inuri Web în modul online.

  Pentru a actualiza plug-inul Web, trebuie să selectezi pachetul de distribuire al plug-inului Web pentru Kaspersky Endpoint Security în interfața componentei Web Console (**Console settings** → **Web plug-ins**). Consola Web verifică dacă există actualizări disponibile pe serverele Kaspersky și descarcă actualizările relevante.

- Actualizează plug-inul Web dintr-un fișier.

  Pentru a actualiza plug-inul web, trebuie să selectezi arhiva ZIP a pachetului de distribuție pentru plug-inului web Kaspersky Endpoint Security în interfața componentei Web Console (**Console settings** → **Web plug-ins**). Pachetul de distribuție al plug-inului Web poate fi descărcat, de exemplu, de pe site-ul Web Kaspersky. Poți să actualizezi plug-inul Web pentru Kaspersky Endpoint Security numai la o versiune mai recentă. Plug-inul Web nu poate fi actualizat la o versiune mai veche.

Dacă este deschis orice element (de exemplu, o politică sau o activitate), plug-inul web verifică informațiile de compatibilitate. Dacă versiunea plug-inului web este aceeași sau ulterioară versiunii specificate în informațiile de compatibilitate, poți modifica setările acestui element. În caz contrar, nu poți folosi plug-inul web pentru a modifica setările elementului selectat. Este recomandat să actualizezi plug-inul Web.

Considerații speciale privind lucrul cu versiuni diferite de plug-inuri de gestionare

Puteți gestiona aplicația Kaspersky Endpoint Security prin intermediul Kaspersky Security Center numai dacă aveți un Plug-in de gestionare a cărui versiune este aceeași sau una ulterioară versiunii specificate în informațiile cu privire la compatibilitatea aplicației Kaspersky Endpoint Security cu Plug-inul de gestionare. Puteți vizualiza versiunea minimă necesară a Plug-in-ului de gestionare în fișierul installer.ini inclus în kitul de distribuție.

Dacă este deschis oricare element(de exemplu, o politică sau o activitate), Plug-inul de gestionare verifică informațiile de compatibilitate. Dacă versiunea Plug-inului de gestionare este aceeași sau ulterioară versiunii specificate în informațiile de compatibilitate, poți modifica setările acestui element. În caz contrar, nu poți folosi Plug-inul de gestionare pentru a modifica setările elementului selectat. Se recomandă upgrade-ul Plug-inului de gestionare.

Dacă Plug-inul de gestionare pentru Kaspersky Endpoint Security este instalat în Consola de administrare, ai în vedere următoarele atunci când instalezi o versiune nouă a Plug-inului de gestionare:

- versiunea anterioară a Plug-inului de gestionare pentru Kaspersky Endpoint Security va fi eliminată;
- versiunea nouă a Plug-inului de gestionare pentru Kaspersky Endpoint Security acceptă gestionarea versiunii anterioare de Kaspersky Endpoint Security for Windows pe computerele utilizatorilor.
- Poți utiliza versiunea nouă a Plug-inului de gestionare pentru a modifica setări în politici, activități și alte elemente create de versiunea anterioară a Plug-inului de gestionare.
- Pentru setările noi, versiunea nouă a Plug-inului de gestionare atribuie valori implicite atunci când o politică, un profil de politică sau o activitate se salvează pentru prima dată.

  După ce faci upgrade pentru Plug-inul de gestionare, este recomandat să verifici și să salvezi valorile setărilor noi din politici și profiluri de politici. Dacă nu faci acest lucru, noile grupuri de setări pentru Kaspersky Endpoint Security de pe computerul utilizatorului vor lua valorile implicite și pot fi editate (atributul). Este recomandat să verifici setările începând cu politicile și profilurile de politici de la nivelul superior al ierarhiei. De asemenea, este recomandat să utilizezi contul de utilizator care are drepturi de acces la toate zonele funcționale ale Kaspersky Security Center.

  Pentru a afla mai multe despre noile capacități ale aplicației, consultați notele de lansare sau ajutorul pentru aplicație.

- Dacă a fost adăugat un parametru nou la un grup de setări din versiunea nouă a Plug-inului de gestionare, starea definită anterior a atributului / pentru acest grup de setări nu este schimbată.

Considerații speciale atunci când se utilizează protocoale criptate pentru interacțiunea cu servicii externe

Kaspersky Endpoint Security și Kaspersky Security Center utilizează un canal de comunicație criptat cu TLS (Transport Layer Security) pentru a funcționa împreună cu serviciile externe ale Kaspersky. Kaspersky Endpoint Security utilizează servicii externe pentru următoarele funcții:

- actualizarea bazelor de date și modulelor software ale aplicației;
- activarea aplicației cu un cod de activare (activare 2.0);
- utilizarea Kaspersky Security Network.

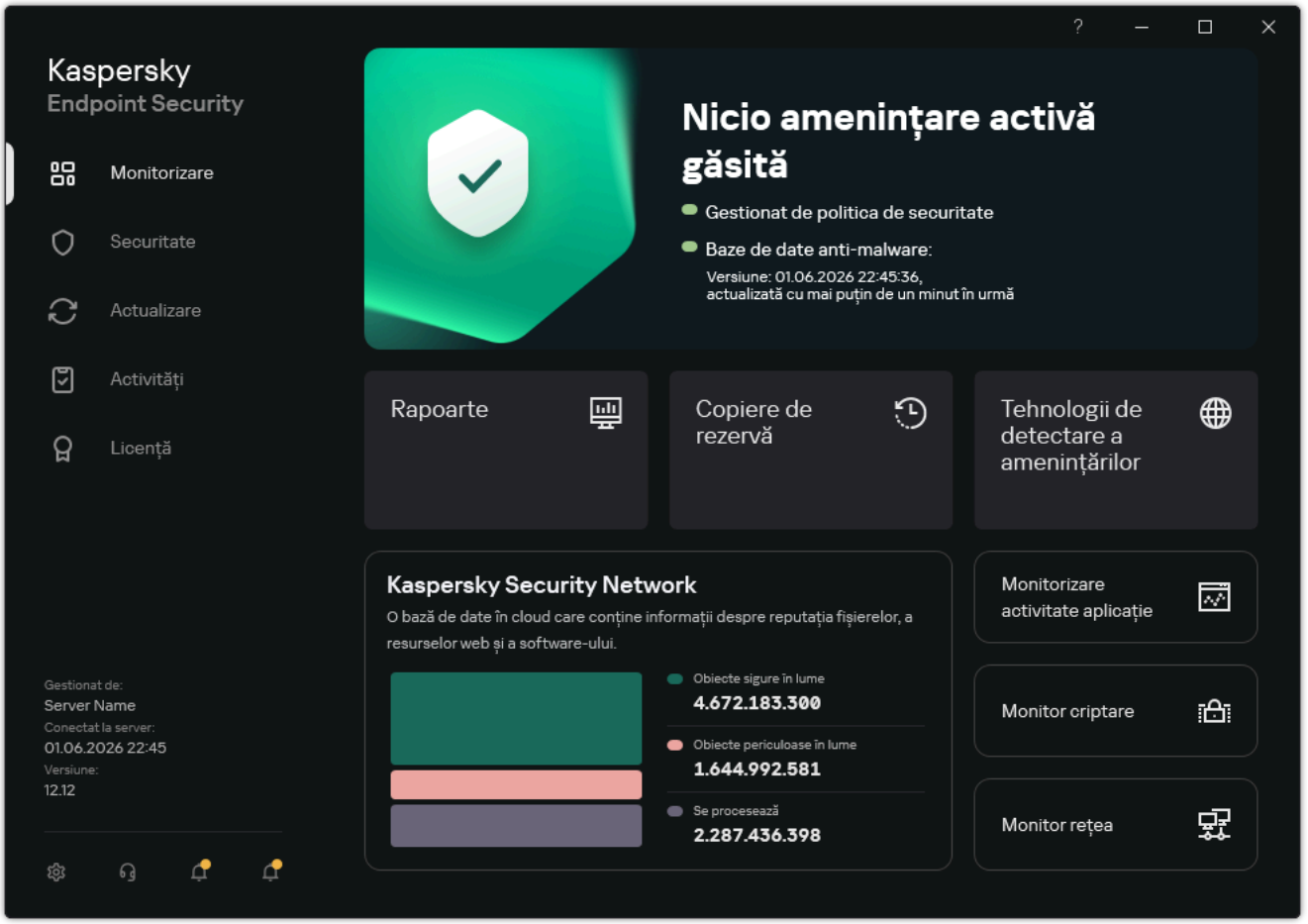
Utilizarea TLS securizează aplicația oferind următoarele caracteristici:

- Criptare. Conținutul mesajelor este confidențial și nu este divulgat utilizatorilor terți.
- Integritate. Destinatarul mesajului este sigur că conținutul mesajului nu a fost modificat de când mesajul a fost redirecționat de către expeditor.
- Autentificare. Destinatarul este sigur că comunicarea este stabilită numai cu un server Kaspersky de încredere.

Kaspersky Endpoint Security utilizează certificate cu cheie publică pentru autentificarea serverului. Este necesară o Public Key Infrastructure (PKI) pentru lucrul cu certificate. O autoritate de certificare face parte dintr-un PKI. Kaspersky folosește propria autoritate de certificare, deoarece serviciile Kaspersky sunt extrem de tehnice și nu sunt publice. În acest caz, atunci când certificatele rădăcină ale Thawte, VeriSign, GlobalTrust și altele sunt revocate, Kaspersky PKI rămâne operațional fără întreruperi.

Mediile care au MITM (instrumente software și hardware care acceptă analiza protocolului HTTPS) sunt considerate a fi nesigure de Kaspersky Endpoint Security. Pot apărea erori atunci când lucrați cu serviciile Kaspersky. De exemplu, pot apărea erori în ceea ce privește utilizarea Self-Signed Certificate. Aceste erori pot apărea deoarece un instrument de inspecție HTTPS din mediul dvs. nu recunoaște Kaspersky PKI. Pentru a remedia aceste probleme, trebuie să configurați excluderile pentru interacțiunea cu serviciile externe.

Interfața aplicației



Fereastra principală a aplicației

Monitorizare	• **Rapoarte**. Vizualizați evenimentele care au avut loc în timpul funcționării aplicației, componentelor individuale și sarcinilor. • **Copiere de rezervă**. Vizualizați o listă a copiilor salvate ale fișierelor infectate pe care aplicația le-a șters. • **Tehnologii de detectare a amenințărilor**. Vizualizați informații despre tehnologiile de detectare a amenințărilor și numărul de amenințări detectate de aceste tehnologii. • **Kaspersky Security Network**. Starea conexiunii dintre Kaspersky Endpoint Security și Kaspersky Security Network și statisticile globale KSN. *Kaspersky Security Network (KSN)* este o infrastructură de servicii în cloud care oferă acces la Baza de cunoștințe online Kaspersky, care conține informații despre reputația fișierelor, a resurselor Web și a programelor software. Utilizarea datelor de la Kaspersky Security Network asigură răspunsul mai rapid prin Kaspersky Endpoint Security la noile amenințări, îmbunătățește eficiența unor componente ale protecției și reduce posibilitatea alarmelor false. Dacă participați la Kaspersky Security Network, serviciile KSN furnizează componentei Kaspersky Endpoint Security informații despre reputația adreselor web scanate, precum și informații despre categoria și reputația fișierelor scanate. • **Monitorizare activitate aplicație**. Vizualizați informații despre funcționarea aplicațiilor instalate. Monitorizare activitate aplicație ține evidența fișierelor, registry-ului și a evenimentelor sistemului de operare asociate cu o aplicație. • **Monitor rețea**. Vizualizați informații despre activitatea de rețea a computerului în timp real. • **Monitor criptare**. Monitorizează procesele de criptare sau de decriptare a discului în timp real. Componenta Monitor criptare este disponibilă atunci când componenta Kaspersky Disk Encryption sau componenta BitLocker Drive Encryption este instalată.
Securitate	Starea de funcționare a componentelor instalate. De asemenea, puteți trece la configurarea componentelor sau vizualizarea rapoartelor.
Actualizare	Gestionați sarcinile de actualizare Kaspersky Endpoint Security. Puteți actualiza bazele de date și modulele de aplicații antivirus și puteți anula ultima actualizare. Un administrator poate ascunde secțiunea de utilizator sau restricționa gestionarea activității.
Activități	Gestionați activitățile de scanare Kaspersky Endpoint Security. Puteți executa o scanare malware și o verificare a integrității aplicației. Un administrator poate ascunde sarcinile unui utilizator sau poate restricționa gestionarea sarcinilor.
Licență	Licențierea aplicației. Puteți cumpăra o licență, activa aplicația sau reînnoi un abonament. De asemenea, puteți vizualiza informații despre licența curentă.
⚙	Configurare setări aplicație. Un administrator poate interzice modificările setărilor din Kaspersky Security Center.

	Informații despre aplicație: versiunea actuală a Kaspersky Endpoint Security, data lansării bazei de date, cheia și alte informații. De asemenea, puteți accesa resursele de informații Kaspersky care oferă informații utile, recomandări și răspunsuri la întrebările frecvente despre cum să cumpărați, să instalați și să utilizați aplicația.
	Mesaje care conțin informații despre actualizări disponibile și solicitări de acces la fișiere și dispozitive criptate.

Pictograma aplicației din zona de notificare a barei de activități

Imediat după instalarea produsului Kaspersky Endpoint Security, pictograma aplicației apare în zona de notificare a barei de activități Microsoft Windows.

Dacă pictograma aplicației din zona de notificare din bara de activități este ascunsă, administratorul a dezactivat afișarea interfeței aplicației în politică.

Pictograma are următoarele funcții:

- Indică activitatea aplicației.
- Acționează ca o comandă rapidă la meniul contextual și la fereastra principală ale aplicației.

Următoarele stări ale pictogramei aplicației sunt furnizate pentru afișarea informațiilor de funcționare a aplicației:

- Pictograma semnifică faptul că componentele de protecție importante ale aplicației sunt activate. Kaspersky Endpoint Security va afișa un avertisment dacă utilizatorul trebuie să efectueze o acțiune, de exemplu, să repornească computerul după actualizarea aplicației.
- Pictograma semnifică faptul că componentele de protecție importante ale aplicației sunt dezactivate sau au funcționat defectuos. Componentele de protecție pot funcționa defectuos, de exemplu, dacă licența a expirat sau ca urmare a unei erori a aplicației. Kaspersky Endpoint Security va afișa un avertisment cu o descriere a problemei în protecția computerului.

Meniul contextual al pictogramei aplicației conține următoarele elemente:

- **Kaspersky Endpoint Security for Windows**. Deschide fereastra principală a aplicației. În această fereastră poți regla funcționarea componentelor și activităților aplicației și poți vizualiza statisticile privind fișierele procesate și amenințările detectate.
- **Pauză protecție** / **Reactivează protecția**. Întrerupeți funcționarea tuturor componentelor de protecție și control care nu sunt marcate cu un lacăt () în politică. Înainte de a efectua această operație, se recomandă dezactivarea politicii Kaspersky Security Center.

  Înainte de a întrerupe funcționarea componentelor de protecție și control, aplicația solicită parola pentru accesarea Kaspersky Endpoint Security (parola contului sau parola temporară). Puteți selecta apoi perioada de pauză: pentru o anumită perioadă de timp, până la o repornire sau la solicitarea utilizatorului.

  Acest element de meniu contextual este disponibil dacă funcția Protecție prin parolă este activată. Pentru a relua funcționarea componentelor de protecție și control, faceți clic pe **Reactivează protecția** în meniul contextual al aplicației.

  Punerea în pauză a funcționării componentelor de protecție și control nu afectează îndeplinirea activităților de actualizare și scanare. Aplicația continuă, de asemenea, să folosească Kaspersky Security Network.

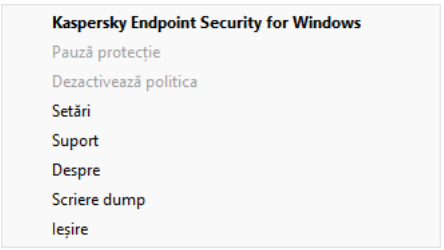
- **Dezactivează politica** / **Activează politică**. Dezactivarea politicii Kaspersky Security Center pe computer. Toate setările Kaspersky Endpoint Security sunt disponibile pentru configurare, inclusiv setările care au lacăt închis în politică (). Dcaă aplicația este dezactivată, aplicația solicită parola pentru accesarea Kaspersky Endpoint Security (parola de cont sau parola temporară). Acest element de meniu contextual este disponibil dacă funcția Protecție prin parolă este activată. Pentru a activa politica, selectați **Activează politică** în meniul contextual al aplicației.

- **Setări**. Deschide fereastra cu setările aplicației.

- **Suport**. Se deschide fereastra care conține informațiile necesare pentru a contacta Suportul tehnic Kaspersky.

- **Despre**. Acest element deschide o fereastră informativă cu detaliile aplicației.

- **Ieșire**. Acest element determină închiderea aplicației Kaspersky Endpoint Security. Dacă faci clic pe acest element al meniului contextual, aplicația este descărcată din memoria RAM a computerului.



Meniul contextual al pictogramei aplicației

Interfață aplicație simplificată

Dacă o politică Kaspersky Security Center configurată să afișeze interfața simplificată a aplicație este aplicată pe un computer client pe care este instalată aplicația Kaspersky Endpoint Security, fereastra principală a aplicației nu va fi disponibilă pe acest computer client. Faceți clic dreapta pentru a deschide meniul contextual al pictogramei Kaspersky Endpoint Security (vezi figura de mai jos), care conține următoarele elemente:

- **Dezactivează politica** / **Activează politică**. Dezactivarea politicii Kaspersky Security Center pe computer. Toate setările Kaspersky Endpoint Security sunt disponibile pentru configurare, inclusiv setările care au lacăt închis în politică (). Dcaă aplicația este dezactivată, aplicația solicită parola pentru accesarea Kaspersky Endpoint Security (parola de cont sau parola temporară). Acest element de meniu contextual este disponibil dacă funcția Protecție prin parolă este activată. Pentru a activa politica, selectați **Activează politică** în meniul contextual al aplicației.

- **Activități**. Listă verticală care conține următoarele elemente:

  - **Verificare integritate aplicație**.

  - **Derularea înapoi a bazelor de date la versiunea anterioară**.

  - **Scanare completă**.

  - **Scanare personalizată**.

  - **Scanare zone critice**.

  - **Actualizare**.

- **Suport**. Se deschide fereastra care conține informațiile necesare pentru a contacta Suportul tehnic Kaspersky.

- **Ieșire**. Acest element determină închiderea aplicației Kaspersky Endpoint Security. Dacă faci clic pe acest element al meniului contextual, aplicația este descărcată din memoria RAM a computerului.



Meniu contextual pentru pictograma aplicației atunci când este afișată interfața simplificată

Configurarea afișării interfeței aplicației

Puteți configura modul de afișare a interfeței aplicației pentru un utilizator. Utilizatorul poate interacționa cu aplicația în următoarele moduri:

- **Afișare interfață simplificată**. Pe un computer client, fereastra principală a aplicației este inaccesibilă și numai pictograma din zona de notificare Windows este disponibilă. În meniul contextual al pictogramei, utilizatorul poate efectua un număr limitat de operații cu Kaspersky Endpoint Security. Kaspersky Endpoint Security afișează, de asemenea, doar notificările care necesită acțiunea utilizatorului deasupra pictogramei aplicației.

- **Afișare interfață utilizator**. Pe un computer client, fereastra principală a Kaspersky Endpoint Security și pictograma din zona de notificare Windows sunt disponibile. În meniul contextual al pictogramei, utilizatorul poate efectua operații cu Kaspersky Endpoint Security. Kaspersky Endpoint Security afișează, de asemenea, notificări deasupra pictogramei aplicației.

- **Nu afișați interfața cu utilizatorul**. Pe un computer client, nu sunt afișate semne de funcționare a Kaspersky Endpoint Security. Pictograma din zona de notificare Windows și notificările sunt disponibile.

Cum se configurează modul de afișare a interfeței aplicației în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.

2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

3. În fereastra politicii, selectați **Setări generale** → **Interfață**.

4. În blocul **Interacțiune cu utilizatorul**, configurați modul în care va fi afișată interfața aplicației:

   - **Afișare interfață utilizator**. Pe un computer client, fereastra principală a Kaspersky Endpoint Security și pictograma din zona de notificare Windows sunt disponibile. În meniul contextual al pictogramei, utilizatorul poate efectua operații cu Kaspersky Endpoint Security. Kaspersky Endpoint Security afișează, de asemenea, notificări deasupra pictogramei aplicației. Dacă este necesar, poți activa funcționalitatea **Ascundeți secțiunea Monitorizare activitate aplicație** pentru a ascunde datele despre activitatea aplicațiilor de pe computer, restricționând astfel accesul utilizatorilor la instrumentul Monitorizare activitate aplicații.

   - **Afișare interfață simplificată**. Pe un computer client, fereastra principală a aplicației este inaccesibilă și numai pictograma din zona de notificare Windows este disponibilă. În meniul contextual al pictogramei, utilizatorul poate efectua un număr limitat de operații cu Kaspersky Endpoint Security. Kaspersky Endpoint Security afișează, de asemenea, doar notificările care necesită acțiunea utilizatorului deasupra pictogramei aplicației.

   - **Nu afișați interfața cu utilizatorul**. Pe un computer client, nu sunt afișate semne de funcționare a Kaspersky Endpoint Security. Pictograma din zona de notificare Windows și notificările sunt disponibile.

5. Salvați-vă modificările.

Cum se configurează modul de afișare a interfeței aplicației în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **General Settings** → **User Interaction**.
5. În blocul **Visibility for users**, configurați modul în care va fi afișată interfața aplicației:

   - **Display user interface**. Dacă această funcționalitate este dezactivată, pe computerul client nu se afișează nicio indicație privind funcționarea Kaspersky Endpoint Security . Pictograma din zona de notificare Windows și notificările sunt disponibile.
   - **Simplified**. Pe un computer client, fereastra principală a aplicației este inaccesibilă și numai pictograma din zona de notificare Windows este disponibilă. În meniul contextual al pictogramei, utilizatorul poate efectua un număr limitat de operații cu Kaspersky Endpoint Security. Kaspersky Endpoint Security afișează, de asemenea, doar notificările care necesită acțiunea utilizatorului deasupra pictogramei aplicației.
   - **Full**. Pe un computer client, fereastra principală a Kaspersky Endpoint Security și pictograma din zona de notificare Windows sunt disponibile. În meniul contextual al pictogramei, utilizatorul poate efectua operații cu Kaspersky Endpoint Security. Kaspersky Endpoint Security afișează, de asemenea, notificări deasupra pictogramei aplicației.
   - **Hide Application Activity Monitor section**. Dacă dorești să ascunzi informațiile despre activitatea aplicației pe computerul unui utilizator, poți restricționa accesul utilizatorului la instrumentul Monitorizare activitate aplicație.
6. Salvați-vă modificările.

Pregătirea aplicației pentru utilizare

După implementarea aplicației pe computere client, pentru a lucra cu aplicația Kaspersky Endpoint Security din Kaspersky Security Center Web Console, trebuie să efectuați următoarele acțiuni:

- Creează și configurați o politică.

  Poți folosi politici pentru a aplica setări identice ale Kaspersky Endpoint Security pentru toate computerele client dintr-un grup de administrare. Quick Start Wizard al Kaspersky Security Center creează automat o politică pentru aplicația Kaspersky Endpoint Security.
- Creați activitățile *Actualizarea modulelor bazelor de date și ale aplicațiilor* și *Scanare malware*.

  Activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* este necesară pentru menținerea actualizată a securității computerului. La efectuarea aceste activități, Kaspersky Endpoint Security actualizează bazele de date antivirus și modulele aplicației. Activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* este creată automat de Expertul de pornire rapidă a Serverului de administrare. Pentru a crea activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor*, instalați plug-inul Kaspersky Endpoint Security for Windows Management în timp ce executați Expertul.

  Activitatea *Scanare malware* este necesară pentru detectarea în timp util a virușilor și a altor programe malware. Trebuie să creați manual activitatea *Scanare malware*.

Cum se creează o activitate Scanare malware în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **New task**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Selectarea tipului activității

Selectați **Kaspersky Endpoint Security for Windows (14.1)** → **Scanare malware**.

Pasul 2. Domeniu de scanare

Creați lista cu obiectele pe care le va scana aplicația Kaspersky Endpoint Security atunci când efectuează o activitate de scanare.

Pasul 3. Acțiune Kaspersky Endpoint Security

Alegeți acțiunea la detectarea amenințărilor:

- **Dezinfectează; șterge dacă dezinfectarea nu reușește**. Dacă selectezi această opțiune, aplicația încearcă automat să dezinfecteze fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, aplicația șterge fișierul.
- **Dezinfectează; informează dacă dezinfectarea nu reușește**. Dacă selectați această opțiune, Kaspersky Endpoint Security încearcă automat să dezinfecteze toate fișierele infectate care sunt detectate. Dacă dezinfectarea eșuează, Kaspersky Endpoint Security adaugă informațiile despre fișierele infectate detectate în lista de amenințări active.
- **Informează**. Dacă este selectată această opțiune, Kaspersky Endpoint Security adaugă informațiile despre fișierele infectate în lista de amenințări active la detectarea acestor fișiere.

- **Execută Dezinfectare avansată imediat**. În cazul în care caseta de selectare este bifată, Kaspersky Endpoint Security folosește tehnologia Dezinfectare avansată pentru a trata amenințările active în timpul scanării.

  Advanced disinfection technology are rolul de a curăța sistemul de operare de aplicații rău intenționate care și-au început deja procesele în memoria RAM și care împiedică eliminarea lor de către Kaspersky Endpoint Security prin alte metode. Prin urmare, amenințarea este neutralizată. În timp ce dezinfectarea avansată este în curs, ți se recomandă să nu pornești procese noi și să nu editezi registrul sistemului de operare. Tehnologia de dezinfectare avansată folosește resurse ale sistemului de operare considerabile, care pot încetini alte aplicații. După finalizarea dezinfectării avansate, Kaspersky Endpoint Security va reporni computerul fără a solicita confirmarea utilizatorului.

- **Run only when the computer is idle**. Amânarea începerii activității atunci când resursele computerului sunt ocupate. Kaspersky Endpoint Security pornește activitatea de scanare dacă computerul este blocat sau dacă economizorul de ecran este pornit. Dacă ați întrerupt executarea activității, de exemplu prin deblocarea computerului, Kaspersky Endpoint Security execută automat activitatea, continuând din punctul în care a fost întreruptă. Această opțiune de planificare vă permite să conservați resursele computerului atunci când acesta este utilizat.

Pasul 4. Selectarea dispozitivelor cărora le va fi atribuită activitatea

Selectați computerele pe care se va efectua activitatea. Sunt disponibile următoarele opțiuni:

- Atribuirea activității unui grup de administrare. În acest caz, activitatea este atribuită computerelor incluse într-un grup de administrare creat anterior.

- Selectare computere detectate în rețea de Serverul de administrare: *dispozitive neatribuite*. Dispozitivele specifice pot include dispozitive din grupuri de administrare, precum și dispozitive neatribuite.

- Specificarea manuală a adreselor computerelor sau importarea adreselor dintr-o listă. Poți specifica nume NetBIOS, adrese IP și subrețele IP ale dispozitivelor cărora dorești să le atribui activitatea.

Pasul 5. Selectarea contului pentru executarea activității

Selectați un cont pentru a executa activitatea *Scanare malware*. În mod implicit, Kaspersky Endpoint Security începe activitatea cu drepturile unui cont de utilizator local. Dacă domeniul de scanare include unități de rețea sau alte obiecte cu acces restricționat, selectați un cont de utilizator cu drepturile de acces suficiente.

Pasul 6. Configurarea unei planificări de pornire a activității

Configurați o planificare pentru începerea unei activități, de exemplu, manual sau după ce bazele de date antivirus sunt descărcate în depozit.

Pasul 7. Definirea numelui activității

Introduceți un nume pentru activitate, de exemplu, *Scanare completă zilnică*.

Pasul 8. Finalizarea creării activității

Ieșiți din Expert. Dacă este necesar, bifați caseta de selectare **Run the task after the wizard finishes**. Puteți monitoriza progresul activității în proprietățile activității. Ca rezultat, activitatea Scanare malware va fi executată pe computerele utilizatorilor în conformitate cu planificarea specificată.

Cum se creează o activitate Scanare malware în Web Console

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **Add**.

   Expertul de activitate pornește.

3. Configurați setările pentru activitate:

   a. În lista verticală **Application**, selectează **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. În lista verticală **Task type**, selectează **Malware Scan**.

   c. În câmpul **Task name**, introdu o descriere succintă, de exemplu *Scanare săptămânală*.

   d. În blocul **Devices to which the task will be assigned**, selectați domeniul activității.

4. Selectați dispozitive în funcție de opțiunea selectată pentru domeniul activității. Mergeți la pasul următor.

5. Selectează un cont pentru a executa activitatea. În mod implicit, Kaspersky Endpoint Security începe activitatea cu drepturile unui cont de utilizator local.

6. Ieșiți din Expert.

   Se va afișa o activitate nouă în lista de activități.

7. Pentru a configura planificarea activității, accesează proprietățile activității.

   Se recomandă să planificați executarea activității cel puțin o dată pe săptămână.

8. Bifați caseta de selectare de lângă activitate.

9. Fă clic pe **Start**.

   Poți monitoriza starea activității și numărul de dispozitive pe care activitatea a fost finalizată cu succes sau finalizată cu o eroare.

Ca rezultat, activitatea Scanare malware va fi executată pe computerele utilizatorilor în conformitate cu planificarea specificată.

- Optimizați performanța Kaspersky Endpoint Security.

Gestionarea politicilor

O *politică* este o colecție de setări pentru o aplicație care sunt definite pentru un grup de administrare. Puteți configura mai multe politici cu valori diferite pentru o singură aplicație. O aplicație se poate executa cu diferite setări pentru diferite grupuri de administrare. Fiecare grup de administrare poate avea propria sa politică pentru o aplicație.

Fiecare setare a politicii are atributul („lacăt"). Starea acestui atribut determină dacă setarea va fi transmisă dispozitivelor gestionate din grupul de administrare:

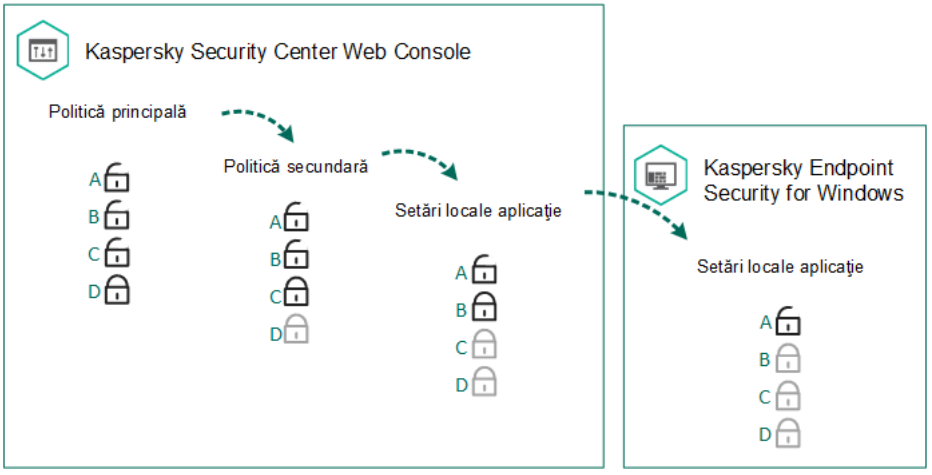
- Dacă „lacătul" este deschis ( ), valoarea acestei setări nu va fi transmisă dispozitivelor gestionate. Setarea va putea fi modificată în interfața locală a aplicației. Astfel de setări sunt considerate *deblocate*.
- Dacă „lacătul" este închis ( ), valoarea acestei setări va fi transmisă și aplicată dispozitivelor gestionate. Astfel de setări sunt considerate *blocate*. Setările blocate nu pot fi modificate în interfața locală a aplicației.

Setările pentru politică se trimit computerelor client de către Agentul de rețea în timpul *sincronizării*. În mod implicit, Serverul de administrare efectuează sincronizarea imediat după modificarea setărilor pentru politică. Pentru sincronizare se folosește portul UDP 15000 de pe computerul client. Serverul de administrare efectuează implicit sincronizarea la fiecare 15 minute. Dacă sincronizarea nu reușește după modificarea setărilor pentru politică, următoarea încercare de sincronizare se va efectua în funcție de planificarea configurată.

Moștenire setări

Politicile, cum ar fi grupurile de administrare, sunt aranjate într-o ierarhie. *Politica subordonată* este o politică pentru niveluri ierarhice imbricate, adică o politică pentru grupuri de administrare imbricate și Servere de administrare secundare.

În mod implicit, o politică secundară moștenește setările din politica principală. Dacă setarea din politica principală are atributul („lacăt" închis), atunci, în politicile secundare și în setările aplicației locale valoarea acelei setări va fi suprascrisă în conformitate cu politica principală, iar setarea va fi blocată. Dacă este necesar, poți dezactiva moștenirea setărilor din politica principală. Politicile Absent de la birou nu afectează alte politici prin intermediul ierarhiei de grupuri de administrare.



Moștenire setări

Drepturile de accesare a setărilor politicii (citire, scriere, executare) sunt specificate pentru fiecare utilizator care are acces la serverul de administrare Kaspersky Security Center și separat pentru fiecare domeniu operațional al Kaspersky Endpoint Security. Pentru a configura drepturile de acces la setările politicii, accesează secțiunea **Security** din fereastra de proprietăți a Serverului de administrare Kaspersky Security Center (în mod implicit, această secțiune este ascunsă în interfața consolei).

Revizuiri ale politicilor

Kaspersky Security Center monitorizează modificarea politicilor și creează revizuiri. O *revizuire* este un set de parametri modificați, salvați de utilizator. Revizuirile vă permit să comparați și să anulați modificările aduse parametrilor politicii. Pe lângă setul de parametri modificați, revizuirea include informații despre utilizatorul care a efectuat modificările, precum și ora, adresa IP, comentariul utilizatorului și alte date relevante.

Pentru a vizualiza jurnalul de revizuiri, deschideți proprietățile politicii și accesați secțiunea **Revision history**. Pentru mai multe detalii despre lucrul cu revizuirile, consultați Ajutor pentru Kaspersky Security Center.

Crearea unei politici

La crearea unei politici, expertul sugerează setări care sunt relevante pentru modul selectat. De exemplu, pentru modul Light Agent, trebuie să adaugi un Server de protecție (SVM). Când utilizezi aplicația pentru a proteja un server SQL, trebuie să adaugi excluderi de la scanare predefinite pentru a te asigura că funcționarea serverului nu este afectată. Expertul sugerează setări relevante ale politicii după selectarea unui mod. Poți edita apoi aceste setări în proprietățile politicii.

Cum se creează o politică în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Managed devices** al arborelui consolei de administrare, selectați directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectează fila **Policies**.
4. Fă clic pe **New policy**.

   Expertul de politică pornește.
5. Urmează instrucțiunile din Expertul de politică.

Pasul 1. Selectarea aplicației pentru crearea politicii de grup

Selectează aplicația **Kaspersky Endpoint Security for Windows (14.1)**.

Pasul 2. Denumirea politicii de grup

Introdu un nume pentru politica de grup, de exemplu, *Politica pentru birou*.

De asemenea, poți crea politici noi pe baza politicilor existente utilizând Expertul pentru politici. Pentru aceasta, atunci când specifici numele politicii de grup, bifează caseta de selectare **Use policy settings for an earlier version of the application**. Expertul permite, de asemenea, crearea unei politici Kaspersky Endpoint Security (KES) bazată pe o politică a unei soluții diferite, de exemplu, Kaspersky Security for Windows Server (KSWS) sau Kaspersky Security for Virtualization Light Agent for Windows

Pasul 3. Participarea la Kaspersky Security Network

Citește și acceptă condițiile din Declarația de Securitate a Rețelei Kaspersky (KSN).

Pasul 4. Selectarea modului de utilizare a aplicației pe computere

În funcție de scopul pentru care se utilizează Kaspersky Endpoint Security, puteți configura o politică pentru următoarele moduri de funcționare:

- Modul standard pentru a proteja gazdelor

  În acest mod, puteți alege modul în care doriți să configurați politica:

  - **Creează politică cu setări implicite**. Setările implicite sunt considerate optime. Aceste setări sunt recomandate de experții Kaspersky. Setările implicite oferă nivelul de protecție recomandat și utilizarea optimă a resurselor.

  - **Modifică setările politicii în Expert**. Această metodă permite gestionarea setărilor politicii pas cu pas, cu ajutorul unui asistent. De asemenea, puteți gestiona setările politicii folosind un fișier de configurare al aplicației (consultați pasul următor).

- Endpoint Detection and Response Agent pentru protecție împotriva amenințărilor avansate și a atacurilor țintite.

  Endpoint Detection and Response Agent este o aplicație care este instalată pe stațiile de lucru și pe serverele individuale din infrastructura IT a organizației pentru a susține soluții Detection and Response de la Kaspersky: La pasul următor, trebuie să alegeți o soluție pentru integrarea cu EDR Agent.

- Light Agent pentru protejarea mediilor virtuale.

  Pentru a utiliza aplicația în modul Light Agent, trebuie să configurați o conexiune cu o mașină virtuală SVM. Aceste setări sunt necesare pentru ca aplicația să funcționeze în modul Light Agent.

Kaspersky Endpoint Security oferă o politică comună pentru toate modurile aplicației și toate tipurile de sisteme de operare. Aceasta înseamnă că politica acoperă întregul set de setări. Cu toate acestea, aplicația poate ignora unele dintre setările politicii, deoarece Kaspersky Endpoint Security este implementat într-un mod în care unele funcționalități nu sunt disponibile. De exemplu, când utilizezi aplicația în modul Endpoint Detection and Response Agent, sunt disponibile numai setările care sunt relevante pentru integrarea cu soluțiile Kaspersky Detection and Response și pentru integrarea cu soluția KUMA.

Îți recomandăm să utilizezi politici diferite pentru diferite moduri și tipuri de sisteme de operare.

Pasul 5. Importarea setărilor

Acest pas este disponibil dacă selectați configurarea manuală a politicii la pasul 4.

Puteți crea o politică pe baza setărilor Kaspersky Endpoint Security dintr-un fișier de configurare CFG. Atunci când se importă un fișier de configurare a aplicației, nu toate setările politicii sunt disponibile pentru expert. De exemplu, profilurile politicii lipsesc din setările aplicației. Dacă doriți să transferați toate setările și profilurile în politică, puteți importa o altă politică dintr-un fișier KLP.

La importarea unui fișier de configurare, Kaspersky Endpoint Security nu transferă parolele pentru containerele crypto. Dacă utilizați autentificarea mutuală atunci când vă conectați la servere, trebuie să specificați de la zero parolele pentru containerele crypto.

Pasul 6 - 10. Configurarea setărilor politicii

Acest pas este disponibil dacă selectați configurarea manuală a politicii la pasul 4.

Urmați pașii pentru a gestiona setările politicii.

Pasul 11. Configurarea zonei de încredere

Configurează zona de încredere. Poți adăuga excluderi de la scanare predefinite și aplicații de încredere. Excluderile de la scanare și aplicațiile de încredere predefinite ajută la configurarea rapidă a Kaspersky Endpoint Security pe serverele SQL, serverele Microsoft Exchange și System Center Configuration Manager. Aceasta înseamnă că nu trebuie să configurați manual o zonă de încredere pentru aplicație pe servere. Excluderile de la scanare predefinite și aplicațiile de încredere te pot ajuta, de asemenea, să configurezi rapid Kaspersky Endpoint Security în modul Light Agent în mediile virtuale Citrix și VMware.

Pasul 12. Selectarea stării politicii

- **Active**. După următoarea sincronizare, politica va fi folosită drept politica activă pe computer.

  Setările unei politici active se salvează pe computerele client în timpul sincronizării. Nu poți aplica simultan mai multe politici pe un singur computer; prin urmare, poate fi activă numai o singură politică în fiecare grup.

- **Inactive**. Faceți o copie de rezervă a politicii. Dacă este necesar, o politică inactivă poate fi comutată la starea Activă.

  Poți crea un număr nelimitat de politici inactive. O politică inactivă nu afectează setările aplicației pe computerele din rețea. Politicile inactive sunt concepute ca pregătiri pentru situații de urgență, cum ar fi un atac de virus. Dacă există un atac prin intermediul unităților flash, poți activa o politică care blochează accesul la unitățile flash. În acest caz, politica activă devine automat inactivă.

- **Out-of-office**. Politica este activată atunci când un computer părăsește perimetrul rețelei organizației.

Finalizați expertul.

Cum se creează o politică în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Fă clic pe **Add**.

   Expertul de politică pornește.
3. Selectați Kaspersky Endpoint Security și faceți clic pe **Next**.
4. Citește și acceptă condițiile din Declarația de Securitate a Rețelei Kaspersky (KSN) și faceți clic pe **Next**.
5. Selectează modul aplicației:

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

     Dacă selectezi acest mod, poți crea o politică pentru a integra computerul cu soluțiile Kaspersky Detection and Response. Expertul îți solicită să configurezi integrarea pentru Kaspersky Managed Detection and Response și apoi Kaspersky Anti Targeted Attack Platform (EDR).
   - Light Agent to protect virtual environments.

     Dacă selectezi acest mod, la pasul următor trebuie să configurezi conexiunea la Serverul de protecție (SVM). Aceste setări sunt necesare pentru ca aplicația să funcționeze în modul Light Agent.

   Kaspersky Endpoint Security oferă o politică comună pentru toate modurile aplicației și toate tipurile de sisteme de operare. Aceasta înseamnă că politica acoperă întregul set de setări. Cu toate acestea, aplicația poate ignora unele dintre setările politicii, deoarece Kaspersky Endpoint Security este implementat într-un mod în care unele funcționalități nu sunt disponibile. De exemplu, când utilizezi aplicația în modul Endpoint Detection and Response Agent, sunt disponibile numai setările care sunt relevante pentru integrarea cu soluțiile Kaspersky Detection and Response și pentru integrarea cu soluția KUMA.

   > Îți recomandăm să utilizezi politici diferite pentru diferite moduri și tipuri de sisteme de operare.

6. Configurează zona de încredere. Poți adăuga excluderi de la scanare predefinite și aplicații de încredere. Excluderile de la scanare și aplicațiile de încredere predefinite ajută la configurarea rapidă a Kaspersky Endpoint Security pe serverele SQL, serverele Microsoft Exchange și System Center Configuration Manager. Aceasta înseamnă că nu trebuie să configurați manual o zonă de încredere pentru aplicație pe servere. Excluderile de la scanare predefinite și aplicațiile de încredere te pot ajuta, de asemenea, să configurezi rapid Kaspersky Endpoint Security în modul Light Agent în mediile virtuale Citrix și VMware.

7. În fila **General** poți efectua următoarele acțiuni:

   - Schimbă numele politicii.
   - Selectați starea politicii:
     - **Active**. După următoarea sincronizare, politica va fi folosită drept politica activă pe computer.

       Setările unei politici active se salvează pe computerele client în timpul sincronizării. Nu poți aplica simultan mai multe politici pe un singur computer; prin urmare, poate fi activă numai o singură politică în fiecare grup.
     - **Inactive**. Faceți o copie de rezervă a politicii. Dacă este necesar, o politică inactivă poate fi comutată la starea Activă.

       Poți crea un număr nelimitat de politici inactive. O politică inactivă nu afectează setările aplicației pe computerele din rețea. Politicile inactive sunt concepute ca pregătiri pentru situații de urgență, cum ar fi un atac de virus. Dacă există un atac prin intermediul unităților flash, poți activa o politică care blochează accesul la unitățile flash. În acest caz, politica activă devine automat inactivă.
     - **Out-of-office**. Politica este activată atunci când un computer părăsește perimetrul rețelei organizației.
   - Configurați moștenirea setărilor:
     - **Inherit settings from parent policy**. Dacă acest buton de comutare este pornit, valorile setărilor pentru politicii se moștenesc de la politica de nivel superior. Setările pentru politici nu pot fi editate dacă este setat pentru politica părinte.
     - **Force inheritance of settings in child policies**. Dacă acest buton de comutare este pornit, valorile setărilor pentru politică se propagă în politicile subordonate. În proprietățile politicii secundare, butonul de comutare **Inherit settings from parent policy** va fi pornit automat și nu poate fi dezactivat. Setările pentru politicile subordonate se vor moșteni de la politica părinte, exceptând setările marcate cu . Setările pentru politicile subordonate nu pot fi editate dacă este setat pentru politica părinte.

8. În fila **Application settings** poți configura setările pentru politici Kaspersky Endpoint Security.

9. Finalizați expertul.

Ca rezultat, setările pentru Kaspersky Endpoint Security vor fi configurate pe computerele client în timpul următoarei sincronizări. Puteți vizualiza informații despre politica care se aplică pe computer în interfața Kaspersky Endpoint Security făcând clic pe butonul de pe ecranul principal (de exemplu, numele politicii). Pentru a face acest lucru, în setările politicii Agent de rețea, trebuie să activați primirea datelor de politică extinsă. Pentru mai multe detalii despre o politică Agent de rețea, consultați Ajutor pentru Kaspersky Security Center.

Exportarea și importarea unei polițe

Kaspersky Endpoint Security permite exportarea unei politici, împreună cu setările și profilurile sale, într-un fișier KLP. Puteți folosi apoi funcționalitatea de exportare/importare a politicilor pentru a crea copii de rezervă ale acestora, pentru a le migra pe un alt server sau, de exemplu, pentru a le migra din Kaspersky Security Center pentru Windows în Kaspersky Security Center pentru Linux. Pentru detalii despre lgestionarea politicilor, consultați secțiunea Ajutor pentru Kaspersky Security Center.

Cum se exportă și se importă o politică în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Managed devices** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectează fila **Policies**.
4. Pentru a exporta o politică:
   a. Faceți clic pe politica pe care doriți să o exportați.
   b. Faceți clic pe linkul **Export policy to file** din partea din dreapta a ferestrei.
   c. În fereastra care se deschide, specificați numele fișierului KLP în care doriți să exportați politica și selectați directorul în care doriți să salvați fișierul.
   d. Salvați fișierul.
5. Pentru a importa o politică:
   a. Fă clic pe **Import policy from file**.
   b. În fereastra care se deschide, selectați fișierul politicii KLP pe care doriți să îl importați.
   c. Deschideți fișierul.

Această acțiune adaugă o nouă politică cu starea *Inactive policy*.

Cum se exportă și se importă o politică în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Pentru a exporta o politică:
   a. Bifați caseta de selectare de lângă politica pe care doriți să o exportați.
   b. Faceți clic pe butonul **Export**.
   c. În fereastra care se deschide, specificați numele fișierului KLP în care doriți să exportați politica și selectați directorul în care doriți să salvați fișierul.
   d. Salvați fișierul.
3. Pentru a importa o politică:
   a. Fă clic pe **Import**.
   b. Selectați fișierul politicii KLP pe care doriți să îl importați.
   c. După ce politica a fost procesată cu succes, selectați grupul de administrare căruia doriți să îi aplicați politica.
   d. Faceți clic pe butonul **Complete** pentru a finaliza importul politicii.

Această acțiune adaugă o nouă politică cu starea *Inactive*.

Indicator nivel de securitate

Indicatorul nivelului de securitate este afișat în partea de sus a ferestrei cu proprietățile politicii: Indicatorul poate avea una dintre valorile următoare:

- **Nivel ridicat de protecție**. Indicatorul prezintă această valoare și culoarea verde dacă sunt activate toate componentele din categoriile următoare:
  - **Critice**. Această categorie include componentele următoare:
    - File Threat Protection.
    - Behavior Detection.
    - Exploit Prevention.
    - Remediation Engine.
    - Protejarea serviciilor aplicației împotriva gestionării externe.
  - **Importante**. Această categorie include componentele următoare:
    - Kaspersky Security Network.
    - Web Threat Protection.
    - Mail Threat Protection.
    - Host Intrusion Prevention.
    - Protecție prin parolă.
- **Nivel mediu de protecție**. Indicatorul prezintă această valoare și culoarea galbenă dacă una dintre componentele importante este dezactivată.
- **Nivel scăzut de protecție**. Indicatorul prezintă această valoare și culoarea roșie în una dintre situațiile următoare:
  - Una sau mai multe componente critice sunt dezactivate.
  - Două sau mai multe componente critice sunt dezactivate.

Dacă indicatorul are valoarea **Nivel mediu de protecție** sau **Nivel scăzut de protecție**, în dreapta indicatorului va apărea linkul **Componente de protecție recomandate**. În această fereastră poți activa pe oricare dintre componentele de protecție recomandate.

După upgradarea aplicației, indicatorul nivelului de protecție poate indica un nivel de protecție mai scăzut decât înainte de upgrade. Acest lucru se întâmplă deoarece versiunea mai nouă a aplicației introduce noi componente sau caracteristici care sunt importante pentru securitatea computerului. După upgradarea aplicației, trebuie să gestionezi noile setări pentru a te asigura că nivelul de protecție rămâne ridicat.



Indicatorul nivelului de securitate al politicii

Gestionare activităților

Poți crea următoarele tipuri de activități pentru a administra Kaspersky Endpoint Security folosind Kaspersky Security Center:

- Activități locale care sunt configurate pentru un computer client individual.
- Activități de grup care sunt configurate pentru computere client din grupuri de administrare.
- Activități pentru o selecție de computere.

Poți crea orice număr de activități de grup, activități pentru o selecție de computere sau activități locale. Pentru mai multe detalii despre lucrul cu grupuri de administrare și selecții de computere, consultați secțiunea Ajutor pentru Kaspersky Security Center.

Kaspersky Endpoint Security acceptă următoarele activități:

- **Scanare malware**. Kaspersky Endpoint Security scanează de viruși și alte amenințări zonele din computer specificate în setările activității. Activitatea *Scanare malware* este necesară pentru funcționarea aplicației Kaspersky Endpoint Security se creează în timpul executării Quick Start Wizard. Se recomandă să planificați executarea activității cel puțin o dată pe săptămână.
- **Adaugă cheie**. Kaspersky Endpoint Security adaugă o cheie pentru activarea aplicației, inclusiv o cheie suplimentară. Înainte de executarea activității, asigură-te că numărul de computere pe care se va executa activitatea nu depășește numărul de computere permis de licență.
- **Modificare componente ale aplicației**. Kaspersky Endpoint Security instalează sau elimină componente pe computere client, în conformitate cu lista de componente din setările activității. Componenta File Threat Protection nu poate fi eliminată. Un set optim de componente ale aplicației Kaspersky Endpoint Security ajută la conservarea resurselor computerului.
- **Inventar**. Kaspersky Endpoint Security primește informații despre toate fișierele executabile ale aplicațiilor care sunt stocate pe computere. Activitatea *Inventar* se efectuează de către componenta Application Control. Dacă nu este instalată componenta Application Control, activitatea se va termina cu o eroare.
- **Actualizarea modulelor bazelor de date și ale aplicațiilor**. Kaspersky Endpoint Security actualizează bazele de date și modulele aplicației. Activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* este necesară pentru funcționarea aplicației Kaspersky Endpoint Security se creează în timpul executării Quick Start Wizard. Este recomandabil să configurezi o planificare care să execute activitatea cel puțin o dată zi.
- **Șterge datele**. Kaspersky Endpoint Security șterge imediat fișierele și directoarele de pe computerele utilizatorilor sau dacă nu există nicio conexiune cu Kaspersky Security Center de mult timp.

- **Derulare înapoi actualizare**. Kaspersky Endpoint Security derulează înapoi ultima actualizare a bazelor de date și a modulelor aplicației. Acest lucru poate fi necesar dacă, de exemplu, noile baze de date conțin date incorecte care pot cauza blocarea unei aplicații sigure de către Kaspersky Endpoint Security.

- **Verificare integritate aplicație**. Kaspersky Endpoint Security analizează fișierele aplicațiilor, verifică dacă fișierele sunt corupte sau modificate și verifică semnăturile digitale ale fișierelor aplicațiilor.

- **Gestionare conturi Agent de Autentificare**. Kaspersky Endpoint Security configurează setările contului Agentului de Autentificare. Un Agent de Autentificare este necesar pentru a lucra cu unități criptate. Înainte de a încărcarea sistemul de operare, utilizatorul trebuie să completeze autentificarea cu Agentul.

Dacă aplicația funcționează ca parte a soluție Endpoint Detection and Response de la Kaspersky, poți executa activități suplimentare ca acțiuni de răspuns la detecție (responses). De exemplu, poți termina de la distanță procesele folosind activitatea *Termină procesul*.

Activitățile se execută pe un computer numai dacă aplicația Kaspersky Endpoint Security se execută.

Crearea unei activități

Cum se creează o activitate în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. Selectați directorul **Tasks** în arborele Consolei de administrare.
3. Fă clic pe **New task**.

   Expertul de activitate pornește.
4. Urmează instrucțiunile din Expertul de activitate.

Cum se creează o activitate în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.
2. Fă clic pe **Add**.

   Expertul de activitate pornește.
3. Configurați setările pentru activitate:
   a. În lista verticală **Application**, selectează **Kaspersky Endpoint Security for Windows 14.1.0**.
   b. În lista verticală **Task type**, selectați activitatea pe care dorești să o execuți pe computere ale utilizatorilor.
   c. În câmpul **Task name**, introduceți o descriere succintă.
   d. În blocul **Devices to which the task will be assigned**, selectați domeniul activității.
4. Selectați dispozitive în funcție de opțiunea selectată pentru domeniul activității. Mergeți la pasul următor.

5. Selectează un cont pentru a executa activitatea. În mod implicit, Kaspersky Endpoint Security începe activitatea cu drepturile unui cont de utilizator local.

6. Finalizați expertul.

Se va afișa o activitate nouă în lista de activități. Activitatea va avea setările implicite. Pentru a configura setările activității, trebuie să accesați proprietățile activității. Pentru a executa o activitate, trebuie să bifați caseta de selectare de lângă activitate și să faceți clic pe butonul **Start**. După ce activitatea a început, o puteți întrerupe și o puteți relua ulterior.

În lista de activități, puteți monitoriza rezultatele activității, care includ starea activității și statisticile pentru performanța activității pe computere. Puteți, de asemenea, să creați o selecție de evenimente pentru monitorizarea finalizării activităților (**Monitoring → Event selections**). Pentru mai multe detalii despre selectarea evenimentelor, consultați Ajutor pentru Kaspersky Security Center. Rezultatele executării activității se salvează tot local, în jurnalul de evenimente Windows și în rapoartele aplicației Kaspersky Endpoint Security.

Gestionarea accesului la activități

Drepturile de accesare a activităților Kaspersky Endpoint Security (citire, scriere, executare) sunt definite pentru fiecare utilizator care are acces la Serverul de administrare Kaspersky Security Center, prin setările de acces la zonele operaționale ale Kaspersky Endpoint Security. Pentru a configura accesul la zonele operaționale ale Kaspersky Endpoint Security, accesează secțiunea **Security** din fereastra de proprietăți a serverului de administrare Kaspersky Security Center. Pentru mai multe detalii despre gestionarea activităților prin intermediul Kaspersky Security Center, consultați Ajutor pentru Kaspersky Security Center.

Poți configura drepturile utilizatorilor pentru a accesa activitățile utilizând o politică (*modul de gestionare a activităților*). De exemplu, puteți ascunde sarcinile de grup în interfața Kaspersky Endpoint Security.

Cum se configurează modul de gestionare a activităților în interfața Kaspersky Endpoint Security prin intermediul Consolei de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.

2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

3. În fereastra politicii, selectați **Activități locale → Gestionare activități**.

4. Configurați modul de gestionare a activităților (consultați tabelul de mai jos).

5. Salvați-vă modificările.

Cum se configurează modul de gestionare a activităților în interfața Kaspersky Endpoint Security prin Web Console

1. În fereastra principală a Web Console, selectați **Asset management → Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **General Settings → User Interaction**.

5. În **Permitted actions**, configurează modul de gestionare a activităților (consultă tabelul de mai jos).

6. Salvați-vă modificările.

Setări pentru Gestionare activități

Parametru	Descriere
Access to local tasks	Dacă această casetă de selectare este bifată, activitățile locale sunt afișate în interfața locală Kaspersky Endpoint Security. Atunci când nu există restricții suplimentare de politică, utilizatorul poate configura și executa activitățile. Cu toate acestea, configurarea planificării executării activității rămâne indisponibilă pentru utilizator. Utilizatorul poate executa manual activitățile. Dacă această casetă de selectare nu este bifată, utilizarea activităților locale este oprită. În acest mod, activitățile locale nu se execută conform planificării. Activitățile nu pot fi pornite sau configurate în interfața locală a Kaspersky Endpoint Security sau atunci când se lucrează în linia de comandă. Un utilizator poate în continuare să pornească o scanare a unui fișier sau director selectând opțiunea **Scanează de viruși** în meniul contextual al fișierului sau directorului respectiv. Activitatea de scanare este pornită cu valorile implicite pentru activitatea de scanare particularizată.
View group tasks	Dacă această casetă de selectare este bifată, activitățile de grup sunt afișate în interfața locală Kaspersky Endpoint Security. Utilizatorul poate vizualiza lista tuturor activităților în interfața aplicației. Dacă această casetă de selectare este debifată, Kaspersky Endpoint Security afișează o listă de activități goală.
Manage group tasks	În cazul în care caseta de selectare este bifată, utilizatorii pot porni și opri activitățile de grup specificate în consola Kaspersky Security Center. Utilizatorii pot începe și opri activitățile în interfața aplicației sau în interfața simplificată a aplicației. În cazul în care caseta de selectare este debifată, Kaspersky Endpoint Security pornește automat activitățile planificate sau administratorul pornește manual activitățile în consola Kaspersky Security Center.

Configurarea setărilor generale ale aplicației

În Kaspersky Security Center puteți configura setările pentru Kaspersky Endpoint Security pe un anumit computer. Acestea sunt *setări locale pentru aplicație*. Unele setări pot fi inaccesibile pentru editare. Aceste setări sunt blocate de atributul din proprietățile politicilor.

Cum se configurează setările locale pentru aplicație în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.

2. În directorul **Managed devices** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.

3. În spațiul de lucru, selectează fila **Devices**.

4. Fă dublu clic pentru a deschide fereastra cu proprietățile computerului.

5. În fereastra cu proprietățile computerului, selectează secțiunea **Applications**.

6. În lista de aplicații Kaspersky instalate pe computer, selectează **Kaspersky Endpoint Security for Windows (14.1)** și fă dublu clic pentru a deschide proprietățile aplicației.

7. În secțiunea **Setări generale**, configurează Kaspersky Endpoint Security, precum și Rapoarte și Spații de stocare.

   Restul secțiunilor din fereastra proprietăților aplicației sunt standard pentru Kaspersky Security Center. O descriere a acestor secțiuni este furnizată în secțiunea de ajutor din Kaspersky Security Center.

Dacă o aplicație este subiectul unei politici care interzice modificările unor setări specifice, nu vei putea să le editezi atunci când configurezi setările aplicației în secțiunea **Setări generale**.

8. Salvați-vă modificările.

Cum se configurează setările locale pentru aplicație în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Assets (Devices)**.
2. Selectează computerul pentru care dorești să configurezi setări locale pentru aplicație.

   Se vor deschide proprietățile computerului.
3. Selectați fila **Applications**.
4. Fă clic pe **Kaspersky Endpoint Security for Windows**.

   Se vor deschide setările locale pentru aplicație.
5. Selectați fila **Application settings**.
6. Configurați setările locale pentru aplicație.
7. Salvați-vă modificările.

Setările locale pentru aplicației sunt identice cu setările pentru politici, exceptând setările pentru criptare.

Pornirea și oprirea Kaspersky Endpoint Security

După instalarea Kaspersky Endpoint Security pe computerul unui utilizator, aplicația este pornită automat. În mod implicit, aplicația Kaspersky Endpoint Security este pornită după pornirea sistemului de operare. Nu este posibil să configurați pornirea automată a aplicației în setările sistemului de operare.

Descărcarea bazelor de date antivirus ale Kaspersky Endpoint Security după pornirea sistemului de operare poate dura până la două minute, în funcție de computer. În acest interval, nivelul de protecție a computerului este redus. Descărcarea bazelor de date antivirus atunci când Kaspersky Endpoint Security este pornit pe un sistem de operare deja pornit nu cauzează o reducere a nivelului de protecție a computerului.

Cum se configurează pornirea Kaspersky Endpoint Security în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Setări generale** → **Setări aplicație**.
4. Folosește caseta de selectare **Pornește aplicația la pornirea computerului (recomandat)** pentru a configura pornirea aplicației.
5. Salvați-vă modificările.

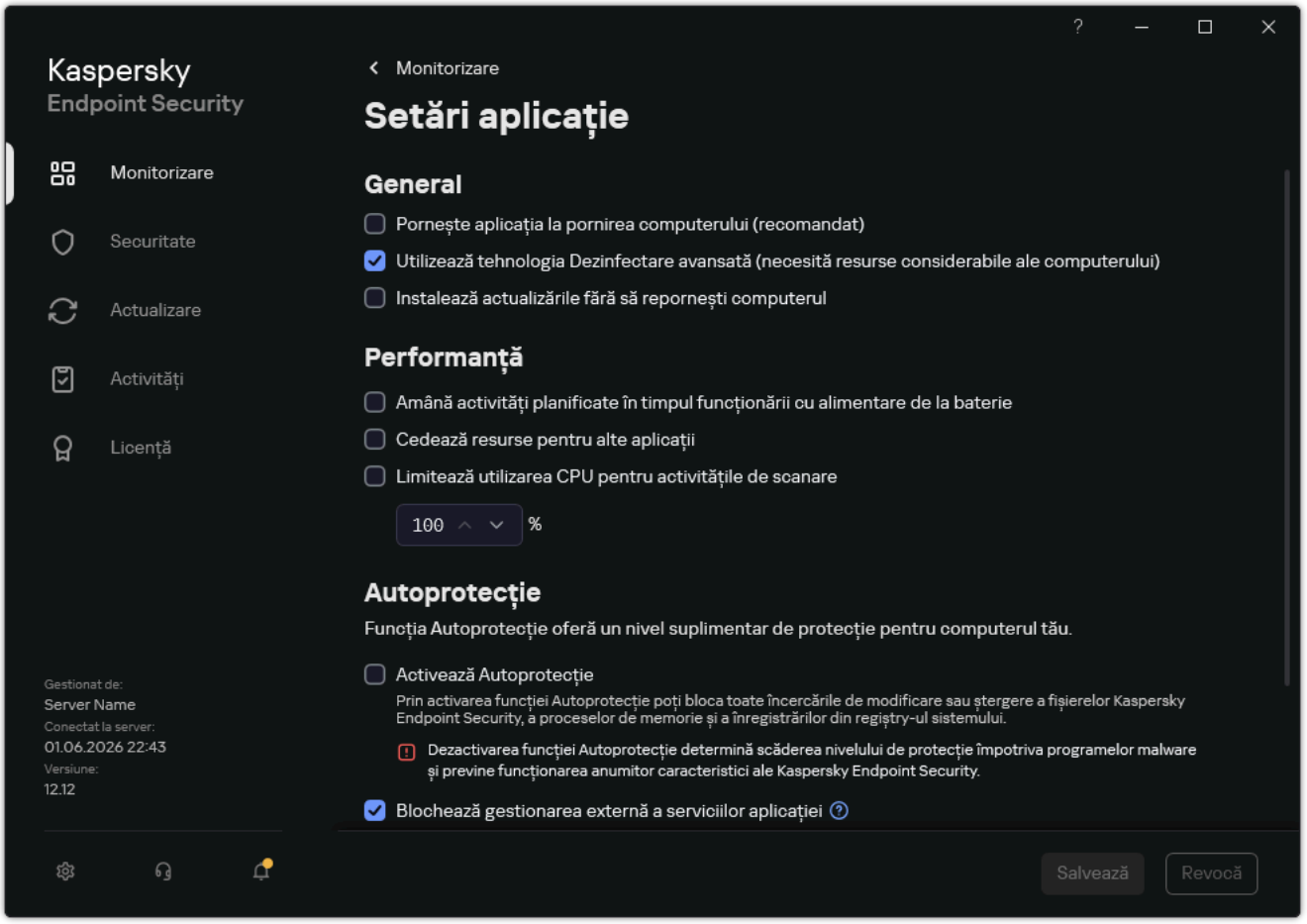
Cum se configurează pornirea Kaspersky Endpoint Security în Web Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **General Settings** → **User Interaction**.
5. Folosește caseta de selectare **Start Kaspersky Endpoint Security on computer startup (recommended)** pentru a configura pornirea aplicației.
6. Salvați-vă modificările.

Cum se configurează pornirea Kaspersky Endpoint Security în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul .
2. În fereastra cu setările aplicației, selectați **Setări generale** → **Setări aplicație**.



Setări Kaspersky Endpoint Security for Windows

3. Folosește caseta de selectare **Pornește aplicația la pornirea computerului (recomandat)** pentru a configura pornirea aplicației.

4. Salvați-vă modificările.

Experții Kaspersky nu recomandă oprirea manuală a aplicației Kaspersky Endpoint Security, deoarece astfel computerul și datele personale sunt expuse la amenințări. Dacă este necesar, poți trece în pauză protecția computerului atât timp cât este necesar, fără a opri aplicația.

Puteți monitoriza starea aplicației utilizând widget-ul **Protection status**.

Cum se pornește sau se oprește Kaspersky Endpoint Security în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.

2. În directorul **Managed devices** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.

3. În spațiul de lucru, selectează fila **Devices**.

4. Fă dublu clic pentru a deschide fereastra cu proprietățile computerului.

5. În fereastra cu proprietățile computerului, selectează secțiunea **Applications**.

6. În lista de aplicații Kaspersky instalate pe computer, selectează **Kaspersky Endpoint Security for Windows (14.1)** și fă dublu clic pentru a deschide proprietățile aplicației.

7. Efectuează una dintre următoarele acțiuni:

   - Pentru a porni aplicația, faceți clic pe butonul  din dreapta listei de aplicații Kaspersky.
   - Pentru a opri aplicația, faceți clic pe butonul  din dreapta listei de aplicații Kaspersky.

Cum se pornește sau se oprește Kaspersky Endpoint Security în Web Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Assets (Devices)**.

2. Faceți clic pe numele computerului pe care dorești să pornești sau să oprești Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți ale computerului.

3. Selectați fila **Applications**.

4. Bifați caseta de selectare din partea opusă a aplicației **Kaspersky Endpoint Security for Windows**.

5. Fă clic pe butonul **Start** sau **Stop**.

Cum se pornește sau se oprește Kaspersky Endpoint Security din linia de comandă

1. Executați interpretorul de linii de comandă (cmd.exe) ca administrator.

2. Deschideți directorul în care se află fișierul executabil klpsm.exe.

3. Pentru a porni aplicația din linia de comandă, introduceți `klpsm.exe start_avp_service`.

4. Pentru a opri aplicația din linia de comandă, introduceți `klpsm.exe stop_avp_service`.

Pentru a opri aplicația din linia de comandă, activați gestionarea externă a serviciilor de sistem.



Pornirea și oprirea aplicației din linia de comandă

Trecerea în pauză și reluarea protecției și controlului computerului

Trecerea în pauză a protecției și controlului computerului înseamnă dezactivarea tuturor componentelor de protecție și control ale aplicației Kaspersky Endpoint Security pentru un timp.

Starea aplicației este afișată folosind pictograma aplicației în zona de notificări din bara de activități.

- Pictograma indică faptul că protecția și controlul computerului au fost trecute în pauză.
- Pictograma indică faptul că protecția și controlul computerului au fost activate.

Trecerea în pauză sau reluarea protecției și controlului computerului nu afectează activitățile de scanare sau de actualizare.

Dacă, atunci când treci în pauză sau reiei protecția și controlul computerului, sunt deja stabilite conexiuni la rețea, se afișează o notificare despre terminarea acestor conexiuni.

Pentru a trece în pauză protecția și controlul computerului:

1. Faceți clic dreapta pe pictograma aplicației din zona de notificare a barei de activități pentru a se afișa meniul contextual.
2. În meniul contextual, selectați **Pauză protecție** (vedeți figura de mai jos).

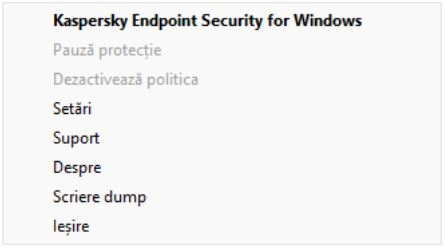
   Acest element de meniu contextual este disponibil dacă funcția Protecție prin parolă este activată.

3. Selectați una dintre următoarele opțiuni:

   - **Pauză timp de <perioada de timp>** – protecția și controlul computerului vor fi reluate după intervalul de timp specificat în lista verticală de mai jos.
   - **Pauză până la repornirea aplicației** – protecția și controlul computerului se vor relua după ce reporniți aplicația sau reporniți sistemul de operare. Pornirea automată a aplicației trebuie să fie activată pentru a folosi această opțiune.
   - **Pauză** – protecția și controlul computerului se vor relua atunci când decideți să le reactivați.

4. Fă clic pe **Pauză protecție**.

   Kaspersky Endpoint Security va întrerupe funcționarea tuturor componentelor de protecție și control care nu sunt marcate cu un lacăt (🔒) în politică. Înainte de a efectua această operație, se recomandă dezactivarea politicii Kaspersky Security Center.



Meniul contextual al pictogramei aplicației

Pentru a relua protecția și controlul computerului:

1. Faceți clic dreapta pe pictograma aplicației din zona de notificare a barei de activități pentru a se afișa meniul contextual.
2. În meniul contextual, selectați **Reactivează protecția**.

Poți relua oricând protecția și controlul computerului, indiferent care este opțiunea de trecere în pauză a protecției și a controlului computerului selectată anterior.

Crearea și folosirea unui fișier de configurare

Un fișier de configurare cu setări Kaspersky Endpoint Security îți permite să realizezi următoarele activități:

- Executarea instalării locale a Kaspersky Endpoint Security din linie de comandă, cu setări predefinite.
- Efectuarea instalării la distanță a Kaspersky Endpoint Security, prin intermediul Kaspersky Security Center, cu setări predefinite.
- Transferul setărilor aplicației într-o politică.
- Migrarea setărilor Kaspersky Endpoint Security de la un computer la altul (consultați instrucțiunile de mai jos).

Exportarea unui fișier de configurare

Pentru a crea un fișier de configurare:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Setări generale** → **Gestionează setările**.
3. Fă clic pe **Exportă**.
4. În fereastra care se deschide, specificați calea către locul în care doriți să salvați fișierul de configurare și introduceți numele acestuia.

   Pentru a folosi fișierul de configurare pentru instalare locală sau la distanță a Kaspersky Endpoint Security, numele trebuie să fie install.cfg.

5. Dacă este necesar, introdu o parolă pentru exportarea configurației aplicației într-un fișier.

   Pentru a salva fișierul de configurare, Protecția prin parolă trebuie activată. Utilizatorul trebuie să aibă permisiunea **Exportă setările**.

6. Salvați fișierul.

Drept urmare, aplicația creează un fișier de configurare. Fișierul de configurare poate conține detalii despre contul de utilizator, prin urmare, Kaspersky Endpoint Security criptează fișierul. Nu poți edita un fișier de configurare. Orice încercare de modificare a unui fișier de configurare îl va altera.

Importarea unui fișier de configurare

Un fișier de configurare poate conține detaliile conturilor de utilizator adăugate în aplicație. Dacă importi fișierul pe același computer pe care a fost creat, Kaspersky Endpoint Security importă parolele conturilor de utilizator. Dacă importi fișierul pe un alt computer, trebuie să introduci parolele manual.

La importarea unui fișier de configurare, Kaspersky Endpoint Security nu transferă parolele pentru containerele crypto. Dacă utilizați autentificarea mutuală atunci când vă conectați la servere, trebuie să specificați de la zero parolele pentru containerele crypto.

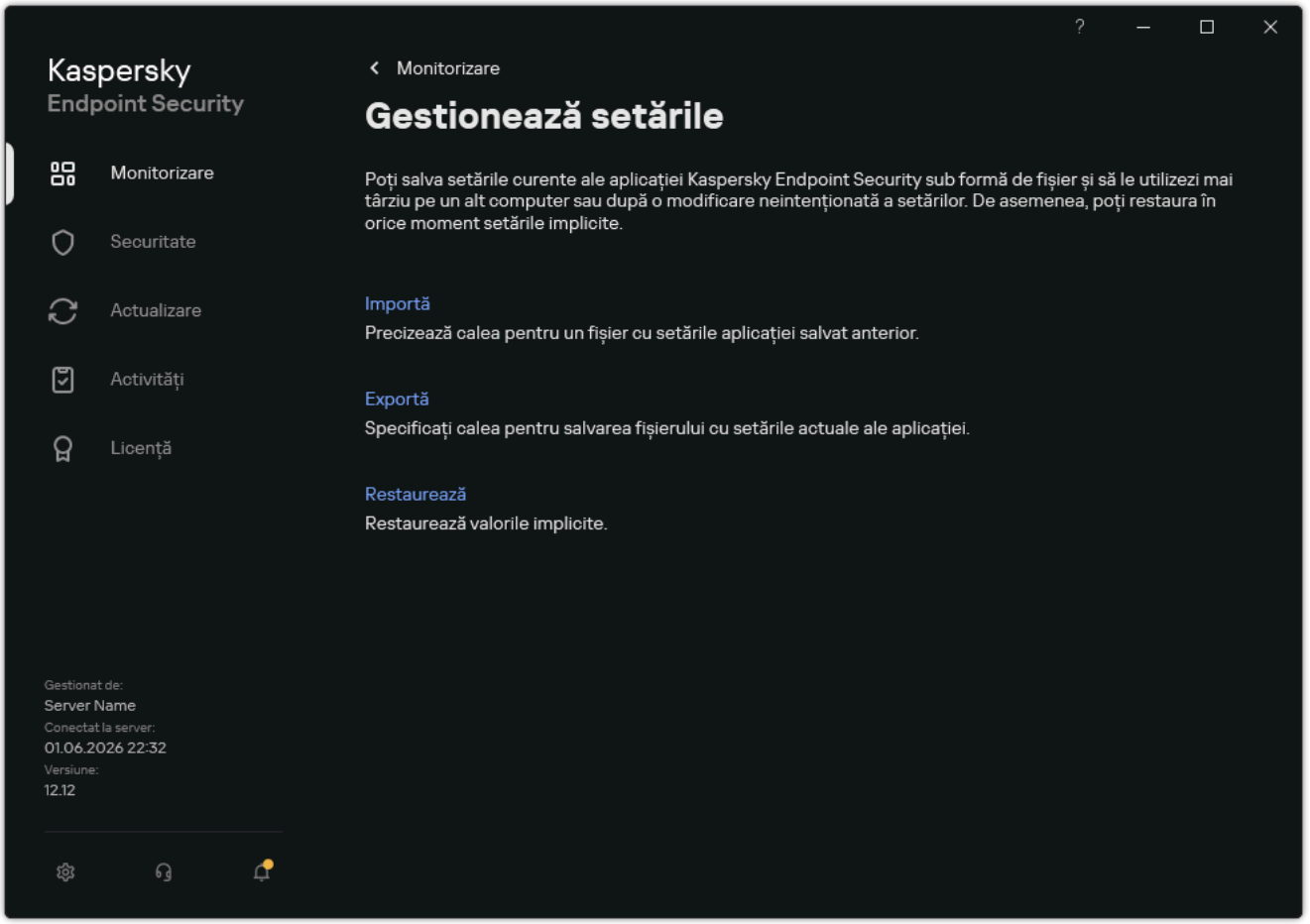
Pentru a importa setările Kaspersky Endpoint Security dintr-un fișier de configurare:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Setări generale** → **Gestionează setările**.
3. Fă clic pe **Importă**.

4. În fereastra care se deschide, introduceți calea către fișierul de configurare.

5. Deschideți fișierul.

Toate valorile setărilor Kaspersky Endpoint Security vor fi setate conform fișierului de configurare selectat.



Gestionarea setărilor aplicației

Restaurarea setărilor implicite ale aplicației

Puteți restaura oricând setările aplicației recomandate de Kaspersky. Când setările sunt restabilite, nivelul de securitate **Recomandat** este setat pentru toate componentele de protecție.

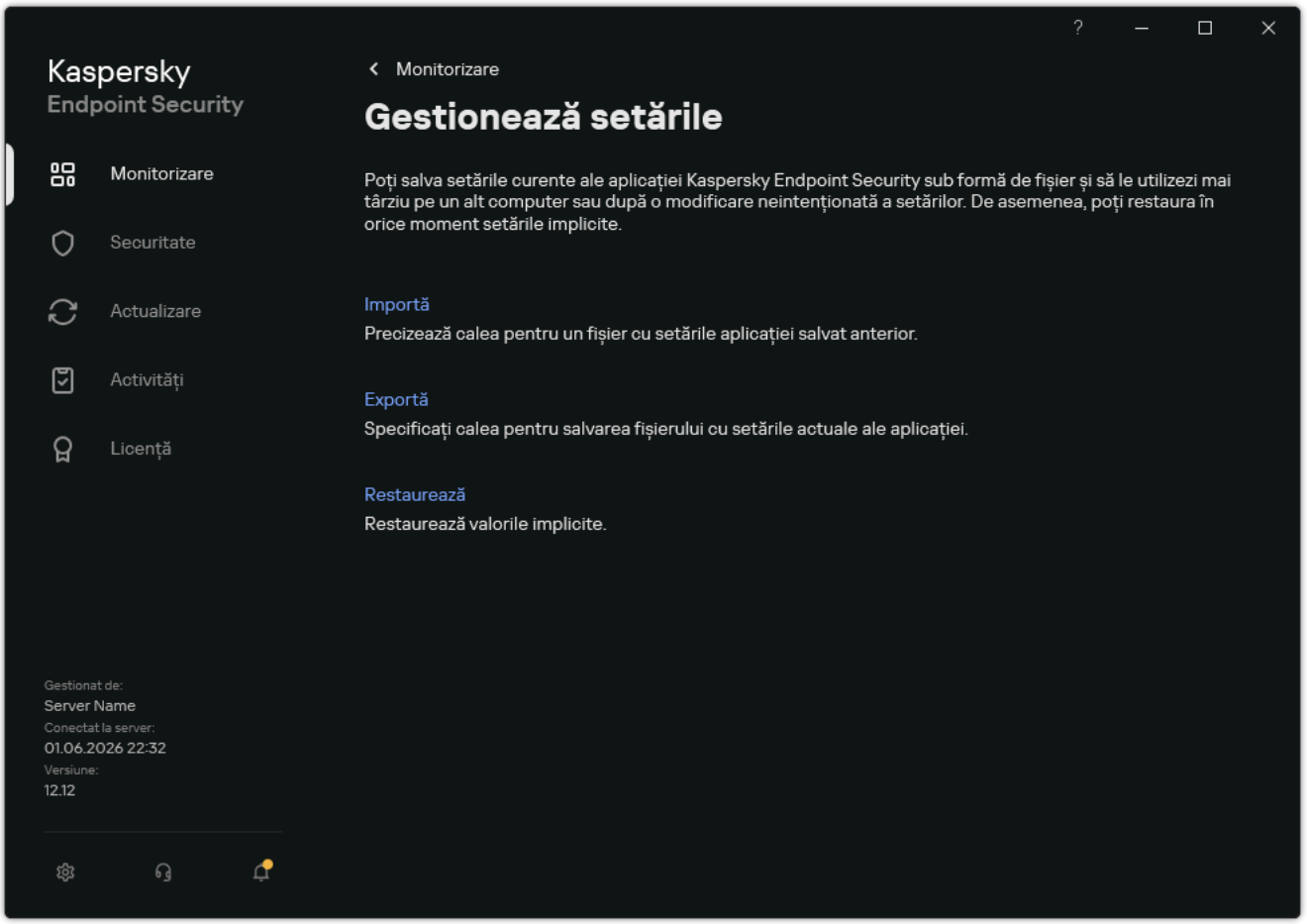
Pentru a restaura setările implicite ale aplicației:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Setări generale** → **Gestionează setările**.

3. Fă clic pe **Restaurează**.

4. Salvați-vă modificările.



Gestionarea setărilor aplicației

Performanța și compatibilitatea produsului Kaspersky Endpoint Security cu alte aplicații

Performanțele Kaspersky Endpoint Security se referă la numărul de tipuri de obiecte ce-ți pot afecta computerul și care pot fi detectate, precum și la consumul de energie și utilizarea resurselor computerului.

Selectarea tipurilor de obiecte detectabile

Kaspersky Endpoint Security îți permite să ajustezi protecția computerului și să selectezi tipurile de obiecte pe care le detectează aplicația în timpul funcționării. Kaspersky Endpoint Security scanează întotdeauna sistemul de operare după viruși, viermi și troieni. Nu poți dezactiva scanarea pentru aceste tipuri de obiecte. Aceste programe malware pot determina pagube grave computerului. Pentru o securitate mai mare pe computer, poți extinde gama de tipuri de obiecte detectabile activând monitorizarea software-ului legal care poate fi folosit de infractori pentru a-ți pune în pericol computerul sau datele personale.

Folosirea modului de economisire a energiei

Consumul de energie de către aplicații este un factor cheie pentru computerele portabile. Activitățile planificate ale Kaspersky Endpoint Security de regulă folosesc resurse considerabile. Atunci când computerul rulează pe baterii, poți folosi modul economisire a energiei pentru a consuma mai puțină putere.

În modul de economisire a energiei, următoarele activități planificate sunt în mod automat amânate:

- activitatea Scanare completă;
- activitatea Scanare zone critice;
- activitatea Scanare personalizată;
- activitatea Verificare integritate.

În funcție de activarea sau nu a modului de economisire a energiei, Kaspersky Endpoint Security pune în pauză activitățile de criptare atunci când un computer portabil trece pe baterie. Aplicația reia activitățile de criptare atunci când computerul portabil trece de la alimentarea pe baterie pe cea de la priză.

Cedarea de resurse pentru alte aplicații

Consumul de resurse ale computerului atunci când se scanează un computer poate crește gradul de încărcare a subsistemelor CPU și ale unității de hard disk. Pentru a rezolva problema funcționării simultane în timp ce procesorul și subsistemele unității de hard disk sunt supuse unul flux de lucru sporit, Kaspersky Endpoint Security poate ceda resursele altor aplicații.

Utilizarea tehnologiei de dezinfectare avansată

Aplicațiile rău intenționate de azi pot pătrunde în zonele cele mai adânci ale sistemului de operare, ceea ce le face practic imposibil de eliminat. După detectarea unei activități periculoase în sistemul de operare, Kaspersky Endpoint Security execută o procedură de dezinfectare extinsă care folosește o tehnologie de dezinfectare avansată. *Advanced disinfection technology* are rolul de a curăța sistemul de operare de aplicații rău intenționate care și-au început deja procesele în memoria RAM și care împiedică eliminarea lor de către Kaspersky Endpoint Security prin alte metode. Prin urmare, amenințarea este neutralizată. În timp ce dezinfectarea avansată este în curs, ți se recomandă să nu pornești procese noi și să nu editezi registrul sistemului de operare. Tehnologia de dezinfectare avansată folosește resurse ale sistemului de operare considerabile, care pot încetini alte aplicații.

După finalizarea procesului de dezinfectare avansată pe un computer pe care se execută Microsoft Windows pentru stații de lucru, Kaspersky Endpoint Security solicită utilizatorului permisiunea de a reporni computerul. După repornirea sistemului, Kaspersky Endpoint Security șterge fișierele programului malware și pornește o scanare completă a computerului.

O solicitare de repornire este imposibilă pe un computer care execută Microsoft Windows pentru servere din cauza aspectelor specifice ale aplicației Kaspersky Endpoint Security. O repornire neplanificată a unui server de fișiere poate conduce la probleme implicând indisponibilitatea temporară a datelor din serverul de fișiere sau pierderea unor date nesalvate. Se recomandă repornirea unui server de fișiere strict conform planificării. De aceea dezinfectarea avansată este dezactivată în mod implicit pentru serverele de fișiere.

Dacă pe un server de fișiere este detectată o infecție activă, este transmis un eveniment către Kaspersky Security Center cu informația că este necesară dezinfectarea avansată. Pentru dezinfectarea unei infectări active de pe un server, activează tehnologia Dezinfectare avansată pentru servere și pornește o activitate de grup *Scanare malware* într-un moment convenabil pentru utilizatorii serverului.

Activarea sau dezactivarea modului de economisire a energiei

Modul Economisire energie este o funcționalitate care reduce solicitarea resurselor laptopului și prelungește durata de viață a bateriei, fără a compromite semnificativ nivelul de securitate. În modul Economisire energie, aplicația limitează lansarea activităților planificate. În acest fel, modul Economisire energie asigură un echilibru între nivelul de securitate și durata de viață a bateriei laptopului.

Atunci când modul de economisire a energiei este activat și computerul funcționează cu alimentare de la baterie, următoarele activități nu sunt executate, chiar dacă sunt planificate:

- *Scanare completă*.
- *Scanare zone critice*.
- *Scanare personalizată*.
- *Verificare integritate aplicație*.
- *Scanare IOC*.
- *Actualizarea modulelor bazelor de date și ale aplicațiilor* (doar corecțiile)

Aplicația omite actualizările planificate ale bazei de date doar atunci când laptopul funcționează pe baterie și nivelul bateriei este sub 30%. În toate celelalte cazuri, Kaspersky Endpoint Security actualizează bazele de date conform planificării, indiferent dacă laptopul este conectat la priză sau funcționează pe baterie sau dacă aplicația este în modul Economisire energie.

Cum se activează sau dezactivează modul Economisire energie în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați **Policies**.
3. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
4. În fereastra politicii, selectați **Setări generale** → **Setări aplicație**.
5. În blocul **Performanță**, bifați sau debifați caseta de selectare **Amână activități planificate la funcționarea cu alimentare de la baterie** pentru a activa sau dezactiva modul de economisire a energiei.
6. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

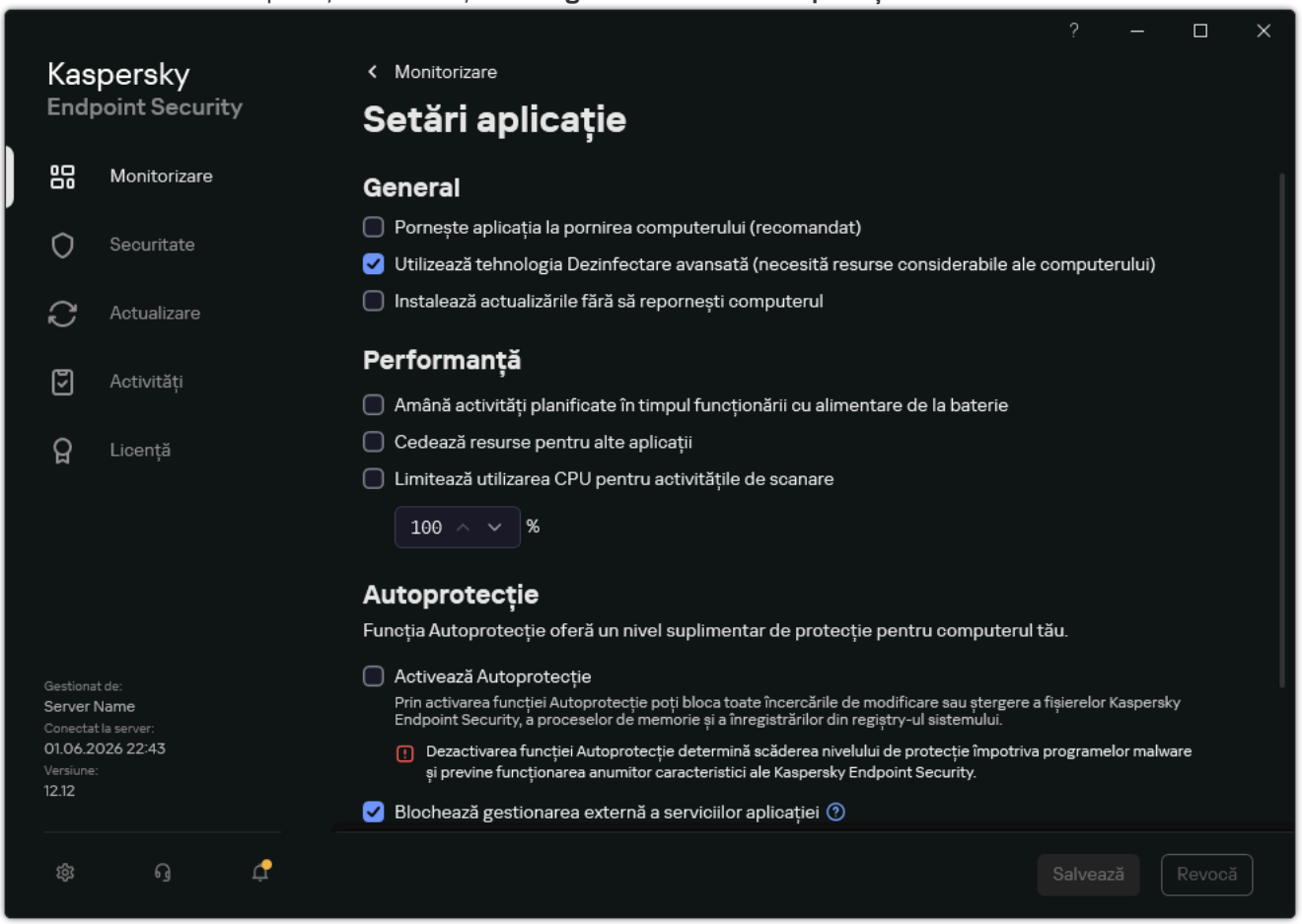
Cum se activează sau dezactivează modul Economisire energie în Web Console

1. În fereastra principală a Web Console, selectați fila **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **General Settings** → **Performance**.
5. În blocul **Postpone or skip scheduled tasks while running on battery power**, bifați sau debifați caseta de selectare **Postpone or skip scheduled tasks while running on battery power (depends on OS)** pentru a activa sau dezactiva modul de economisire a energiei.
6. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se activează sau dezactivează modul Economisire energie în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul .
2. În fereastra cu setările aplicației, selectați **Setări generale** → **Setări aplicație**.



Setări Kaspersky Endpoint Security for Windows

3. În blocul **Performanță**, bifați sau debifați caseta de selectare **Amână activități planificate în timpul funcționării cu alimentare de la baterie** pentru a activa sau dezactiva modul de economisire a energiei.
4. Salvați-vă modificările.

Activarea sau dezactivarea cedării de resurse pentru alte aplicații

Consumul de resurse ale computerului de către Kaspersky Endpoint Security atunci când scanează un computer poate crește gradul de încărcare a subsistemelor CPU și ale unității de hard disk. Acest lucru poate încetini alte aplicații. Pentru a optimiza performanța, Kaspersky Endpoint Security oferă un *mod de transfer al resurselor către alte aplicații*. În acest mod, sistemul de operare poate scădea prioritatea firelor de execuție a activităților de scanare ale Kaspersky Endpoint Security atunci când încărcarea CPU este mare. Acest lucru permite redistribuirea resurselor sistemului de operare către alte aplicații. Astfel, activitățile de scanare vor beneficia de mai puțin timp de procesare. Ca urmare, Kaspersky Endpoint Security va avea nevoie de mai mult timp pentru a scana computerul. În mod implicit, aplicația este configurată să cedeze resurse pentru alte aplicații.

Cum se activează sau dezactivează cedarea resurselor către alte aplicații în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Setări generale** → **Setări aplicație**.
4. În blocul **Performanță**, utilizați caseta de selectare **Cedează resurse pentru alte aplicații** pentru a activa sau dezactiva cedarea resurselor către alte aplicații.
5. Salvați-vă modificările.

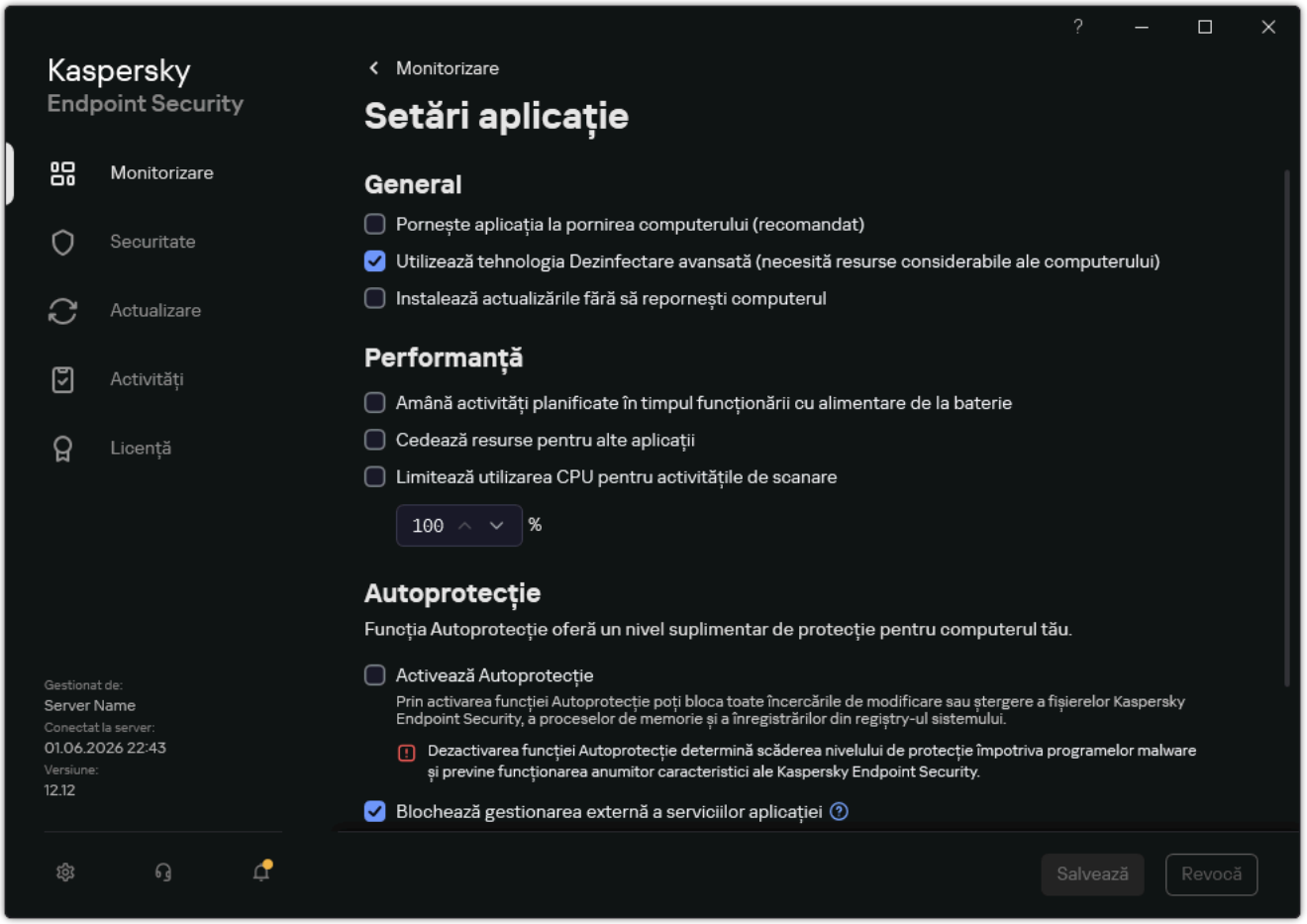
Cum se activează sau dezactivează cedarea resurselor către alte aplicații în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **General Settings** → **Performance**.
5. În blocul **Yield resources to other applications**, utilizează comutatorul **Yield resources to other applications** pentru a activa sau dezactiva cedarea resurselor către alte aplicații.
6. Salvați-vă modificările.

Cum se activează sau se dezactivează cedarea resurselor pentru alte aplicații în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul .
2. În fereastra cu setările aplicației, selectați **Setări generale** → **Setări aplicație**.



Setări Kaspersky Endpoint Security for Windows

3. În blocul **Performanță**, utilizați caseta de selectare **Cedează resurse pentru alte aplicații** pentru a activa sau dezactiva cedarea resurselor către alte aplicații.
4. Salvați-vă modificările.

Cele mai bune practici pentru optimizarea performanței Kaspersky Endpoint Security

Când implementați Kaspersky Endpoint Security for Windows, puteți utiliza următoarele recomandări pentru a configura protecția computerului și pentru a optimiza performanța. Pentru mai multe informații despre rezolvarea problemelor privind performanța computerului, consultă Baza de cunoștințe pentru Suport tehnic.

General

Configurați setările generale ale aplicației în conformitate cu următoarele recomandări:

1. Actualizați Kaspersky Endpoint Security la cea mai recentă versiune.

   Versiunile mai noi ale aplicației au erorile remediate, stabilitatea îmbunătățită și performanța optimizată.

2. Activați componentele de protecție cu setările implicite.

   Setările implicite sunt considerate optime. Aceste setări sunt recomandate de experții Kaspersky. Setările implicite oferă nivelul de protecție recomandat și utilizarea optimă a resurselor. Dacă este necesar, poți restaura setările implicite ale aplicației.

3. Activați funcțiile de optimizare a performanței aplicațiilor.

   Aplicația are funcții de optimizare a performanței: modul de conservare a energiei și acordarea de resurse altor aplicații. Asigurați-vă că aceste opțiuni sunt activate.

Scanare malware pe stațiile de lucru

Este recomandată activarea opțiunii Scanare în fundal pentru activitatea Scanare malware pentru stații de lucru. *Scanare în fundal* este un mod de scanare al aplicației Kaspersky Endpoint Security care nu afișează notificări pentru utilizator. Scanarea în fundal necesită mai puține resurse ale computerului decât alte tipuri de scanări (cum ar fi o scanare completă). În acest mod, Kaspersky Endpoint Security scanează obiectele de pornire, memoria kernel și partiția de sistem. Setările de scanare în fundal sunt considerate optime. Aceste setări sunt recomandate de experții Kaspersky. Astfel, pentru a efectua o Scanare malware a computerului, puteți utiliza doar modul de scanare în fundal, fără a utiliza alte activități de scanare.

Dacă scanarea în fundal nu se potrivește nevoilor dvs., configurați activitatea *Scanare malware* în conformitate cu următoarele recomandări:

1. Setează o limită pentru consumul resurselor procesorului în timpul scanării computerului.

   Poți limita utilizarea procesorului atunci când se execută activitatea *Scanare malware*. Pentru a face acest lucru, în setările aplicației, specifică procentul maxim de încărcare a procesorului pentru toate nucleele care pot fi utilizate în timpul scanării computerului. Acest lucru poate crește timpul necesar pentru scanarea computerului.

2. Configurați planificarea optimă de scanare a computerului.

   Puteți configura ca activitatea să fie executată atunci când computerul funcționează la încărcare minimă. De exemplu, puteți configura ca activitatea să fie executată noaptea sau în weekend-uri.

   Dacă utilizatorii închid computerul în afara programului de lucru, poți activa funcția Wake-on-LAN. Caracteristica Wake-on-LAN permite pornirea de la distanță a computerului, prin trimiterea unui semnal special prin rețeaua locală. Pentru a utiliza această caracteristică, trebuie să activezi Wake-on-LAN în setările BIOS. De asemenea, puteți seta închiderea automată a computerului după terminarea scanării.

   Dacă nu ați putut configura o planificare optimă de scanare, setați ca activitățile să fie executate numai atunci când computerul este inactiv. Kaspersky Endpoint Security pornește activitatea de scanare dacă computerul este blocat sau dacă economizorul de ecran este pornit. Dacă ați întrerupt executarea activității, de exemplu prin deblocarea computerului, Kaspersky Endpoint Security execută automat activitatea, continuând din punctul în care a fost întreruptă.

3. Definiți un domeniu de scanare.

Selectați următoarele obiecte pentru scanare (setul minim de domenii de scanare):

- memoria kernel
- procesele în execuție și obiectele de pornire
- sectoarele de boot
- %systemroot% (fără a include subdirectoarele)
- %systemroot%\System (fără a include subdirectoarele)
- %systemroot%\System32 (fără a include subdirectoarele)
- %systemroot%\System32\drivers (fără a include subdirectoarele)
- %systemroot%\SysWOW64 (fără a include subdirectoarele)
- %systemroot%\SysWOW64\drivers (fără a include subdirectoarele)

4. Activați tehnologiile iSwift și iChecker.

   - Tehnologia iSwift.

     Această tehnologie permite creșterea vitezei de scanare excluzând de la scanare anumite fișiere. Fișierele sunt excluse de la scanări utilizând un algoritm special care ia în considerare data lansării bazelor de date Kaspersky Endpoint Security, data celei mai recente scanări a fișierului și orice modificare adusă setărilor scanării. Tehnologia iSwift reprezintă o versiune îmbunătățită a tehnologiei iChecker și este destinată sistemului de fișiere NTFS.

   - Tehnologia iChecker.

     Această tehnologie permite creșterea vitezei de scanare excluzând de la scanare anumite fișiere. Fișierele sunt excluse de la scanări utilizând un algoritm special care ia în considerare data lansării bazelor de date Kaspersky Endpoint Security, data celei mai recente scanări a fișierului și orice modificare adusă setărilor scanării. Există limitări ale tehnologiei iChecker: aceasta nu funcționează în cazul fișierelor mari și se aplică numai la fișierele cu o structură pe care aplicația o recunoaște (de exemplu, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP și RAR).

   Puteți activa tehnologiile iSwift și iChecker numai în Consola de administrare (MMC) și interfața Kaspersky Endpoint Security. Nu puteți activa aceste tehnologii în Kaspersky Security Center Web Console.

5. Dezactivați scanarea arhivelor protejate prin parolă.

   Dacă scanarea arhivelor protejate prin parolă este activată, este afișată o fereastră de introducere a parolei înainte ca arhiva să fie scanată. Deoarece este recomandat ca activitatea să fie planificată după orele de program, utilizatorul nu poate introduce parola. Puteți scana manual arhivele protejate prin parolă.

6. Dezactivează lansarea simultană a mai multor activități de scanare.

   Kaspersky Endpoint Security va plasa în coadă activitățile noi de scanare dacă scanarea curentă continuă. Acest lucru ajută la optimizarea încărcării computerului.

Scanare malware pe servere

Configurați activitatea *Scanare malware* în conformitate cu următoarele recomandări:

1. Setează o limită pentru consumul resurselor procesorului în timpul scanării computerului.

   Poți limita utilizarea procesorului atunci când se execută activitatea *Scanare malware*. Pentru a face acest lucru, în setările aplicației, specifică procentul maxim de încărcare a procesorului pentru toate nucleele care pot fi utilizate în timpul scanării computerului. Acest lucru poate crește timpul necesar pentru scanarea computerului.

2. Configurați planificarea optimă de scanare a computerului.

   Puteți configura ca activitatea să fie executată atunci când computerul funcționează la încărcare minimă. De exemplu, puteți configura ca activitatea să fie executată noaptea sau în weekend-uri.

3. Activați tehnologiile iSwift și iChecker.

   - Tehnologia iSwift.

     Această tehnologie permite creșterea vitezei de scanare excluzând de la scanare anumite fișiere. Fișierele sunt excluse de la scanări utilizând un algoritm special care ia în considerare data lansării bazelor de date Kaspersky Endpoint Security, data celei mai recente scanări a fișierului și orice modificare adusă setărilor scanării. Tehnologia iSwift reprezintă o versiune îmbunătățită a tehnologiei iChecker și este destinată sistemului de fișiere NTFS.

   - Tehnologia iChecker.

     Această tehnologie permite creșterea vitezei de scanare excluzând de la scanare anumite fișiere. Fișierele sunt excluse de la scanări utilizând un algoritm special care ia în considerare data lansării bazelor de date Kaspersky Endpoint Security, data celei mai recente scanări a fișierului și orice modificare adusă setărilor scanării. Există limitări ale tehnologiei iChecker: aceasta nu funcționează în cazul fișierelor mari și se aplică numai la fișierele cu o structură pe care aplicația o recunoaște (de exemplu, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP și RAR).

   Puteți activa tehnologiile iSwift și iChecker numai în Consola de administrare (MMC) și interfața Kaspersky Endpoint Security. Nu puteți activa aceste tehnologii în Kaspersky Security Center Web Console.

4. Dezactivați scanarea arhivelor protejate prin parolă.

   Dacă scanarea arhivelor protejate prin parolă este activată, este afișată o fereastră de introducere a parolei înainte ca arhiva să fie scanată. Deoarece este recomandat ca activitatea să fie planificată după orele de program, utilizatorul nu poate introduce parola. Puteți scana manual arhivele protejate prin parolă.

5. Dezactivează lansarea simultană a mai multor activități de scanare.

   Kaspersky Endpoint Security va plasa în coadă activitățile noi de scanare dacă scanarea curentă continuă. Acest lucru ajută la optimizarea încărcării computerului.

Kaspersky Security Network

Pentru a-ți proteja mai eficient computerul, Kaspersky Endpoint Security folosește informații primite de la utilizatori de pe întregul glob. Kaspersky Security Network este conceput pentru a obține aceste date.

Kaspersky Security Network (KSN) este o infrastructură de servicii în cloud care oferă acces la Baza de cunoștințe online Kaspersky, care conține informații despre reputația fișierelor, a resurselor Web și a programelor software. Utilizarea datelor de la Kaspersky Security Network asigură răspunsul mai rapid prin Kaspersky Endpoint Security la noile amenințări, îmbunătățește eficiența unor componente ale protecției și reduce posibilitatea alarmelor false. Dacă participați la Kaspersky Security Network, serviciile KSN furnizează componentei Kaspersky Endpoint Security informații despre reputația adreselor web scanate, precum și informații despre categoria și reputația fișierelor scanate.

Editați setările Kaspersky Security Network în conformitate cu următoarele recomandări:

1. Dezactivați modul KSN extins.

   Mod KSN extins este un mod în care Kaspersky Endpoint Security trimite date suplimentare către Kaspersky.

2. Configurează Kaspersky Private Security Network.

   Kaspersky Private Security Network (KPSN) este o soluție care permite utilizatorilor de computere care găzduiesc Kaspersky Endpoint Security sau alte aplicații Kaspersky să obțină acces la bazele de date privind reputația ale Kaspersky și la alte date statistice, fără a trimite date către Kaspersky de la propriile lor computere.

3. Activați modul Cloud.

   Mod cloud se referă la modul de operare al aplicației în care Kaspersky Endpoint Security utilizează o versiune light a bazelor de date antivirus. Kaspersky Security Network acceptă funcționarea aplicației atunci când sunt utilizate baze de date antivirus light. Versiunea light a bazelor de date antivirus vă permite să utilizați aproximativ jumătate din memoria RAM a computerului care ar fi, altfel, utilizată cu bazele de date obișnuite. Dacă nu participați la Kaspersky Security Network sau dacă modul cloud este dezactivat, Kaspersky Endpoint Security descarcă versiunea completă a bazelor de date antivirus de pe serverele Kaspersky.

Scanare malware

Scanarea malware este esențială pentru securitatea computerului. Efectuați regulat scanări malware pentru a elimina posibilitatea de răspândire a programelor malware nedetectate de componentele protecției din cauza unei setări reduse a nivelului de securitate sau din alte motive.

Kaspersky Endpoint Security nu scanează fișierele al căror conținut se află în spațiul de stocare cloud OneDrive și creează intrări de jurnal care menționează că aceste fișiere nu au fost scanate.

Scanare completă

O scanare completă a întregului computer. Kaspersky Endpoint Security scanează următoarele obiecte:

- memoria kernel
- Obiectele încărcate la pornirea sistemului de operare
- sectoarele de boot
- Crearea unei copii de rezervă a sistemului de operare
- Toate unitățile de disc și amovibile

Experții Kaspersky recomandă să nu schimbați domeniul de scanare al activității *Scanare completă*.

Pentru a conserva resursele computerului, este recomandată utilizarea unei activități de scanare în fundal în locul uneia de scanare completă. Acest lucru nu va afecta nivelul de securitate al computerului.

Scanare zone critice

În mod implicit, Kaspersky Endpoint Security scanează memoria kernel, procesele care se execută și sectoarele de boot ale discurilor.

Experții Kaspersky recomandă să nu schimbați domeniul de scanare al activității *Scanare zone critice*.

Scanare personalizată

Kaspersky Endpoint Security scanează obiectele selectate de utilizator. Poți scana orice obiect din următoarea listă:

- Memorie sistem
- Obiectele încărcate la pornirea sistemului de operare
- Crearea unei copii de rezervă a sistemului de operare
- Unități de hard disk, amovibile și de rețea
- Orice fișier selectat

Scanare în fundal

Scanare în fundal este un mod de scanare al aplicației Kaspersky Endpoint Security care nu afișează notificări pentru utilizator. Scanarea în fundal necesită mai puține resurse ale computerului decât alte tipuri de scanări (cum ar fi o scanare completă). În acest mod, Kaspersky Endpoint Security scanează obiectele de pornire, memoria kernel și partiția de sistem.

Verificare integritate aplicație

Kaspersky Endpoint Security verifică modulele aplicației pentru a vedea dacă sunt deteriorate sau modificate.

Scanarea computerului

O scanare este esențială pentru securitatea computerului. Efectuați regulat scanări malware pentru a elimina posibilitatea de răspândire a programelor malware nedetectate de componentele protecției din cauza unei setări reduse a nivelului de securitate sau din alte motive. Componenta oferă protecție computerului cu ajutorul bazelor de date antivirus, a serviciului cloud Kaspersky Security Network și a analizei euristice.

Kaspersky Endpoint Security are următoarele activități standard predefinite: *Scanare completă*, *Scanare zone critice*, *Scanare personalizată*. Dacă organizația dvs. are implementat sistemul de administrare Kaspersky Security Center, puteți crea o activitate *Scanare malware* și configura scanarea.

Cum se execută o activitate de scanare în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați **Tasks**.

3. Selectați activitatea de scanare și faceți dublu clic pentru a deschide proprietățile activității.

   Dacă este necesar, creați activitatea *Scanare malware*.

4. În fereastra cu proprietățile activității, selectați secțiunea **Setări**.

5. Configurați activitatea de scanare (consultați tabelul de mai jos).

   Dacă este necesar, configurați planificarea activității de scanare.

6. Salvați-vă modificările.

7. Executați activitatea de scanare.

Kaspersky Endpoint Security va începe scanarea computerului. Dacă utilizatorul a întrerupt executarea activității (de exemplu, prin închiderea computerului), Kaspersky Endpoint Security execută automat activitatea, continuând din punctul în care scanarea a fost întreruptă.

Cum se execută o activitate de scanare în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe activitatea de scanare.

   Se va deschide fereastra de proprietăți a activității.

3. Selectați fila **Application settings**.

4. Configurați activitatea de scanare (consultați tabelul de mai jos).

   Dacă este necesar, configurați planificarea activității de scanare.

5. Salvați-vă modificările.

6. Executați activitatea de scanare.

Kaspersky Endpoint Security va începe scanarea computerului. Dacă utilizatorul a întrerupt executarea activității (de exemplu, prin închiderea computerului), Kaspersky Endpoint Security execută automat activitatea, continuând din punctul în care scanarea a fost întreruptă.

Cum se execută o activitate de scanare în interfața aplicației

1. În fereastra principală a aplicației, accesați secțiunea **Activități**.

2. În lista de activități, selectați activitatea de scanare și faceți clic pe ⚙.

3. Configurați activitatea de scanare (consultați tabelul de mai jos).

   Dacă este necesar, configurați planificarea activității de scanare.

4. Salvați-vă modificările.

5. Executați activitatea de scanare.

Kaspersky Endpoint Security va începe scanarea computerului. Aplicația va afișa progresul scanării, numărul de fișiere scanate și timpul de scanare rămas. Puteți opri activitatea în orice moment făcând clic pe butonul **Oprește**. Dacă activitatea de scanare nu este afișată, înseamnă că administratorul a interzis utilizarea activităților locale în politică.

Pentru a optimiza performanța Kaspersky Endpoint Security în timpul scanării computerului, puteți gestiona setările avansate ale activității *Scanare completă* și limita utilizarea resurselor procesorului.

În Kaspersky Security Center, puteți utiliza, de asemenea, activitatea *Scanare în fundal* în locul activității *Scanare completă* pentru a optimiza performanța aplicației. Acest lucru nu va afecta nivelul de securitate al computerului. Scanarea în fundal nu poate fi configurată.

Ca urmare, Kaspersky Endpoint Security scanează computerul și, dacă este detectată o amenințare, execută acțiunea configurată în setările aplicației. De obicei, aplicația încearcă să dezinfecteze fișierele infectate. Ca urmare, fișierele infectate pot primi următoarele stări:

- **Amânat**. Fișierul infectat nu a putut fi dezinfectat. Aplicația șterge fișierul infectat după repornirea computerului.
- **Înregistrat în jurnal**. Fișierul infectat nu a putut fi dezinfectat. Aplicația adaugă informații despre fișierele infectate detectate la lista amenințărilor active.
- **Nu se acceptă scrierea** sau **Eroare la scriere**. Fișierul infectat nu a putut fi dezinfectat. Aplicația nu are acces la scriere.
- **A fost deja procesat**. Aplicația a detectat mai devreme un fișier infectat. Aplicația dezinfectează sau șterge fișierul infectat după repornirea computerului.

Setări scanare

Parametru	Descriere
Nivel de securitate	Kaspersky Endpoint Security poate utiliza diferite grupuri de setări pentru executarea unei scanări. Aceste grupuri de setări care sunt stocate în aplicație sunt denumite *niveluri de securitate*: • **Ridicat**. Kaspersky Endpoint Security scanează toate tipurile de fișiere. La scanarea fișierelor compuse, aplicația scanează arhive, pachete de distribuție, fișiere în format Office, dar nu scanează arhivele protejate prin parolă. Când acest nivel de securitate este setat, aplicația utilizează analiza euristică cu nivelul detaliilor **Scanare profundă**. • **Recomandat**. Kaspersky Endpoint Security scanează toate tipurile de fișiere. La scanarea fișierelor compuse, aplicația scanează arhive, pachete de distribuție, fișiere în format Office, dar nu scanează arhivele protejate prin parolă. Când acest nivel de securitate este setat, aplicația utilizează analiza euristică cu nivelul detaliilor **Scanare medie**. • **Redus**. Kaspersky Endpoint Security scanează doar formatele de fișiere specificate. La scanarea fișierelor compuse, aplicația scanează arhive, pachete de distribuție, fișiere în format Office, dar nu scanează arhivele protejate prin parolă. Când acest nivel de securitate este setat, aplicația utilizează analiza euristică cu nivelul detaliilor **Scanare ușoară**. Poți să selectezi unul dintre nivelurile de securitate presetate sau să configurezi manual setările pentru nivelul de securitate. Dacă modifici setările pentru nivelul de securitate, poți reveni oricând la setările recomandate pentru nivelul de securitate.

Parametru	Descriere
Acțiune la detectarea amenințării	**Dezinfectează; șterge dacă dezinfectarea nu reușește**. Dacă selectezi această opțiune, aplicația încearcă automat să dezinfecteze fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, aplicația șterge fișierul. **Dezinfectează; informează dacă dezinfectarea nu reușește**. Dacă selectați această opțiune, Kaspersky Endpoint Security încearcă automat să dezinfecteze toate fișierele infectate care sunt detectate. Dacă dezinfectarea eșuează, Kaspersky Endpoint Security adaugă informațiile despre fișierele infectate detectate în lista de amenințări active. **Informează**. Dacă este selectată această opțiune, Kaspersky Endpoint Security adaugă informațiile despre fișierele infectate în lista de amenințări active la detectarea acestor fișiere. Înainte de a încerca să dezinfectați sau să ștergeți un fișier infectat, aplicația creează o copie de rezervă a fișierului în cazul în care trebuie să restaurați fișierul sau dacă acesta poate fi dezinfectat în viitor. Dacă sunt detectate fișiere infectate care fac parte din aplicația Windows Store, Kaspersky Endpoint Security încearcă să șteargă fișierul.
Execută Dezinfectare avansată imediat *(disponibil numai în consola Kaspersky Security Center)*	Dezinfectarea avansată în timpul unei activități de scanare de viruși pe computer se efectuează doar dacă este activată caracteristica Dezinfectare avansată în proprietățile politicii aplicate pe acest computer. Dacă este bifată caseta de selectare, Kaspersky Endpoint Security dezinfectează infecția activă imediat după ce a fost detectată, în timpul executării activității de scanare de viruși. După dezinfectarea infecției active, Kaspersky Endpoint Security repornește computerul fără a informa utilizatorul. Dacă este debifată caseta de selectare, Kaspersky Endpoint Security nu dezinfectează infecția activă imediat după ce a fost detectată, în timpul executării activității de scanare de viruși. Kaspersky Endpoint Security generează evenimente de infecție activă în rapoartele aplicațiilor locale și în Kaspersky Security Center. Infecția activă poate fi dezinfectată atunci când activitatea de scanare de viruși este executată din nou, având funcția Dezinfectare avansată activată. În acest fel, administratorul de sistem poate alege momentul potrivit pentru a efectua Dezinfecția avansată și apoi să repornească automat computerele.
Domeniu de scanare	Lista obiectelor pe care le scanează aplicația Kaspersky Endpoint Security atunci când efectuează o activitate de scanare. Obiectele din domeniul de scanare pot include memoria kernelului, procesele care rulează, sectoarele de boot, stocarea copiilor de rezervă ale sistemului, hard diskul, unitatea amovibilă sau unitatea, directorul sau fișierul de rețea. În Kaspersky Endpoint Security for Windows 12.12 e-mailul este exclus din domeniul de scanare al aplicației. Scanarea mesajelor de e-mail primite și trimise este efectuată de componenta Mail Threat Protection. Dacă utilizezi o versiune anterioară a plug-in-ului de administrare, aplicația exclude e-mailurile din domeniul de scanare, chiar dacă politica le include.
Planificare scanare	**Manually**. Modul de executare în care puteți porni scanarea manuală la un moment în care vă este convenabil. **By schedule**. În acest mod de executare a activității de scanare, aplicația pornește activitatea de scanare în conformitate cu planificarea specificată. Dacă este selectat acest mod de executare a activității de scanare, activitatea de scanare poate fi pornită și manual.
Amână executarea după pornirea aplicației timp de N minute	Amânarea pornirii activității de scanare după pornirea aplicației. La pornirea sistemului de operare se execută multe procese, de aceea este avantajos să amânați executarea activității de scanare, în loc să o executați imediat după pornirea Kaspersky Endpoint Security.
Execută activitățile omise	Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security pornește activitatea omisă imediat ce acest lucru devine posibil. Activitatea poate fi omisă, de exemplu, dacă computerul a fost oprit la ora programată pentru începerea activității. Când aplicația are ocazia să execute activitățile omise, aceasta le execută aleatoriu într-un anumit interval de timp pentru a distribui încărcarea pe computer. Dacă această casetă de selectare este debifată, Kaspersky Endpoint Security nu execută activitățile omise. În schimb, aplicația execută următoarea activitate în conformitate cu planificarea curentă.
Execută doar atunci când computerul este inactiv	Amânarea începerii activității atunci când resursele computerului sunt ocupate. Kaspersky Endpoint Security pornește activitatea de scanare dacă computerul este blocat sau dacă economizorul de ecran este pornit. Dacă ați întrerupt executarea activității, de exemplu prin deblocarea computerului, Kaspersky Endpoint Security execută automat activitatea, continuând din punctul în care a fost întreruptă. Această opțiune de planificare vă permite să conservați resursele computerului atunci când acesta este utilizat.

Parametru	Descriere
Execută scanarea ca	În mod implicit, activitatea de scanare este executată în numele utilizatorului cu drepturile căruia sunteți înregistrat în sistemul de operare. Domeniul de protecție poate include unități de rețea sau alte obiecte care necesită drepturi speciale de acces. Puteți specifica un utilizator care are drepturile solicitate în setările aplicația și puteți rula activitatea de scanare în contul acestui utilizator.
Tipuri de fișiere	Kaspersky Endpoint Security consideră fișierele fără extensie ca fiind fișiere executabile. Aplicația scanează întotdeauna fișierele executabile, indiferent de tipurile de fișiere selectate pentru scanare. **Toate fișierele**. Dacă se activează această setare, Kaspersky Endpoint Security verifică toate fișierele, fără excepție (toate formatele și toate extensiile). **Fișiere scanate după format**. Dacă se activează această setare, aplicația scanează numai fișierele infectabile. Înainte de scanarea unui fișier pentru detectarea de cod rău intenționat, se analizează antetul intern al fișierului pentru a se determina formatul fișierului (de exemplu, .txt, .doc sau .exe). De asemenea, scanarea caută fișiere cu anumite extensii de fișiere. **Fișiere scanate după extensie**. Dacă se activează această setare, aplicația scanează numai fișierele infectabile. Formatul fișierului se determină în funcție de extensia sa. În mod implicit, Kaspersky Endpoint Security scanează fișierele după formatul acestora. Scanarea fișierelor după extensie este mai puțin sigură, deoarece un fișier rău intenționat poate avea o extensie care nu se află pe lista potențialilor infectabili (de exemplu, `.123`).
Scanează numai fișierele noi și modificate	Scanează numai fișierele noi și acele fișiere care au fost modificate de la ultima dată când au fost scanate. Acest lucru reduce durata unei scanări. Acest mod se aplică atât fișierelor simple, cât și celor compuse.
Omite fișierul scanat acum mai mult de N (de) secunde	Limitarea timpului de executare a activității. După scurgerea duratei specificate, Kaspersky Endpoint Security oprește activitatea. Activitatea nu este marcată ca finalizată. Data viitoare când Kaspersky Endpoint Security execută activitatea, aceasta va fi executată de la început și conform planificării.
Nu executa mai multe activități de scanare în același timp	Amânarea începerii activităților de scanare dacă o scanare este deja în curs de execuție. Kaspersky Endpoint Security va plasa în coadă activitățile noi de scanare dacă scanarea curentă continuă. Acest lucru ajută la optimizarea încărcării computerului. De exemplu, să presupunem că aplicația a început o activitate Scanare completă conform planificării. Dacă un utilizator încearcă să pornească o scanare rapidă din interfața aplicației, Kaspersky Endpoint Security va plasa în coadă această activitate de scanare rapidă și apoi va începe automat această activitate după ce activitatea Scanare completă este finalizată. Cu toate acestea, Kaspersky Endpoint Security începe imediat o activitate de scanare chiar dacă se execută una dintre următoarele activități de scanare: • Scanarea unităților amovibile la conectare. • Scanare din Meniu contextual. • Scanarea zonelor critice care a fost începută după detectarea unui indicator de compromitere (IoC). Dacă această casetă de selectare este debifată, Kaspersky Endpoint Security vă permite să executați mai multe activități de scanare în același timp. Executarea mai multor activități de scanare necesită mai multe resurse ale computerului.
Scanează arhivele	Scanarea arhivelor ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE și a altor arhive. Aplicația scanează arhivele nu doar după extensie, dar și după format. La verificarea arhivelor, aplicația efectuează o dezarhivare recursivă. Acest lucru permite detectarea amenințărilor din arhivele cu mai multe niveluri (o arhivă într-o arhivă).
Scanează pachetele de distribuție	Scanarea pachetelor de distribuție ale aplicațiilor terțe.
Scanează fișierele în formate Microsoft Office	Scanează fișierele Microsoft Office (DOC, DOCX, XLS, PPT și alte extensii Microsoft). Fișierele în format Office includ și obiecte OLE. Aplicația scanează fișierele în format office mai mici de 1 MO, indiferent dacă această casetă de selectare este bifată sau nu.

Parametru	Descriere
Scanează fișierele în format de e-mail	Scanarea fișierelor în format de e-mail și a bazei de date de e-mail. Aplicația scanează fișierele PST și OST utilizate de clienții de e-mail MS Outlook și Windows Mail, precum și fișierele EML. Kaspersky Endpoint Security nu acceptă versiunea pe 64 de biți a clientului de mail Microsoft Outlook. Aceasta înseamnă că Kaspersky Endpoint Security nu scanează fișierele Microsoft Outlook (fișiere PST și OST) dacă pe computer este instalată o versiune de Microsoft Outlook pe 64 de biți, chiar dacă e-mailul este inclus în domeniul de scanare. Dacă este bifată caseta de selectare, Kaspersky Endpoint Security împarte fișierul în format de e-mail în componentele sale (antet, corp, atașamente) și le scanează pentru a detecta amenințări. În cazul în care caseta de selectare este debifată, Kaspersky Endpoint Security scanează fișierul de format de e-mail ca întreg. Când un obiect rău intenționat este descoperit în fișierele PST sau OST, Kaspersky Endpoint Security îl face inofensiv în conformitate cu acțiunea selectată (de exemplu, dezinfectarea sau ștergerea fișierului). Când se detectează un fișier rău intenționat în fișierele altor clienți de e-mail (de exemplu, Mozilla Thunderbird), Kaspersky Endpoint Security doar marchează mesajul infectat. Trebuie să ștergi manual mesajul care conține un atașament infectat.
Scanează arhivele protejate prin parolă	Dacă este bifată caseta de selectare, aplicația scanează arhivele protejate prin parolă. Pentru ca fișierele dintr-o arhivă să fie scanate, ți se solicită să introduci parola. În cazul în care caseta de selectare este debifată, aplicația omite scanarea arhivelor protejate prin parolă.
Nu dezarhiva fișierele compuse mari	Dacă această casetă de selectare este bifată, aplicația nu scanează fișierele compuse a căror dimensiune depășește valoarea specificată. În cazul în care această casetă de selectare este nebifată, aplicația scanează fișierele compuse indiferent de dimensiuni. Aplicația scanează fișierele mari extrase din arhive, indiferent dacă această casetă de selectare este bifată sau nu.
Învățare programată și analiza semnăturilor	Tehnologia Machine și analiza semnăturilor utilizează bazele de date Kaspersky Endpoint Security, care conțin descrieri ale amenințărilor cunoscute și metode de neutralizare a acestora. Protecția care utilizează această metodă asigură un nivel de securitate minim acceptabil. În urma recomandărilor experților Kaspersky, tehnologia Machine learning și analiza semnăturilor este activată în permanență.
Analiză euristică	Tehnologia a fost dezvoltată pentru detectarea amenințărilor care nu se pot detecta utilizând versiunea curentă a bazelor de date ale aplicației Kaspersky. Aceasta detectează fișiere care este posibil să fie infectate cu un virus necunoscut sau cu o variație nouă a unui virus cunoscut. Când scanează fișierele pentru codul rău intenționat, analizatorul euristic execută instrucțiunile din fișierele executabile. Numărul de instrucțiuni executate de analizorul euristic depinde de nivelul specificat pentru analizorul euristic. Nivelul analizei euristice asigură un echilibru între gradul de detaliere a căutării de amenințări noi, gradul de solicitare a resurselor sistemului de operare și durata analizei euristice.
Tehnologia iSwift *(disponibil numai în Consola de administrare (MMC) și în interfața Kaspersky Endpoint Security)*	Această tehnologie permite creșterea vitezei de scanare excluzând de la scanare anumite fișiere. Fișierele sunt excluse de la scanări utilizând un algoritm special care ia în considerare data lansării bazelor de date Kaspersky Endpoint Security, data celei mai recente scanări a fișierului și orice modificare adusă setărilor scanării. Tehnologia iSwift reprezintă o versiune îmbunătățită a tehnologiei iChecker și este destinată sistemului de fișiere NTFS.
Tehnologia iChecker *(disponibil numai în Consola de administrare (MMC) și în interfața Kaspersky Endpoint Security)*	Această tehnologie permite creșterea vitezei de scanare excluzând de la scanare anumite fișiere. Fișierele sunt excluse de la scanări utilizând un algoritm special care ia în considerare data lansării bazelor de date Kaspersky Endpoint Security, data celei mai recente scanări a fișierului și orice modificare adusă setărilor scanării. Există limitări ale tehnologiei iChecker: aceasta nu funcționează în cazul fișierelor mari și se aplică numai la fișierele cu o structură pe care aplicația o recunoaște (de exemplu, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP și RAR).

Scanarea unităților amovibile atunci când sunt conectate la computer

Kaspersky Endpoint Security scanează toate fișierele pe care le execuți sau le copiezi, chiar dacă fișierul se află pe o unitate amovibilă (componenta File Threat Protection). Pentru a preveni răspândirea virușilor și a altor programe malware, puteți configura scanări automate ale unităților amovibile atunci când acestea sunt conectate la computer. Kaspersky Endpoint Security încearcă automat să dezinfecteze toate fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, Kaspersky Endpoint Security șterge fișierele. Componenta menține un computer în siguranță prin executarea scanărilor care implementează învățarea programată, analiza euristică (la nivel înalt) și analiza semnăturilor. Kaspersky Endpoint Security utilizează, de asemenea, tehnologiile de scanare optimizate iSwift și iChecker. Tehnologiile sunt pornite întotdeauna și nu pot fi dezactivate.

Cum se configurează executarea funcției Scanare unități amovibile în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Activități locale** → **Scanare unități amovibile**.
4. În lista verticală **Acțiune la conectarea unei unități amovibile**, selectați **Scanare detaliată** sau **Scanare rapidă**.
5. Configurați opțiunile avansate pentru funcția Scanare unități amovibile (consultați tabelul de mai jos).
6. Salvați-vă modificările.

Cum se configurează executarea funcției Scanare unități amovibile în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.
   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Host Threat Protection** → **Removable Drives Scan**.
5. Utilizați comutatorul **Removable Drives Scan ENABLED** pentru a activa sau a dezactiva componenta.
6. În secțiunea **Scan type**, selectați **Detailed Scan** sau **Quick Scan**.
7. Configurați opțiunile avansate pentru funcția Scanare unități amovibile (consultați tabelul de mai jos).
8. Salvați-vă modificările.

Cum se configurează executarea funcției Scanare unități amovibile în interfața aplicației

1. În fereastra principală a aplicației, accesați secțiunea **Activități**.
2. În lista de activități, selectați activitatea de scanare și faceți clic pe ⚙.

3. Utilizați comutatorul **Scanare unități amovibile** pentru a activa sau a dezactiva scanările unităților amovibile la conectarea la computer.

4. Configurați opțiunile avansate pentru funcția Scanare unități amovibile (consultați tabelul de mai jos).

5. Salvați-vă modificările.

Drept urmare, Kaspersky Endpoint Security execută o scanare a unităților amovibile pentru unitățile amovibile care nu sunt mai mari decât dimensiunea maximă specificată. Dacă activitatea *Scanare unități amovibile* nu este afișată, înseamnă că administratorul a interzis utilizarea activităților locale în politică.

Setări pentru activitatea Scanare unități amovibile

Parametru	Descriere
Scan type	**Detailed Scan**. Dacă este selectată această opțiune, Kaspersky Endpoint Security scanează toate fișierele atunci când este conectată o unitate amovibilă, inclusiv fișierele imbricate în obiecte compuse, arhive, pachete de distribuție și fișiere în formate Office. Kaspersky Endpoint Security nu scanează fișiere în formate de e-mail sau arhive protejate prin parolă. **Quick Scan**. Dacă această opțiune este selectată, după conectarea unei unități amovibile, Kaspersky Endpoint Security va scana doar fișierele cu anumite formate care sunt cele mai vulnerabile să fie infectate și nu va dezarhiva obiectele compuse.
Maximum drive size (MB)	Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security execută acțiunea selectată pe unitățile amovibile cu o dimensiune mai mică decât dimensiunea maximă specificată a unității. Dacă dimensiunea unității amovibile depășește valoarea configurată, Kaspersky Endpoint Security omite scanarea. În cazul în care caseta de selectare este debifată, Kaspersky Endpoint Security efectuează acțiunea selectată pe unitățile amovibile de orice dimensiune.
Hide scan progress bar	Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security afișează progresul scanării unităților amovibile într-o fereastră separată și în secțiunea **Activități**. Dacă această casetă de selectare este debifată, Kaspersky Endpoint Security începe în fundal scanarea unităților amovibile.
Prevent users from stopping the scan	Dacă această casetă de selectare este bifată, pentru activitatea de scanare a unităților amovibile în interfața locală a Kaspersky Endpoint Security, butonul **Oprește** din secțiunea **Activități** și butonul **Oprește** din fereastra de scanare a unităților amovibile nu sunt disponibile.

Scanare în fundal

Scanare în fundal este un mod de scanare al aplicației Kaspersky Endpoint Security care nu afișează notificări pentru utilizator. Scanarea în fundal necesită mai puține resurse ale computerului decât alte tipuri de scanări (cum ar fi o scanare completă). În acest mod, Kaspersky Endpoint Security scanează obiectele de pornire, memoria kernel și partiția de sistem.

Pentru a conserva resursele computerului, este recomandată utilizarea unei activități de scanare în fundal în locul uneia de scanare completă. Acest lucru nu va afecta nivelul de securitate al computerului. Aceste activități au același domeniu de scanare. Pentru a optimiza încărcarea pe computer, aplicația nu execută simultan o activitate Scanare completă și una Scanare în fundal. Dacă ați executat deja o activitate Scanare completă, Kaspersky Endpoint Security nu va porni o activitate Scanare în fundal timp de șapte zile după finalizarea activității Scanare completă.

Scanarea în fundal este pornită în următoarele cazuri:

- După actualizarea bazei de date antivirus.
- După 30 de minute de la pornirea aplicației Kaspersky Endpoint Security.
- La fiecare șase ore.
- Când computerul rămâne inactiv timp de cinci minute sau mai mult (computerul este blocat sau screensaverul este pornit).

Scanarea în fundal atunci când computerul este inactiv este întreruptă când oricare dintre următoarele condiții sunt adevărate:

- Computerul a intrat în modul activ.

  Dacă scanarea în fundal nu a fost executată mai mult de zece zile, scanarea nu este întreruptă.

- Computerul (laptopul) a trecut la modul baterie.

Când se execută scanarea în fundal, Kaspersky Endpoint Security nu scanează fișiere al căror conținut este localizat în spațiul de stocare în cloud OneDrive.

Cum se activează scanarea în fundal în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Activități locale** → **Scanare în fundal**.
4. Utilizați caseta de selectare **Activare scanarea în fundal** pentru a activa sau dezactiva scanarea în fundal.
5. Salvați-vă modificările.

Cum se activează scanarea în fundal în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesează **Host Threat Protection** → **File Threat Protection**.
5. În **Background Scan**, utilizați comutatorul **Background Scan ENABLED** pentru a activa sau dezactiva componenta.
6. Salvați-vă modificările.

Cum se activează scanarea în fundal în interfața aplicației

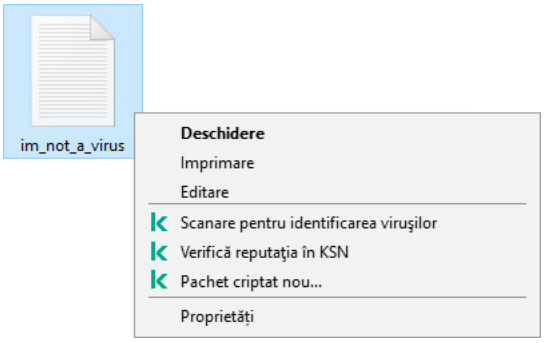
1. În fereastra principală a aplicației, accesați secțiunea **Activități**.
2. În lista de activități, selectați activitatea de scanare și faceți clic pe ⚙.
3. Utilizați comutatorul **Scanare în fundal** pentru a activa sau dezactiva scanările în fundal.
4. Salvați-vă modificările.

Dacă activitatea *Scanare în fundal* nu este afișată, înseamnă că administratorul a interzis utilizarea activităților locale în politică.

Scanare din meniu contextual

Kaspersky Endpoint Security vă permite să executați o scanare a fișierelor individuale pentru viruși și alte programe malware din meniul contextual (vezi figura de mai jos).

Atunci când se execută scanarea din meniul contextual, Kaspersky Endpoint Security nu scanează fișiere al căror conținut este localizat în spațiul de stocare în cloud OneDrive.



Scanare din meniu contextual

Cum se configurează Scanarea din meniul contextual în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Activități locale → Scanează din Meniu contextual**.
4. Configurați Scanare din meniul contextual (consultați tabelul de mai jos).
5. Salvați-vă modificările.

Cum se configurează Scanarea din meniul contextual în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management → Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesează **Host Threat Protection → File Threat Protection**.
5. În **Scan from Context Menu**, configurează opțiunea Scanare din meniul contextual (consultă tabelul de mai jos).
6. Salvați-vă modificările.

Cum se configurează Scanarea din meniul contextual în interfața aplicației

1. În fereastra principală a aplicației, accesați secțiunea **Activități**.
2. În lista de activități, selectați activitatea de scanare și faceți clic pe ⚙.
3. Configurați Scanare din meniul contextual (consultați tabelul de mai jos).
4. Salvați-vă modificările.

Dacă activitatea *Scanare din Meniu contextual* nu este afișată, înseamnă că administratorul a interzis utilizarea activităților locale în politică.

Setările activității Scanare din Meniu contextual

Parametru	Descriere
Nivel de securitate	Kaspersky Endpoint Security poate utiliza diferite grupuri de setări pentru executarea unei scanări. Aceste grupuri de setări care sunt stocate în aplicație sunt denumite *niveluri de securitate*: • **Ridicat**. Kaspersky Endpoint Security scanează toate tipurile de fișiere. La scanarea fișierelor compuse, aplicația scanează arhive, pachete de distribuție, fișiere în format Office, dar nu scanează arhivele protejate prin parolă. Când acest nivel de securitate este setat, aplicația utilizează analiza euristică cu nivelul detaliilor **Scanare profundă**. • **Recomandat**. Kaspersky Endpoint Security scanează toate tipurile de fișiere. La scanarea fișierelor compuse, aplicația scanează arhive, pachete de distribuție, fișiere în format Office, dar nu scanează arhivele protejate prin parolă. Când acest nivel de securitate este setat, aplicația utilizează analiza euristică cu nivelul detaliilor **Scanare medie**. • **Redus**. Kaspersky Endpoint Security scanează doar formatele de fișiere specificate. La scanarea fișierelor compuse, aplicația scanează arhive, pachete de distribuție, fișiere în format Office, dar nu scanează arhivele protejate prin parolă. Când acest nivel de securitate este setat, aplicația utilizează analiza euristică cu nivelul detaliilor **Scanare ușoară**.
Acțiune la detectarea amenințării	**Dezinfectează; șterge dacă dezinfectarea nu reușește**. Dacă selectezi această opțiune, aplicația încearcă automat să dezinfecteze fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, aplicația șterge fișierul. **Dezinfectează; informează dacă dezinfectarea nu reușește**. Dacă selectați această opțiune, Kaspersky Endpoint Security încearcă automat să dezinfecteze toate fișierele infectate care sunt detectate. Dacă dezinfectarea eșuează, Kaspersky Endpoint Security adaugă informațiile despre fișierele infectate detectate în lista de amenințări active. **Informează**. Dacă este selectată această opțiune, Kaspersky Endpoint Security adaugă informațiile despre fișierele infectate în lista de amenințări active la detectarea acestor fișiere.
Tipuri de fișiere	Kaspersky Endpoint Security consideră fișierele fără extensie ca fiind fișiere executabile. Aplicația scanează întotdeauna fișierele executabile, indiferent de tipurile de fișiere selectate pentru scanare. **Toate fișierele**. Dacă se activează această setare, Kaspersky Endpoint Security verifică toate fișierele, fără excepție (toate formatele și toate extensiile). **Fișiere scanate după format**. Dacă se activează această setare, aplicația scanează numai fișierele infectabile. Înainte de scanarea unui fișier pentru detectarea de cod rău intenționat, se analizează antetul intern al fișierului pentru a se determina formatul fișierului (de exemplu, .txt, .doc sau .exe). De asemenea, scanarea caută fișiere cu anumite extensii de fișiere. **Fișiere scanate după extensie**. Dacă se activează această setare, aplicația scanează numai fișierele infectabile. Formatul fișierului se determină în funcție de extensia sa. În mod implicit, Kaspersky Endpoint Security scanează fișierele după formatul acestora. Scanarea fișierelor după extensie este mai puțin sigură, deoarece un fișier rău intenționat poate avea o extensie care nu se află pe lista potențialilor infectabili (de exemplu, `.123`).
Scanează numai fișierele noi și modificate	Scanează numai fișierele noi și acele fișiere care au fost modificate de la ultima dată când au fost scanate. Acest lucru reduce durata unei scanări. Acest mod se aplică atât fișierelor simple, cât și celor compuse.
Omite fișierul scanat acum mai mult de N (de) secunde	Limitarea timpului de executare a activității. După scurgerea duratei specificate, Kaspersky Endpoint Security oprește activitatea. Activitatea nu este marcată ca finalizată. Data viitoare când Kaspersky Endpoint Security execută activitatea, aceasta va fi executată de la început și conform planificării.
Scanează arhivele	Scanarea arhivelor ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE și a altor arhive. Aplicația scanează arhivele nu doar după extensie, dar și după format. La verificarea arhivelor, aplicația efectuează o dezarhivare recursivă. Acest lucru permite detectarea amenințărilor din arhivele cu mai multe niveluri (o arhivă într-o arhivă).
Scanează pachetele de distribuție	Această casetă de selectare activează/dezactivează scanarea pachetelor de distribuție.

Parametru	Descriere
Scanează fișierele în formate Microsoft Office	Scanează fișierele Microsoft Office (DOC, DOCX, XLS, PPT și alte extensii Microsoft). Fișierele în format Office includ și obiecte OLE. Aplicația scanează fișierele în format office mai mici de 1 MO, indiferent dacă această casetă de selectare este bifată sau nu.
Scanează fișierele în format de e-mail	Scanarea fișierelor în format de e-mail și a bazei de date de e-mail. Aplicația scanează fișierele PST și OST utilizate de clienții de e-mail MS Outlook și Windows Mail, precum și fișierele EML. Kaspersky Endpoint Security nu acceptă versiunea pe 64 de biți a clientului de mail Microsoft Outlook. Aceasta înseamnă că Kaspersky Endpoint Security nu scanează fișierele Microsoft Outlook (fișiere PST și OST) dacă pe computer este instalată o versiune de Microsoft Outlook pe 64 de biți, chiar dacă e-mailul este inclus în domeniul de scanare. Dacă este bifată caseta de selectare, Kaspersky Endpoint Security împarte fișierul în format de e-mail în componentele sale (antet, corp, atașamente) și le scanează pentru a detecta amenințări. În cazul în care caseta de selectare este debifată, Kaspersky Endpoint Security scanează fișierul de format de e-mail ca întreg. Când un obiect rău intenționat este descoperit în fișierele PST sau OST, Kaspersky Endpoint Security îl face inofensiv în conformitate cu acțiunea selectată (de exemplu, dezinfectarea sau ștergerea fișierului). Când se detectează un fișier rău intenționat în fișierele altor clienți de e-mail (de exemplu, Mozilla Thunderbird), Kaspersky Endpoint Security doar marchează mesajul infectat. Trebuie să ștergi manual mesajul care conține un atașament infectat.
Scanează arhivele protejate prin parolă	Dacă este bifată caseta de selectare, aplicația scanează arhivele protejate prin parolă. Pentru ca fișierele dintr-o arhivă să fie scanate, ți se solicită să introduci parola. În cazul în care caseta de selectare este debifată, aplicația omite scanarea arhivelor protejate prin parolă.
Nu dezarhiva fișierele compuse mari	Dacă această casetă de selectare este bifată, aplicația nu scanează fișierele compuse a căror dimensiune depășește valoarea specificată. În cazul în care această casetă de selectare este nebifată, aplicația scanează fișierele compuse indiferent de dimensiuni. Aplicația scanează fișierele mari extrase din arhive, indiferent dacă această casetă de selectare este bifată sau nu.
Învățare programată și analiza semnăturilor	Tehnologia Machine și analiza semnăturilor utilizează bazele de date Kaspersky Endpoint Security, care conțin descrieri ale amenințărilor cunoscute și metode de neutralizare a acestora. Protecția care utilizează această metodă asigură un nivel de securitate minim acceptabil. În urma recomandărilor experților Kaspersky, tehnologia Machine learning și analiza semnăturilor este activată în permanență.
Analiză euristică	Tehnologia a fost dezvoltată pentru detectarea amenințărilor care nu se pot detecta utilizând versiunea curentă a bazelor de date ale aplicației Kaspersky. Aceasta detectează fișiere care este posibil să fie infectate cu un virus necunoscut sau cu o variație nouă a unui virus cunoscut. Când scanează fișierele pentru codul rău intenționat, analizatorul euristic execută instrucțiunile din fișierele executabile. Numărul de instrucțiuni executate de analizorul euristic depinde de nivelul specificat pentru analizorul euristic. Nivelul analizei euristice asigură un echilibru între gradul de detaliere a căutării de amenințări noi, gradul de solicitare a resurselor sistemului de operare și durata analizei euristice.
Tehnologia iSwift	Această tehnologie permite creșterea vitezei de scanare excluzând de la scanare anumite fișiere. Fișierele sunt excluse de la scanări utilizând un algoritm special care ia în considerare data lansării bazelor de date Kaspersky Endpoint Security, data celei mai recente scanări a fișierului și orice modificare adusă setărilor scanării. Tehnologia iSwift reprezintă o versiune îmbunătățită a tehnologiei iChecker și este destinată sistemului de fișiere NTFS.
Tehnologia iChecker	Această tehnologie permite creșterea vitezei de scanare excluzând de la scanare anumite fișiere. Fișierele sunt excluse de la scanări utilizând un algoritm special care ia în considerare data lansării bazelor de date Kaspersky Endpoint Security, data celei mai recente scanări a fișierului și orice modificare adusă setărilor scanării. Există limitări ale tehnologiei iChecker: aceasta nu funcționează în cazul fișierelor mari și se aplică numai la fișierele cu o structură pe care aplicația o recunoaște (de exemplu, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP și RAR).

Verificare integritate aplicație

Kaspersky Endpoint Security verifică modulele aplicației pentru a vedea dacă sunt deteriorate sau modificate. De exemplu, dacă o bibliotecă a aplicației are o semnătură digitală incorectă, biblioteca este considerată deteriorată. Activitatea *Verificare integritate aplicație* este destinată verificării fișierelor aplicațiilor. Executați activitatea *Verificare integritate aplicație* dacă Kaspersky Endpoint Security a detectat un obiect rău intenționat, dar nu l-a neutralizat.

Puteți crea activitatea *Verificare integritate aplicație* atât în Kaspersky Security Center Web Console, cât și în Consola de administrare. Nu este posibilă crearea unei activități în Kaspersky Security Center Cloud Console.

Încălcări ale integrității aplicației pot apărea în următoarele cazuri:

- Un obiect rău intenționat a modificat fișierele Kaspersky Endpoint Security. În acest caz, efectuați procedura pentru restaurarea Kaspersky Endpoint Security, utilizând instrumentele sistemului de operare. După restaurare, executați o scanare completă a computerului și repetați verificarea integrității.
- Semnătura digitală a expirat. În acest caz, actualizați Kaspersky Endpoint Security.

Cum se rulează o verificare a integrității aplicației prin Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **New task**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Selectarea tipului activității

Selectați **Kaspersky Endpoint Security for Windows (14.1)** → **Verificare integritate aplicație**.

Pasul 2. Selectarea dispozitivelor cărora le va fi atribuită activitatea

Selectați computerele pe care se va efectua activitatea. Sunt disponibile următoarele opțiuni:

- Atribuirea activității unui grup de administrare. În acest caz, activitatea este atribuită computerelor incluse într-un grup de administrare creat anterior.
- Selectare computere detectate în rețea de Serverul de administrare: *dispozitive neatribuite*. Dispozitivele specifice pot include dispozitive din grupuri de administrare, precum și dispozitive neatribuite.
- Specificarea manuală a adreselor computerelor sau importarea adreselor dintr-o listă. Poți specifica nume NetBIOS, adrese IP și subrețele IP ale dispozitivelor cărora dorești să le atribui activitatea.

Pasul 3. Configurarea unei planificări de pornire a activității

Configurați o planificare pentru începerea unei activități, de exemplu, manual sau atunci când este detectată o infectare cu viruși.

Pasul 4. Definirea numelui activității

Introduceți un nume pentru activitate, de exemplu, *Verificare integritate după ce computerul a fost infectat*.

Pasul 5. Finalizarea creării activității

Ieșiți din Expert. Dacă este necesar, bifați caseta de selectare **Run the task after the wizard finishes**. Puteți monitoriza progresul activității în proprietățile activității. Drept urmare, Kaspersky Endpoint Security va verifica integritatea aplicației. Puteți configura, de asemenea, o planificare a verificării integrității aplicației în proprietățile activității (consultați tabelul de mai jos).

Cum se rulează o verificare a integrității aplicației prin Web Console

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **Add**.

   Expertul de activitate pornește.

3. Configurați setările pentru activitate:

   a. În lista verticală **Application**, selectează **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. În lista verticală **Task type**, selectează **Application Integrity Check**.

   c. În câmpul **Task name**, introduceți o descriere succintă, de exemplu, *Verifică integritatea aplicației după o infectare a computerului*.

   d. În blocul **Devices to which the task will be assigned**, selectați domeniul activității.

4. Selectați dispozitive în funcție de opțiunea selectată pentru domeniul activității. Mergeți la pasul următor.

5. Selectează un cont pentru a executa activitatea. În mod implicit, Kaspersky Endpoint Security începe activitatea cu drepturile unui cont de utilizator local.

6. Ieșiți din Expert.

   Se va afișa o activitate nouă în lista de activități.

7. Bifați caseta de selectare de lângă activitate.

Drept urmare, Kaspersky Endpoint Security va verifica integritatea aplicației. Puteți configura, de asemenea, o planificare a verificării integrității aplicației în proprietățile activității (consultați tabelul de mai jos).

Cum se execută o verificare a integrității în interfața aplicației

1. În fereastra principală a aplicației, accesați secțiunea **Activități**.
2. Se deschide lista de activități; selectați activitatea *Verificare integritate aplicație* și faceți clic pe **Execută**.

Drept urmare, Kaspersky Endpoint Security va verifica integritatea aplicației. Puteți configura, de asemenea, o planificare a verificării integrității aplicației în proprietățile activității (consultați tabelul de mai jos). Dacă activitatea *Verificare integritate aplicație* nu este afișată, înseamnă că administratorul a interzis utilizarea activităților locale în politică.

Setările activității de verificare a integrității

Parametru	Descriere
Planificare scanare	**Manual**. Modul de executare în care puteți porni scanarea manuală la un moment în care vă este convenabil. **Conform planificării**. În acest mod de executare a activității de scanare, aplicația pornește activitatea de scanare în conformitate cu planificarea specificată. Dacă este selectat acest mod de executare a activității de scanare, activitatea de scanare poate fi pornită și manual.
Execută activitățile omise	Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security pornește activitatea omisă imediat ce acest lucru devine posibil. Activitatea poate fi omisă, de exemplu, dacă computerul a fost oprit la ora programată pentru începerea activității. Când aplicația are ocazia să execute activitățile omise, aceasta le execută aleatoriu într-un anumit interval de timp pentru a distribui încărcarea pe computer. Dacă această casetă de selectare este debifată, Kaspersky Endpoint Security nu execută activitățile omise. În schimb, aplicația execută următoarea activitate în conformitate cu planificarea curentă.
Execută doar atunci când computerul este inactiv	Amânarea începerii activității atunci când resursele computerului sunt ocupate. Kaspersky Endpoint Security pornește activitatea de scanare dacă computerul este blocat sau dacă economizorul de ecran este pornit. Dacă ați întrerupt executarea activității, de exemplu prin deblocarea computerului, Kaspersky Endpoint Security execută automat activitatea, continuând din punctul în care a fost întreruptă. Această opțiune de planificare vă permite să conservați resursele computerului atunci când acesta este utilizat.

Editarea domeniului de scanare

Domeniu de scanare este o listă de căi către directoare și căi pe care Kaspersky Endpoint Security le scanează atunci când execută activitatea. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști.

Pentru a edita domeniul de scanare, vă recomandăm să utilizați activitatea *Scanare personalizată*. Experții Kaspersky recomandă să nu schimbați domeniul de scanare al activităților *Scanare completă* și *Scanare zone critice*.

Kaspersky Endpoint Security are următoarele obiecte predefinite ca parte a domeniului de scanare:

- **Memorie sistem**.
- **Procese în execuție și obiecte de pornire**.

  Memoria ocupată de procese și fișierele executabile ale aplicației care sunt executate la pornirea sistemului.
- **Sectoare de încărcare de pe disc**.

  Sectoarele de încărcare de pe unitatea de hard disc și de pe discul amovibil.
- **Copie de rezervă sistem**.

  Conținutul directorului Informații despre volumul sistemului.
- **Toate dispozitivele externe**.

- **Toate unitățile de hard disk**.
- **Toate unitățile de rețea**.

> În Kaspersky Endpoint Security for Windows 12.12 e-mailul este exclus din domeniul de scanare al aplicației. Scanarea mesajelor de e-mail primite și trimise este efectuată de componenta Mail Threat Protection. Dacă utilizezi o versiune anterioară a plug-in-ului de administrare, aplicația exclude e-mailurile din domeniul de scanare, chiar dacă politica le include.

> Vă recomandăm să creați o activitate de scanare separată pentru scanarea unităților de rețea sau a directoarelor partajate. În setările activității *Scanare malware*, specificați un utilizator care are acces de scriere la această unitate; acest lucru este necesar pentru a atenua amenințările detectate. Dacă serverul pe care se află unitatea de rețea are propriile instrumente de securitate, nu executați activitatea de scanare pentru acea unitate. În acest fel, puteți evita verificarea obiectului de două ori și puteți îmbunătăți performanța serverului.

Pentru a exclude directoare sau fișiere din domeniul de scanare, adăugați directorul sau fișierul în zona de încredere.

Cum se editează un domeniu de scanare în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați **Tasks**.
3. Selectați activitatea de scanare și faceți dublu clic pentru a deschide proprietățile activității.

   Dacă este necesar, creați activitatea *Scanare malware*.
4. În fereastra cu proprietățile activității, selectați secțiunea **Setări**.
5. În secțiunea **Domeniu de scanare**, faceți clic pe **Setări**.
6. În fereastra care se deschide, selectează obiectele pe care dorești să le adaugi la domeniul de scanare sau să le excluzi din acesta.
7. Dacă dorești să adaugi un obiect nou la domeniul de scanare:

   a. Fă clic pe **Adaugă**.

   b. În câmpul **Obiect**, introduceți calea către director sau fișier.

Folosiți măști:

- Caracterul `*` (asterisc) ține locul oricărui set de caractere, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\*\*.txt` va include toate căile către fișierele cu extensia TXT din directoarele de pe unitatea C:, dar nu și din subdirectoare.

- Două caractere `*` consecutive țin locul oricărui set de caractere (inclusiv un set gol) din numele de fișier sau director, inclusiv caracterele `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\**\*.txt` va include toate căile către fișierele cu extensia TXT localizată în directoarele imbricate în `Folder`, cu excepția `Folder` în sine. Masca trebuie să includă cel puțin un nivel de imbricare. Masca `C:\**\*.txt` nu este o mască validă.

- `?` (semn de întrebare) ține locul oricărui caracter individual, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\???.txt` va include căi pentru toate fișierele din directorul denumit `Folder` care au extensia TXT și un nume format din trei caractere.

Puteți utiliza măști oriunde într-o cale de fișier sau director. De exemplu, dacă doriți ca domeniul de scanare să includă directorul Descărcări pentru toate conturile de utilizator de pe computer, introduceți masca `C:\Users\*\Downloads\`.

Obiectul **Acest PC** din lista de resurse de fișiere a computerului include următoarele obiecte: **Toate unitățile de hard disk**, **Toate unitățile de rețea** și **Toate unitățile amovibile**.

Puteți exclude un obiect din scanări fără a-l șterge din lista de obiecte din domeniul de scanare. Pentru aceasta, debifați caseta de selectare de lângă obiect.

8. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se editează un domeniu de scanare în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe activitatea de scanare.

   Se va deschide fereastra de proprietăți a activității. Dacă este necesar, creați activitatea *Malware Scan*.

3. Selectați fila **Application settings**.

4. În secțiunea **Scan scope**, selectați obiectele pe care doriți să le adăugați la domeniul de scanare sau să le excludeți din acesta.

5. Dacă dorești să adaugi un obiect nou la domeniul de scanare:

   a. Fă clic pe **Add**.

   b. Introdu calea către director sau fișier.

Folosiți măști:

- Caracterul `*` (asterisc) ține locul oricărui set de caractere, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\*\*.txt` va include toate căile către fișierele cu extensia TXT din directoarele de pe unitatea C:, dar nu și din subdirectoare.

- Două caractere `*` consecutive țin locul oricărui set de caractere (inclusiv un set gol) din numele de fișier sau director, inclusiv caracterele `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\**\*.txt` va include toate căile către fișierele cu extensia TXT localizată în directoarele imbricate în `Folder`, cu excepția `Folder` în sine. Masca trebuie să includă cel puțin un nivel de imbricare. Masca `C:\**\*.txt` nu este o mască validă.

- `?` (semn de întrebare) ține locul oricărui caracter individual, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\???.txt` va include căi pentru toate fișierele din directorul denumit `Folder` care au extensia TXT și un nume format din trei caractere.

Puteți utiliza măști oriunde într-o cale de fișier sau director. De exemplu, dacă doriți ca domeniul de scanare să includă directorul Descărcări pentru toate conturile de utilizator de pe computer, introduceți masca `C:\Users\*\Downloads\`.

Puteți exclude un obiect din scanări fără a-l șterge din lista de obiecte din domeniul de scanare. Pentru aceasta, setați comutatorul de lângă acesta în poziția oprit.

6. Salvați-vă modificările.

Cum se editează un domeniu de scanare în interfața aplicației

1. În fereastra principală a aplicației, accesați secțiunea **Activități**.

2. Se deschide lista de activități; selectați activitatea *Scanare personalizată* și faceți clic pe **Selectează**.

   De asemenea, puteți edita domeniul de scanare pentru alte activități. Experții Kaspersky recomandă să nu schimbați domeniul de scanare al activităților *Scanare completă* și *Scanare zone critice*.

3. În fereastra care se deschide, selectează obiectele pe care dorești să le adaugi la domeniul de scanare.

4. Salvați-vă modificările.

Dacă activitatea de scanare nu este afișată, înseamnă că administratorul a interzis utilizarea activităților locale în politică.

Executarea unei scanări planificate

Scanarea pentru depistarea programelor malware folosind activitatea *Scanare malware* poate dura mult timp și poate crește consumul de resurse ale computerului de către Kaspersky Endpoint Security. Prin urmare, se recomandă alegerea unui moment optim pentru executarea activității, astfel încât impactul asupra performanței celorlalte aplicații să fie redus la minimum.

De exemplu, dacă angajații din organizația dvs. lucrează după un program fix, puteți configura o scanare a computerului să se execute noaptea sau în weekend. Dacă nu se poate executa activitatea dintr-un anumit motiv (de exemplu, computerul este oprit la momentul respectiv), poți configura activitatea omisă pentru executare automată atunci când este posibil. Această funcție trebuie utilizată cu precauție, deoarece poate încetini aplicațiile de pe computerul utilizatorului atunci când acesta este pornit dimineața.

Dacă nu puteți stabili un program de scanare optim care să se potrivească nevoilor dvs., puteți configura ca scanarea să se execute atunci când este îndeplinită una dintre următoarele condiții speciale:

- După o actualizare a bazei de date.

  Kaspersky Endpoint Security execută scanarea computerului cu bazele de date de semnături actualizate.

- După pornirea aplicației.

  Kaspersky Endpoint Security efectuează o scanare a computerului după o anumită perioadă de timp de la pornirea aplicației. La pornirea sistemului de operare se execută multe procese, de aceea este avantajos să amânați executarea activității de scanare, în loc să o executați imediat după pornirea Kaspersky Endpoint Security.

- Caracteristica Wake-on-LAN.

  Kaspersky Endpoint Security execută o scanare a computerului conform planificării, chiar dacă computerul este oprit. Pentru aceasta, aplicația folosește caracteristica Wake-on-LAN a sistemului de operare. Caracteristica Wake-on-LAN permite pornirea de la distanță a computerului, prin trimiterea unui semnal special prin rețeaua locală. Pentru a utiliza această caracteristică, trebuie să activezi Wake-on-LAN în setările BIOS.

  Poți configura executarea scanării utilizând Wake-on-LAN numai pentru activitatea *Scanare malware* în Kaspersky Security Center. Nu poți activa Wake-on-LAN pentru scanarea computerului în interfața aplicației.

- Când computerul este inactiv.

  Kaspersky Endpoint Security execută o scanare a computerului conform planificării, atunci când economizorul de ecran este activ sau ecranul este blocat. Dacă utilizatorul deblochează computerul, Kaspersky Endpoint Security pune în pauză scanarea. În acest caz, Scanarea completă poate dura câteva zile.

- Când activitatea a fost omisă.

  Kaspersky Endpoint Security execută activitatea omisă imediat ce este posibil. Activitatea poate fi omisă, de exemplu, dacă computerul a fost oprit la ora programată pentru începerea activității. Când aplicația are ocazia să execute activitățile omise, aceasta le execută aleatoriu într-un anumit interval de timp pentru a distribui încărcarea pe computer.

Cum se configurează planificarea scanării în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe activitatea de scanare.

   Se va deschide fereastra de proprietăți a activității.

3. În fereastra cu proprietățile activității, selectați fila **Schedule**.

4. Configurați programul activității de scanare.

5. În funcție de frecvența selectată, configurați setările avansate care specifică programul de executare a activității (consultați tabelul de mai jos).

6. Salvați-vă modificările.

Cum se editează planificarea scanării în interfața aplicației

Puteți configura programul de scanare numai dacă o politică nu este aplicată computerului. Pentru computerele cărora le este aplicată politica, puteți configura planificarea activității *Scanare malware* în Kaspersky Security Center.

1. În fereastra principală a aplicației, accesați secțiunea **Activități**.
2. În lista de activități, selectați activitatea de scanare și faceți clic pe .

   Puteți configura un program pentru a executa o Scanare completă, o Scanare zone critice sau o Verificare integritate. Puteți executa o Scanare personalizată numai manual.
3. Fă clic pe **Planificare scanare**.
4. În fereastra care se deschide, configurează planificarea de executare a activității de scanare.
5. În funcție de frecvența selectată, configurați setările avansate care specifică programul de executare a activității (consultați tabelul de mai jos).
6. Salvați-vă modificările.

Setări planificare scanare

Parametru	Descriere
Planificare scanare	**Manual**. Modul de executare în care puteți porni scanarea manuală la un moment în care vă este convenabil. **Conform planificării**. În acest mod de executare a activității de scanare, aplicația pornește activitatea de scanare în conformitate cu planificarea specificată. Dacă este selectat acest mod de executare a activității de scanare, activitatea de scanare poate fi pornită și manual.
Amână executarea după pornirea aplicației timp de N minute	Amânarea pornirii activității de scanare după pornirea aplicației. La pornirea sistemului de operare se execută multe procese, de aceea este avantajos să amânați executarea activității de scanare, în loc să o executați imediat după pornirea Kaspersky Endpoint Security.
Execută activitățile omise	Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security pornește activitatea omisă imediat ce acest lucru devine posibil. Activitatea poate fi omisă, de exemplu, dacă computerul a fost oprit la ora programată pentru începerea activității. Când aplicația are ocazia să execute activitățile omise, aceasta le execută aleatoriu într-un anumit interval de timp pentru a distribui încărcarea pe computer. Dacă această casetă de selectare este debifată, Kaspersky Endpoint Security nu execută activitățile omise. În schimb, aplicația execută următoarea activitate în conformitate cu planificarea curentă.
Execută doar atunci când computerul este inactiv	Amânarea începerii activității atunci când resursele computerului sunt ocupate. Kaspersky Endpoint Security pornește activitatea de scanare dacă computerul este blocat sau dacă economizorul de ecran este pornit. Dacă ați întrerupt executarea activității, de exemplu prin deblocarea computerului, Kaspersky Endpoint Security execută automat activitatea, continuând din punctul în care a fost întreruptă. Această opțiune de planificare vă permite să conservați resursele computerului atunci când acesta este utilizat.
Use automatically randomized delay for task starts *(disponibil numai în consola Kaspersky Security Center)*	Dacă este bifată caseta de selectare, activitatea nu se execută strict conform planificării, ci aleatoriu într-un anumit interval, adică orele de începere ale sarcinii sunt împrăștiate. Orele de pornire aleatorii ajută la evitarea unui număr mare de computere care accesează simultan Serverul de administrare atunci când activitatea este executată conform planificării. Intervalul orelor de pornire aleatorii este calculat automat la crearea activității, în funcție de numărul de computere care au atribuită activitatea. Ulterior, activitatea se execută întotdeauna la ora de începere calculată. Cu toate acestea, ori de câte ori setările activității sunt modificate sau activitatea este executată manual, ora de începere calculată se modifică. În cazul în care caseta de selectare este debifată, activitatea se execută exact la ora programată.
Use randomized delay for task starts within an interval of (min)	Dacă această casetă de selectare este bifată, activitatea este executată pe computere la un moment aleator, într-un anumit interval de timp. Orele de pornire aleatorii ajută la evitarea unui număr mare de computere care accesează simultan Serverul de administrare atunci când activitatea este executată conform planificării. În cazul în care caseta de selectare este debifată, activitatea se execută exact la ora programată.

Parametru	Descriere
Stop the task if it runs longer than (min) *(disponibil numai în consola Kaspersky Security Center)*	Limitarea timpului de executare a activității. După scurgerea duratei specificate, Kaspersky Endpoint Security oprește activitatea. Activitatea nu este marcată ca finalizată. Data viitoare când Kaspersky Endpoint Security execută activitatea, aceasta va fi executată de la început și conform planificării. Pentru a reduce timpul de execuție a activității, puteți, de exemplu, să configurați domeniul de scanare sau să optimizați scanarea.
Turn on devices by using the Wake-on-LAN function before starting the task (min) *(disponibil numai în consola Kaspersky Security Center)*	Dacă este bifată caseta de selectare, sistemului de operare al computerului i se acordă un avans pentru a finaliza pornirea înainte de executarea activității. Avansul implicit este de 5 minute. Bifați caseta de selectare dacă doriți să executați activitatea pe toate computerele, inclusiv pe computerele oprite.
Shut down the devices after completing the task *(disponibil numai în consola Kaspersky Security Center)*	De exemplu, puteți activa această funcționalitate pentru a scana computerul în zilele de vineri, după programul de lucru. Când actvitatea se termină, aplicația oprește computerul pe parcursul weekendului.
Pauză activitate	Poți specifica un interval de timp în care execuția unei activități programate anterior va fi întreruptă. După expirarea perioadei de timp specificate, activitatea va fi reluată. Acest lucru poate fi necesar, de exemplu, pentru a minimiza impactul Kaspersky Endpoint Security asupra performanței computerului în perioadele de utilizare maximă.
Dezactivează planificarea începând cu	Dacă este bifată caseta de selectare, Kaspersky Endpoint Security va opri executarea activității programate începând cu data specificată. Activitatea va fi setată în modul **Manual**.

Executarea unei scanări ca utilizator diferit

În mod implicit, activitatea de scanare este executată în numele utilizatorului cu drepturile căruia sunteți înregistrat în sistemul de operare. Domeniul de protecție poate include unități de rețea sau alte obiecte care necesită drepturi speciale de acces. Puteți specifica un utilizator care are drepturile solicitate în setările aplicația și puteți rula activitatea de scanare în contul acestui utilizator.

Puteți executa următoarele scanări ca utilizator diferit:

- Scanare zone critice.
- Scanare completă.
- Scanare particularizată.
- Scanare din Meniu contextual.

Nu puteți configura drepturile utilizatorului pentru a executa o Scanare unități amovibile, o Scanare în fundal sau o Verificare integritate.

Cum se execută o scanare ca utilizator diferit în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Managed devices** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectează fila **Tasks**.
4. Selectați activitatea de scanare și faceți dublu clic pentru a deschide proprietățile activității.
5. În fereastra cu proprietățile activității, selectați secțiunea **Account**.

6. Introduceți acreditările contului utilizatorului ale cărui drepturi doriți să le utilizați pentru a executa o activitate de scanare.

7. Salvați-vă modificările.

Cum se execută o scanare ca utilizator diferit în Web Console sau Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe activitatea de scanare.

   Se va deschide fereastra de proprietăți a activității.

3. Selectați fila **Settings**.

4. În blocul **Account**, fă clic pe butonul **Settings**.

5. Introduceți acreditările contului utilizatorului ale cărui drepturi doriți să le utilizați pentru a executa o activitate de scanare.

6. Salvați-vă modificările.

Cum se execută o scanare ca utilizator diferit în interfața aplicației

1. În fereastra principală a aplicației, accesați secțiunea **Activități**.

2. În lista de activități, selectați activitatea de scanare și faceți clic pe ⚙.

3. În proprietățile activității, selectați **Setări avansate** → **Execută scanarea ca**.

4. În fereastra care se deschide, introdu acreditările contului ale cărui drepturi dorești să le utilizezi pentru a executa o activitate de scanare.

5. Salvați-vă modificările.

Dacă activitatea de scanare nu este afișată, înseamnă că administratorul a interzis utilizarea activităților locale în politică.

Optimizarea scanării

Limitarea utilizării procesorului în timpul scanării computerului

Poți limita utilizarea procesorului atunci când se execută activitatea *Scanare malware*. Acest lucru poate crește timpul necesar pentru scanarea computerului.

Cum să limitezi utilizarea procesorului la scanarea computerului în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.

2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

3. În fereastra politicii, selectați **Setări generale** → **Setări aplicație**.

4. În **Performanță**, bifează caseta de selectare **Limitează utilizarea CPU pentru activitățile de scanare** și introdu valoarea medie a consumului resursei procesorului în procente.

5. Salvați-vă modificările.

Cum să limitezi utilizarea procesorului la scanarea computerului în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **General Settings** → **Performance**.

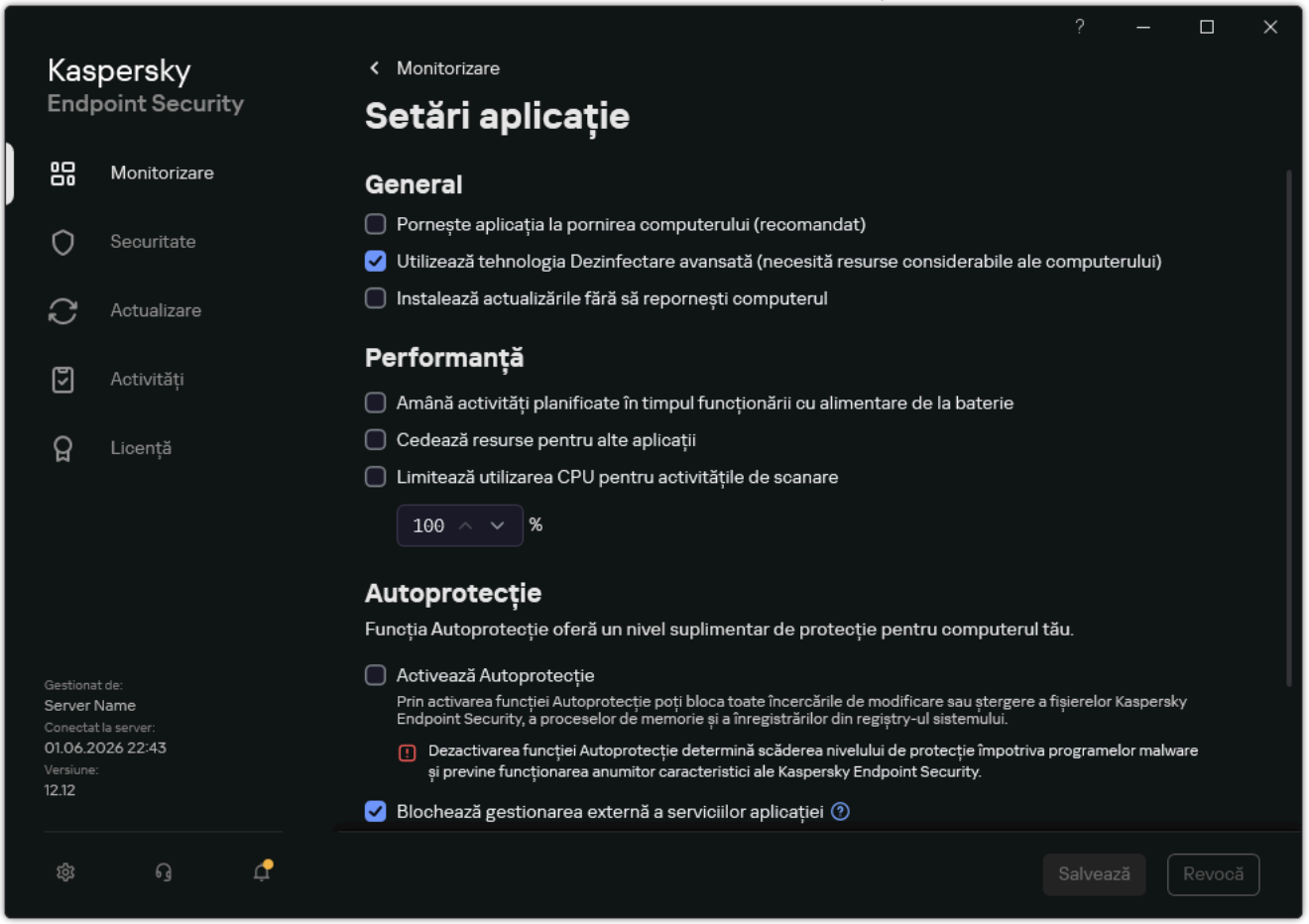
5. În **Limit CPU usage for scan tasks**, setează comutatorul la **Limit CPU usage for scan tasks** și introdu valoarea medie a consumului resursei procesorului în procente.

6. Salvați-vă modificările.

Cum să limitezi utilizarea procesorului la scanarea computerului în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Setări generale** → **Setări aplicație**.



Setări Kaspersky Endpoint Security for Windows

3. În **Performanță**, bifează caseta de selectare **Limitează utilizarea CPU pentru activitățile de scanare** și introdu valoarea medie a consumului resursei procesorului în procente.

4. Salvați-vă modificările.

Configurarea setările avansate ale activității pentru Scanare malware.

Poți optimiza scanarea fișierelor, reducând durata scanării și sporind viteza de funcționare a aplicației Kaspersky Endpoint Security. Acest lucru se obține prin scanarea numai a fișierelor noi și a celor care au fost modificate din momentul scanării ulterioare. Acest mod se aplică atât fișierelor simple, cât și celor compuse. De asemenea, poți seta o limită pentru scanarea unui fișier individual. După expirarea intervalului de timp specificat, Kaspersky Endpoint Security exclude fișierul din scanarea curentă (cu excepția arhivelor și a obiectelor care includ mai multe fișiere).

O tehnică obișnuită de ascundere a virușilor și a altor programe malware o reprezintă introducerea acestora în fișiere compuse, precum arhive sau baze de date. Pentru a detecta virușii și celelalte programe malware ascunse în acest mod, fișierul compus trebuie dezarhivat, fapt care poate încetini scanarea. Poți limita tipurile de fișiere compuse de scanat, accelerând astfel scanarea.

De asemenea, puteți activa tehnologiile iChecker și iSwift. Tehnologiile iChecker și iSwift optimizează viteza de scanare a fișierelor, excluzând fișierele care nu au fost modificate de la cea mai recentă scanare.

Cum se optimizează scanarea în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.

2. În arborele consolei, selectați **Tasks**.

3. Selectați activitatea de scanare și faceți dublu clic pentru a deschide proprietățile activității.

   Dacă este necesar, creați activitatea *Scanare malware*.

4. În fereastra cu proprietățile activității, selectați secțiunea **Setări**.

5. În blocul **Nivel de securitate**, fă clic pe butonul **Setări**.

   Se deschide fereastra de setări pentru activitatea de scanare.

6. În blocul **Optimizare**, configurați setările de scanare:

   - **Scanează numai fișiere noi și modificate**. Scanează numai fișierele noi și acele fișiere care au fost modificate de la ultima dată când au fost scanate. Acest lucru reduce durata unei scanări. Acest mod se aplică atât fișierelor simple, cât și celor compuse.

     De asemenea, puteți configura scanarea fișierelor noi după tip. De exemplu, puteți scana toate pachetele de distribuție și puteți scana numai arhive noi și fișiere în format office.

- **Omite fișiere scanate mai mult de N sec**. Limitarea timpului de executare a activității. După scurgerea duratei specificate, Kaspersky Endpoint Security oprește activitatea. Activitatea nu este marcată ca finalizată. Data viitoare când Kaspersky Endpoint Security execută activitatea, aceasta va fi executată de la început și conform planificării.

- **Nu executa mai multe activități de scanare în același timp**. Amânarea începerii activităților de scanare dacă o scanare este deja în curs de execuție. Kaspersky Endpoint Security va plasa în coadă activitățile noi de scanare dacă scanarea curentă continuă. Acest lucru ajută la optimizarea încărcării computerului. De exemplu, să presupunem că aplicația a început o activitate Scanare completă conform planificării. Dacă un utilizator încearcă să pornească o scanare rapidă din interfața aplicației, Kaspersky Endpoint Security va plasa în coadă această activitate de scanare rapidă și apoi va începe automat această activitate după ce activitatea Scanare completă este finalizată.

7. Fă clic pe **Suplimentar**.

   Se deschide fereastra de setări pentru scanarea fișierelor compuse.

8. În blocul **Limită dimensiune**, bifați caseta de selectare **Nu dezarhiva fișierele compuse mari**. Limitarea timpului de executare a activității. După scurgerea duratei specificate, Kaspersky Endpoint Security oprește activitatea. Activitatea nu este marcată ca finalizată. Data viitoare când Kaspersky Endpoint Security execută activitatea, aceasta va fi executată de la început și conform planificării.

   > Kaspersky Endpoint Security scanează fișierele de dimensiuni mari extrase din arhive indiferent dacă este bifată sau nu caseta de selectare **Nu dezarhiva fișierele compuse mari**.

9. Fă clic pe **OK**.

10. Accesați fila **Suplimentar**.

11. În blocul **Tehnologii de scanare**, bifați casetele de selectare de lângă numele tehnologiilor care doriți să fie utilizate în timpul unei scanări:

    - **Tehnologia iSwift**. Această tehnologie permite creșterea vitezei de scanare excluzând de la scanare anumite fișiere. Fișierele sunt excluse de la scanări utilizând un algoritm special care ia în considerare data lansării bazelor de date Kaspersky Endpoint Security, data celei mai recente scanări a fișierului și orice modificare adusă setărilor scanării. Tehnologia iSwift reprezintă o versiune îmbunătățită a tehnologiei iChecker și este destinată sistemului de fișiere NTFS.

    - **Tehnologia iChecker**. Această tehnologie permite creșterea vitezei de scanare excluzând de la scanare anumite fișiere. Fișierele sunt excluse de la scanări utilizând un algoritm special care ia în considerare data lansării bazelor de date Kaspersky Endpoint Security, data celei mai recente scanări a fișierului și orice modificare adusă setărilor scanării. Există limitări ale tehnologiei iChecker: aceasta nu funcționează în cazul fișierelor mari și se aplică numai la fișierele cu o structură pe care aplicația o recunoaște (de exemplu, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP și RAR).

12. Salvați-vă modificările.

Cum se optimizează scanarea în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe activitatea de scanare.

   Se va deschide fereastra de proprietăți a activității. Dacă este necesar, creați activitatea *Malware Scan*.

3. Selectați fila **Application settings**.

4. În blocul **Action on threat detection**, bifați caseta de selectare **Scan only new and modified files**. Scanează numai fișierele noi și acele fișiere care au fost modificate de la ultima dată când au fost scanate. Acest lucru reduce durata unei scanări. Acest mod se aplică atât fișierelor simple, cât și celor compuse.

   De asemenea, puteți configura scanarea fișierelor noi după tip. De exemplu, puteți scana toate pachetele de distribuție și puteți scana numai arhive noi și fișiere în format office.

5. În blocul **Scan optimization**, bifați caseta de selectare **Do not unpack large compound files**. Limitarea timpului de executare a activității. După scurgerea duratei specificate, Kaspersky Endpoint Security oprește activitatea. Activitatea nu este marcată ca finalizată. Data viitoare când Kaspersky Endpoint Security execută activitatea, aceasta va fi executată de la început și conform planificării.

   > Kaspersky Endpoint Security scanează fișierele de dimensiuni mari extrase din arhive indiferent dacă este bifată sau nu caseta de selectare **Do not unpack large compound files**.

6. Bifați caseta de selectare **Do not run multiple scan tasks at the same time**. Amânarea începerii activităților de scanare dacă o scanare este deja în curs de execuție. Kaspersky Endpoint Security va plasa în coadă activitățile noi de scanare dacă scanarea curentă continuă. Acest lucru ajută la optimizarea încărcării computerului. De exemplu, să presupunem că aplicația a început o activitate Scanare completă conform planificării. Dacă un utilizator încearcă să pornească o scanare rapidă din interfața aplicației, Kaspersky Endpoint Security va plasa în coadă această activitate de scanare rapidă și apoi va începe automat această activitate după ce activitatea Scanare completă este finalizată.

7. În blocul **Advanced settings**, bifați caseta de selectare **Skip file that is scanned for longer than (sec)**. Limitarea timpului de executare a activității. După scurgerea duratei specificate, Kaspersky Endpoint Security oprește activitatea. Activitatea nu este marcată ca finalizată. Data viitoare când Kaspersky Endpoint Security execută activitatea, aceasta va fi executată de la început și conform planificării.

8. Salvați-vă modificările.

Cum se optimizează scanarea în interfața aplicației

1. În fereastra principală a aplicației, accesați secțiunea **Activități**.

2. În lista de activități, selectați activitatea de scanare și faceți clic pe ⚙.

3. Fă clic pe **Setări avansate**.

4. În blocul **Optimizare**, configurați setările de scanare:

   - **Scanează numai fișierele noi și modificate**. Scanează numai fișierele noi și acele fișiere care au fost modificate de la ultima dată când au fost scanate. Acest lucru reduce durata unei scanări. Acest mod se aplică atât fișierelor simple, cât și celor compuse.

     De asemenea, puteți configura scanarea fișierelor noi după tip. De exemplu, puteți scana toate pachetele de distribuție și puteți scana numai arhive noi și fișiere în format office.

- **Omite fișierul scanat acum mai mult de N (de) secunde**. Limitarea timpului de executare a activității. După scurgerea duratei specificate, Kaspersky Endpoint Security oprește activitatea. Activitatea nu este marcată ca finalizată. Data viitoare când Kaspersky Endpoint Security execută activitatea, aceasta va fi executată de la început și conform planificării.

- **Nu executa mai multe activități de scanare în același timp**. Amânarea începerii activităților de scanare dacă o scanare este deja în curs de execuție. Kaspersky Endpoint Security va plasa în coadă activitățile noi de scanare dacă scanarea curentă continuă. Acest lucru ajută la optimizarea încărcării computerului. De exemplu, să presupunem că aplicația a început o activitate Scanare completă conform planificării. Dacă un utilizator încearcă să pornească o scanare rapidă din interfața aplicației, Kaspersky Endpoint Security va plasa în coadă această activitate de scanare rapidă și apoi va începe automat această activitate după ce activitatea Scanare completă este finalizată.

5. În blocul **Limită dimensiune**, bifați caseta de selectare **Nu dezarhiva fișierele compuse mari**. Limitarea timpului de executare a activității. După scurgerea duratei specificate, Kaspersky Endpoint Security oprește activitatea. Activitatea nu este marcată ca finalizată. Data viitoare când Kaspersky Endpoint Security execută activitatea, aceasta va fi executată de la început și conform planificării.

   Kaspersky Endpoint Security scanează fișierele de dimensiuni mari extrase din arhive indiferent dacă este bifată sau nu caseta de selectare **Nu dezarhiva fișierele compuse mari**.

6. În blocul **Tehnologii de scanare**, bifați casetele de selectare de lângă numele tehnologiilor care doriți să fie utilizate în timpul unei scanări:

   - **Tehnologia iSwift**. Această tehnologie permite creșterea vitezei de scanare excluzând de la scanare anumite fișiere. Fișierele sunt excluse de la scanări utilizând un algoritm special care ia în considerare data lansării bazelor de date Kaspersky Endpoint Security, data celei mai recente scanări a fișierului și orice modificare adusă setărilor scanării. Tehnologia iSwift reprezintă o versiune îmbunătățită a tehnologiei iChecker și este destinată sistemului de fișiere NTFS.

   - **Tehnologia iChecker**. Această tehnologie permite creșterea vitezei de scanare excluzând de la scanare anumite fișiere. Fișierele sunt excluse de la scanări utilizând un algoritm special care ia în considerare data lansării bazelor de date Kaspersky Endpoint Security, data celei mai recente scanări a fișierului și orice modificare adusă setărilor scanării. Există limitări ale tehnologiei iChecker: aceasta nu funcționează în cazul fișierelor mari și se aplică numai la fișierele cu o structură pe care aplicația o recunoaște (de exemplu, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP și RAR).

7. Salvați-vă modificările.

Dacă activitatea de scanare nu este afișată, înseamnă că administratorul a interzis utilizarea activităților locale în politică.

Actualizarea bazelor de date și modulelor aplicației

Actualizarea bazelor de date și modulelor aplicației Kaspersky Endpoint Security asigură o protecție actualizată pe computer. Zilnic apar în întreaga lume viruși și alte tipuri de programe malware noi. Bazele de date Kaspersky Endpoint Security conțin informații despre amenințări și despre modurile de neutralizare a acestora. Pentru a detecta rapid amenințările, este esențial să actualizezi în mod regulat bazele de date și modulele aplicației.

Este posibil ca funcționalitatea Actualizări (inclusiv furnizarea de actualizări ale semnăturii antivirus și actualizări ale bazei de cod) să nu fie disponibile în software în SUA.

Actualizările regulate necesită o licență activă. Dacă nu există nicio licență curentă, vei avea posibilitatea să efectuezi doar o singură actualizare.

Computerul trebuie să fie conectat la Internet pentru a descărca cu succes pachetul de actualizare de pe serverele de actualizare Kaspersky. În mod implicit, setările de conectare la Internet sunt stabilite automat. Dacă utilizați un server proxy, trebuie să configurați setările serverului proxy.

Actualizările se descarcă prin protocolul HTTPS. Acestea pot fi descărcate, de asemenea, prin protocolul HTTP atunci când este imposibilă descărcarea actualizărilor prin protocolul HTTPS.

La efectuarea unei actualizări, pe computer sunt descărcate și instalate următoarele obiecte:

- Baze de date Kaspersky Endpoint Security. Protecția computerului este furnizată folosind baze de date care conțin semnături de viruși și alte amenințări și informații despre modalitățile pentru neutralizarea acestora. Componentele protecției utilizează aceste informații la căutarea de fișiere infectate pe computer și la neutralizarea acestora. Bazele de date sunt actualizate constant cu înregistrări de amenințări noi și metode pentru contracararea lor. Prin urmare, îți recomandăm să actualizezi bazele de date regulat.

  Pe lângă bazele de date Kaspersky Endpoint Security, sunt actualizate și driverele de rețea care le permit componentelor aplicației să intercepteze traficul de rețea.

- Modulele aplicației. Pe lângă bazele de date Kaspersky Endpoint Security, poți actualiza și modulele aplicației. Actualizarea modulelor aplicației remediază vulnerabilitățile din Kaspersky Endpoint Security, adaugă funcții noi și îmbunătățește funcțiile existente.

În timpul actualizării, modulele și bazele de date ale aplicației de pe computer sunt comparate cu versiunile lor actualizate din sursa de actualizare. Dacă bazele de date și modulele actuale ale aplicației diferă de versiunile lor actualizate, porțiunea lipsă care să regăsește în actualizări este instalată pe computer.

Dacă bazele de date sunt neactuale, este posibil ca dimensiunea pachetului de actualizare să fie mare (până la câteva zeci de MB), fapt care poate cauza sporirea traficului din Internet.

Informațiile despre starea curentă a bazelor de date Kaspersky Endpoint Security sunt afișate în fereastra principală a aplicației sau în sfatul pe ecran pe care îl vedeți când deplasați cursorul peste pictograma aplicației din zona de notificare.

Informațiile despre rezultatele actualizărilor și despre toate evenimentele care apar în timpul funcționării activității de actualizare sunt înregistrate în Raportul Kaspersky Endpoint Security.

Dacă aplicația funcționează în modul Light Agent, consideratii speciale sunt implicate în actualizarea bazelor de date și a modulelor aplicațiilor.

Scenarii de actualizare a bazei de date și a modulului de aplicație

Actualizarea bazelor de date și modulelor aplicației Kaspersky Endpoint Security asigură o protecție actualizată pe computer. Zilnic apar în întreaga lume viruși și alte tipuri de programe malware noi. Bazele de date Kaspersky Endpoint Security conțin informații despre amenințări și despre modurile de neutralizare a acestora. Pentru a detecta rapid amenințările, este esențial să actualizezi în mod regulat bazele de date și modulele aplicației.

Următoarele obiecte sunt actualizate pe computerele utilizatorilor:

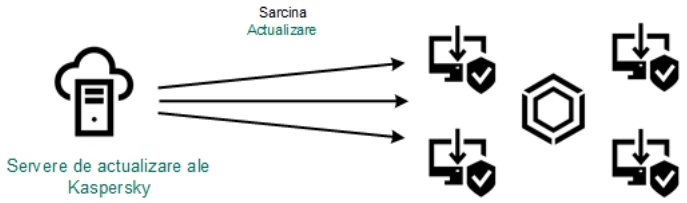
- Bazele de date antivirus. Bazele de date antivirus includ baze de date cu semnături de programe malware, descrieri ale atacurilor de rețea, baze de date de adrese Web rău intenționate și phishing, baze de date de bannere, baze de date de mesaje spam și alte date.

- Modulele aplicației. Actualizările pentru module sunt destinate eliminării vulnerabilităților din aplicație și îmbunătățirii metodelor de protecție pentru computere. Actualizările pentru module pot să schimbe comportarea componentelor aplicației și să adaugi capabilități noi.

Kaspersky Endpoint Security acceptă următoarele scenarii pentru actualizarea bazelor de date și a modulelor aplicației:

- Actualizare de pe servere Kaspersky.

  Serverele de actualizare Kaspersky sunt localizate în diverse țări din întreaga lume. Acest lucru asigură o fiabilitate ridicată a actualizărilor. Dacă o actualizare nu poate fi efectuată de la un singur server, Kaspersky Endpoint Security trece la următorul server.



Actualizare de pe serverele Kaspersky.

- Actualizare centralizată.

  Actualizarea centralizată reduce traficul Internet extern și asigură o monitorizare comodă a actualizării.

  Actualizarea centralizată constă în următorii pași:

  1. Descărcarea pachetului de actualizare într-un depozit din rețeaua organizației.

     Pachetul de actualizare este descărcat în depozit prin activitatea Serverului de administrare numită *Download updates to the Administration Server repository*.

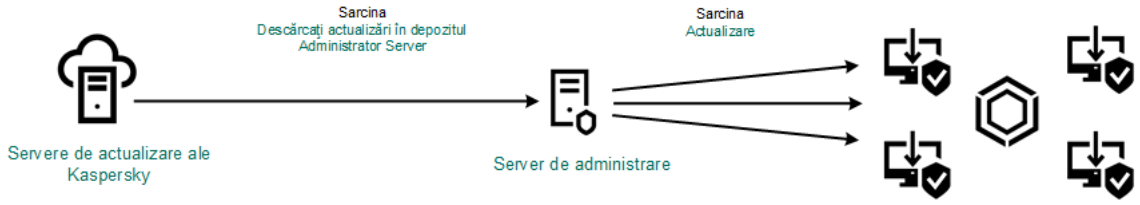
  2. Descărcați pachetul de actualizare într-un director partajat (opțional).

Puteți descărca pachetul de actualizare într-un director partajat folosind următoarele metode:

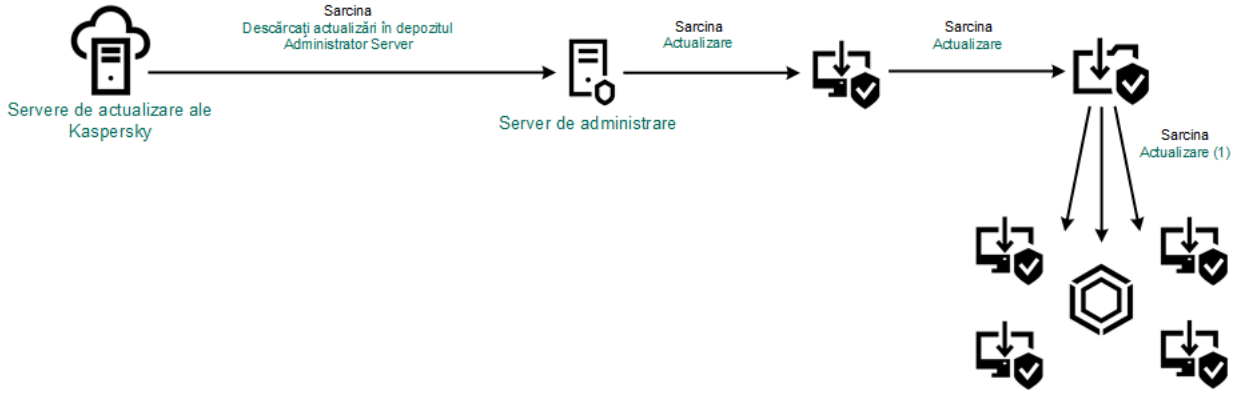
- Utilizând activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* din aplicația Kaspersky Endpoint Security. Activitatea este destinată unuia dintre computerele din rețeaua locală a companiei.
- Folosirea Utilitarului de actualizare Kaspersky. Pentru informații detaliate despre utilizarea Utilitarului de actualizare Kaspersky, consultați Baza de cunoștințe Kaspersky.

3. Distribuirea pachetului de actualizare către computere client.

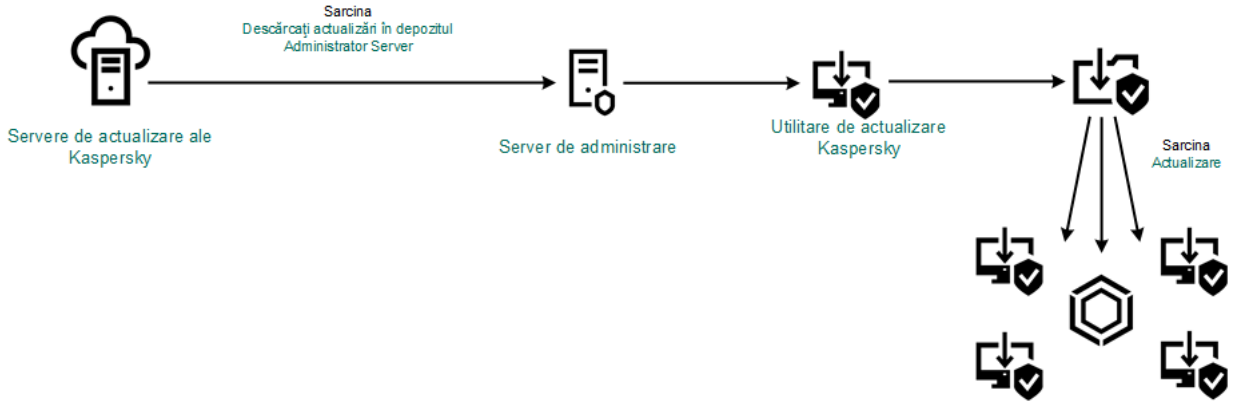
   Pachetul de actualizare este distribuit către computere client prin intermediul activității *Actualizarea modulelor bazelor de date și ale aplicațiilor* a aplicației Kaspersky Endpoint Security. Poți crea un număr nelimitat de activități de actualizare pentru fiecare grup de administrare.



Actualizarea din depozitul unui server



Actualizarea dintr-un director partajat



Actualizarea folosind Utilitarul de actualizare Kaspersky

Pentru Kaspersky Security Center, lista implicită cu sursele de actualizare conține Serverul de administrare Kaspersky Security Center și serverele de actualizare ale Kaspersky. Pentru Kaspersky Security Center Cloud Console, lista implicită de surse de actualizare conține puncte de distribuție și servere de actualizare ale Kaspersky. Pentru mai multe detalii despre punctele de distribuire, consultați Ajutorul pentru Kaspersky Security Center Cloud Console. Poți adăuga la listă alte surse de actualizare. Potț specifica drept surse de actualizare servere HTTP/FTP și directoare partajate. Dacă o actualizare nu poate fi efectuată de la o sursă de actualizare, Kaspersky Endpoint Security comută la următoarea sursă.

Actualizările se descarcă de pe servere de actualizare Kaspersky sau de pe alte servere FTP ori HTTP prin protocoale de rețea standard. Dacă este necesară conectarea la un server proxy pentru accesarea sursei de actualizare, specifică setările pentru serverul proxy în setările politicilor Kaspersky Endpoint Security.

Actualizarea din depozitul unui server

Pentru a conserva traficul pe Internet, poți configura actualizări ale bazelor de date și modulelor aplicației pe computere din rețeaua locală a organizației din depozitul unui server. În acest scop, Kaspersky Security Center trebuie să descarce un pachet de actualizare în depozit (server FTP sau HTTP, director de rețea sau local) de pe servere de actualizare ale Kaspersky. Alte computere din rețeaua locală a organizației vor putea primi pachetul de actualizare din depozitul serverului.

Configurarea actualizărilor pentru bazele de date și modulele aplicației din depozitul unui server constă din următorii pași:

1. Configurează descărcarea unui pachet de actualizare în depozitul Serverului de administrare (activitatea *Download updates to the Administration Server repository*).

   Activitatea *Download updates to the Administration Server repository* este creată automat de expertul de pornire rapidă a Serverului de administrare și această activitate poate avea numai o singură instanță. În mod implicit, Kaspersky Security Center copiază pachetul de actualizare în directorul `\\<server name>\KLSHARE\Updates`. Pentru mai multe informații despre descărcarea actualizărilor în depozitul Serverului de administrare, consultați Ajutor pentru Kaspersky Security Center.

2. Configurarea actualizărilor pentru bazele de date și modulele aplicației din depozitul serverului specificat pe celelalte computere din rețeaua locală a organizației (activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor*).

   Cum se configurează actualizarea Kaspersky Endpoint Security din spațiul de stocare specificat al serverului în Consola de administrare (MMC)

   1. Deschide Consolă de administrare a Kaspersky Security Center.

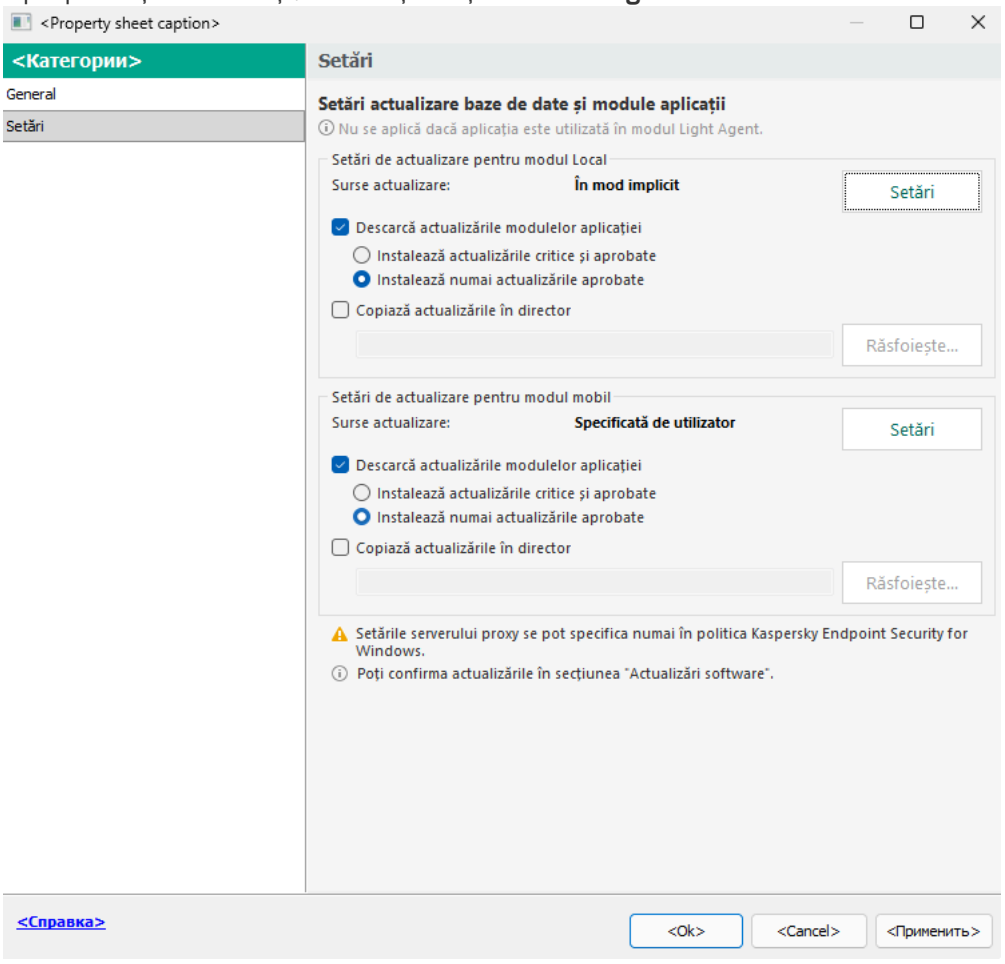
      În arborele consolei, selectați **Tasks**.

   2. Faceți clic pe activitatea **Actualizarea modulelor bazelor de date și ale aplicațiilor** a Kaspersky Endpoint Security.

      Se va deschide fereastra de proprietăți a activității.

      Activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* este creată automat de Expertul de pornire rapidă a Serverului de administrare. Pentru a crea activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor*, instalați plug-inul Kaspersky Endpoint Security for Windows Management în timp ce executați Expertul.

3. În fereastra cu proprietățile activității, selectați secțiunea **Settings**.



Setări activitate Actualizarea modulelor bazelor de date și ale aplicațiilor

4. În blocul **Setări de actualizare pentru modul Local**, fă clic pe butonul **Setări**.

5. În lista surselor de actualizare, asigurați-vă că actualizarea din sursa **Kaspersky Security Center** este activată. În plus, sursa **Kaspersky Security Center** trebuie să aibă cea mai mare prioritate.

6. Dacă este necesar, adăugați sursele de actualizare:

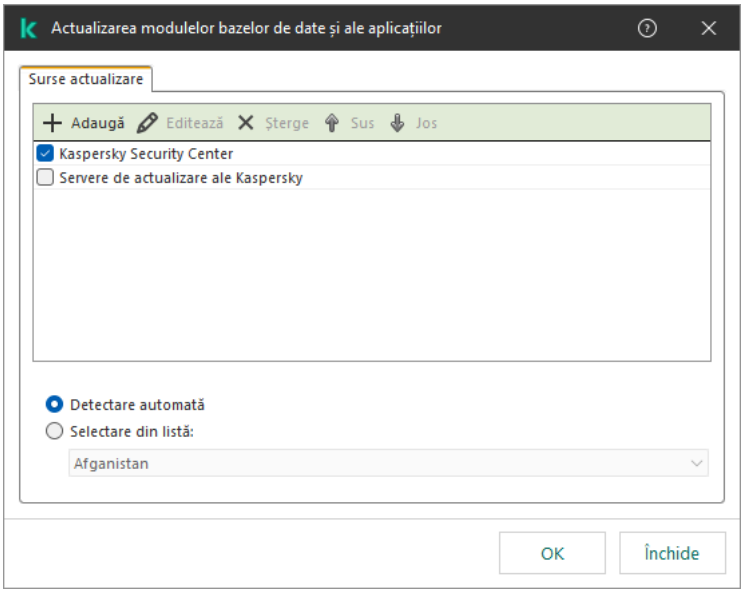
   a. În lista de surse de actualizări, faceți clic pe butonul **Adaugă**.

   b. În câmpul **Surse actualizare**, specifică adresa serverului FTP sau HTTP, directorul de rețea ori directorul local unde Kaspersky Security Center va copia pachetul de actualizare primit de la servere de actualizare Kaspersky.

   > Adresa sursei de actualizare trebuie să se potrivească cu adresa pe care ai specificat-o în câmpul **Folder for storing updates** atunci când ai configurat descărcarea actualizărilor în spațiul de stocare al serverului (activitatea *Download updates to the Administration Server repository*).

   c. Fă clic pe **OK**.

Puteți exclude sursa de actualizare fără a o elimina din lista de surse de actualizare. Pentru aceasta, debifați caseta de selectare de lângă obiect.



Surse de actualizare

7. Configurați prioritățile surselor de actualizări folosind butoanele **Sus** și **Jos**.

   Dacă o actualizare nu poate fi efectuată din prima sursă de actualizare, Kaspersky Endpoint Security comută automat la sursa următoare.

8. În fereastra cu proprietățile activității, selectați secțiunea **Schedule** și configurați modul de executare a activității.

9. În mod implicit, Kaspersky Endpoint Security execută activitatea în modul manual.

10. Salvați-vă modificările.

Cum se configurează actualizarea Kaspersky Endpoint Security din spațiul de stocare specificat al serverului în Web Console

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe activitatea **Update** a Kaspersky Endpoint Security.

   Se va deschide fereastra de proprietăți a activității.

   Activitatea *Update* este creată automat de Expertul de pornire rapidă a Serverului de administrare. Pentru a crea activitatea *Update*, instalați plug-inul Kaspersky Endpoint Security for Windows Management în timp ce executați Expertul.

3. Selectează fila **Application settings** → **Local mode**.

4. În lista surselor de actualizare, asigurați-vă că actualizarea din sursa **Kaspersky Security Center** este activată. În plus, sursa **Kaspersky Security Center** trebuie să aibă cea mai mare prioritate.

5. Dacă este necesar, adăugați sursele de actualizare:

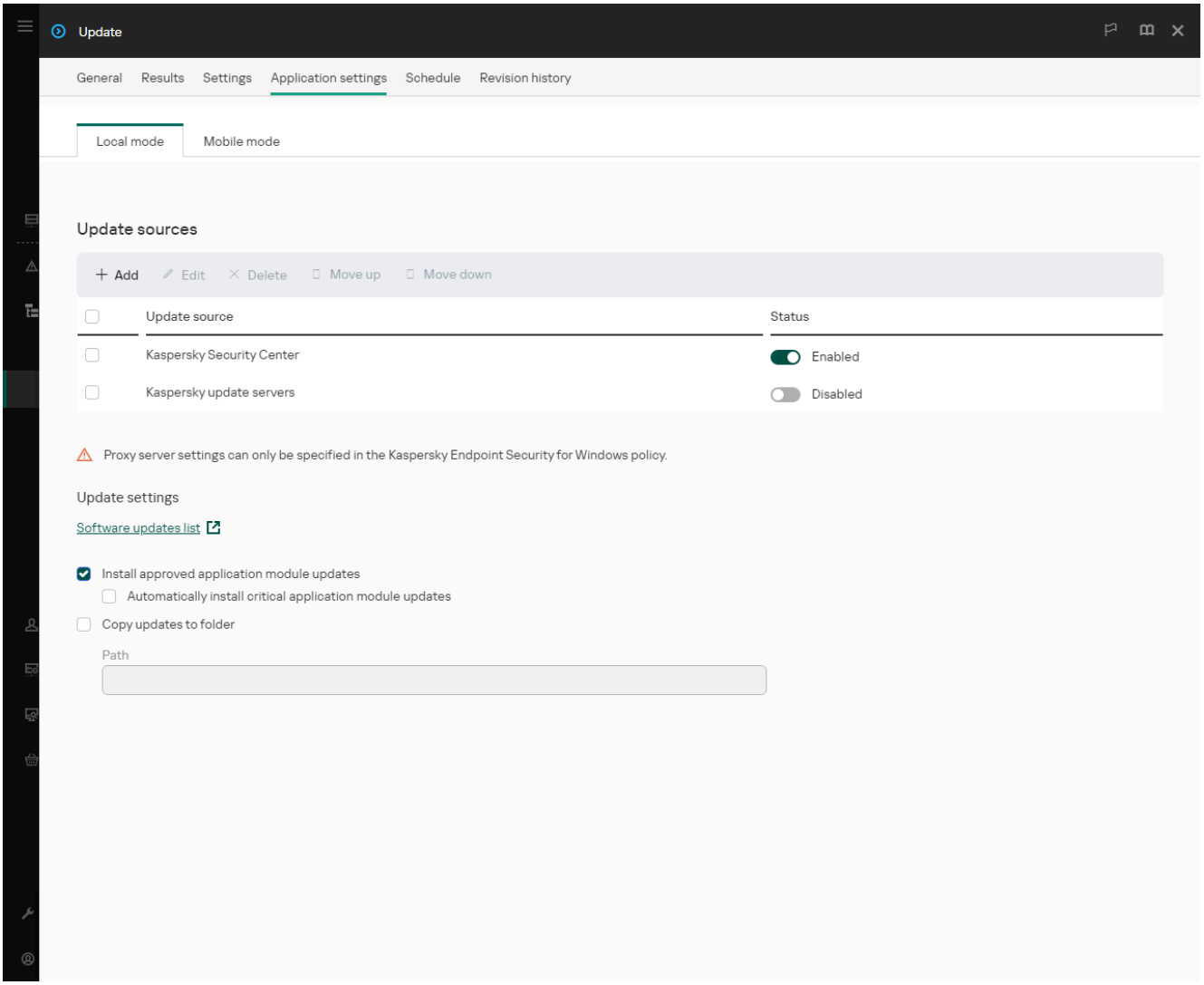
   a. În lista de surse de actualizări, faceți clic pe butonul **Add**.

   b. În câmpul **Update sources**, specifică adresa serverului FTP sau HTTP, directorul de rețea ori directorul local unde Kaspersky Security Center va copia pachetul de actualizare primit de la servere de actualizare Kaspersky.

      Adresa sursei de actualizare trebuie să se potrivească cu adresa pe care ai specificat-o în câmpul **Folder for storing updates** atunci când ai configurat descărcarea actualizărilor în spațiul de stocare al serverului (activitatea *Download updates to the Administration Server repository*).

   c. Fă clic pe **Save**.

Puteți exclude sursa de actualizare fără a o elimina din lista de surse de actualizare. Pentru aceasta, setați comutatorul de lângă acesta în poziția oprit.



Surse de actualizare

6. Configurați prioritățile surselor de actualizări folosind butoanele **Up** și **Down**.

   Dacă o actualizare nu poate fi efectuată din prima sursă de actualizare, Kaspersky Endpoint Security comută automat la sursa următoare.

7. În fereastra cu proprietățile activității, selectați secțiunea **Schedule** și configurați modul de executare a activității.

8. În mod implicit, Kaspersky Endpoint Security execută activitatea în modul manual.

9. Salvați-vă modificările.

Cum se configurează actualizarea Kaspersky Endpoint Security din spațiul de stocare specificat al serverului în interfața aplicației

Nu puteți configura activitatea de grup *Actualizarea modulelor bazelor de date și ale aplicațiilor* în interfața aplicației. Doar o activitate de actualizare locală, *Actualizarea modulelor bazelor de date și ale aplicațiilor*, este disponibilă pentru utilizator. Dacă activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* nu este afișată, înseamnă că administratorul a interzis utilizarea activităților locale în politică.

1. În fereastra principală a aplicației, accesați secțiunea **Actualizare**.



Activitate de actualizare locală

2. Se deschide lista de activități; selectați activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* și faceți clic pe ⚙.

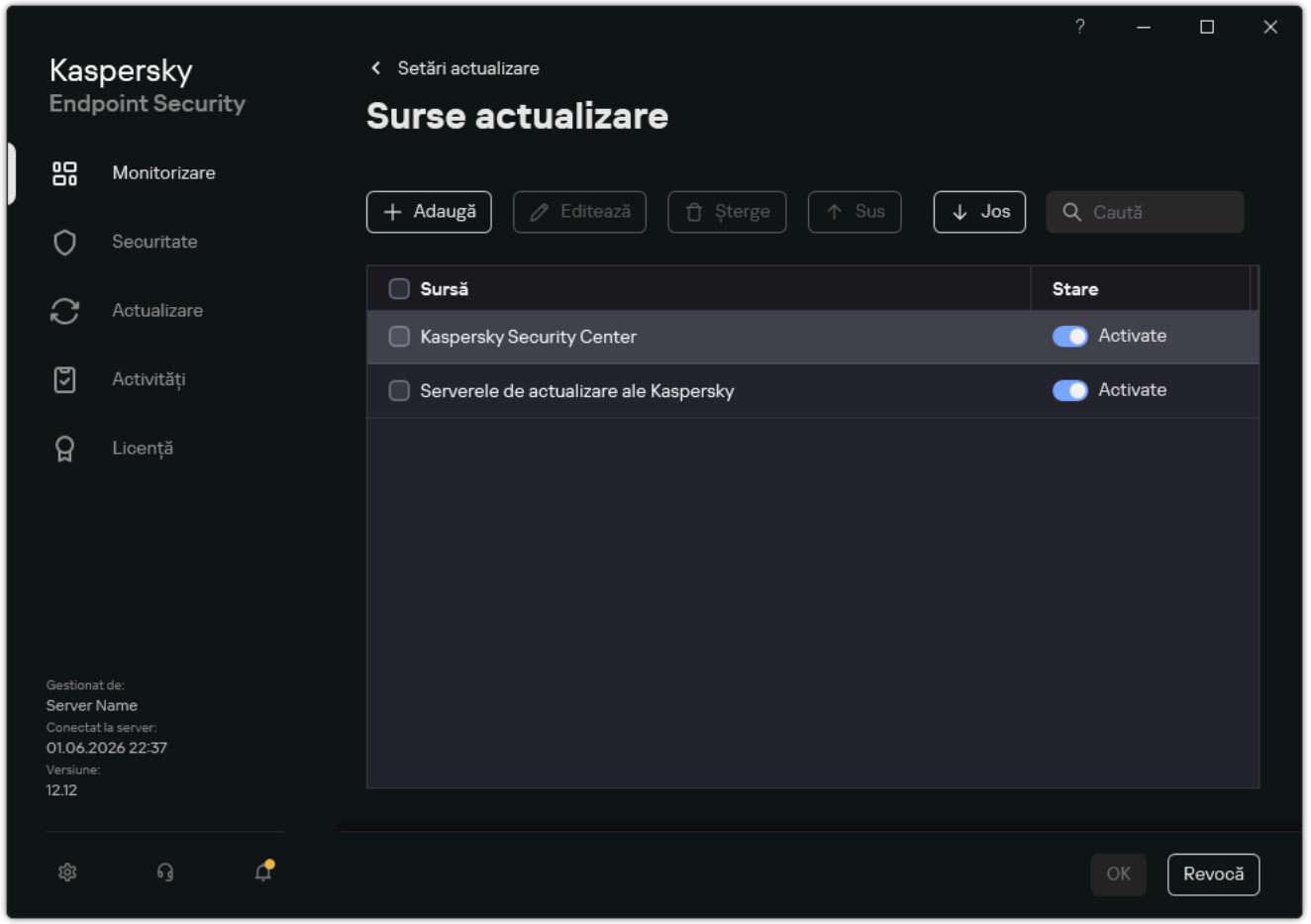
   Se va deschide fereastra de proprietăți a activității.

3. În fereastra cu proprietățile activității faceți clic pe **Selectează sursele de actualizare**.

4. În lista surselor de actualizare, asigurați-vă că actualizarea din sursa **Kaspersky Security Center** este activată. În plus, sursa **Kaspersky Security Center** trebuie să aibă cea mai mare prioritate.

5. Dacă este necesar, adăugați sursele de actualizare:

   a. În lista de surse de actualizări, faceți clic pe butonul **Adaugă**.



Surse de actualizare

   a. Specifică adresa serverului FTP- sau HTTP, directorul de rețea ori directorul local unde Kaspersky Security Center va copia pachetul de actualizare primit de la servere de actualizare Kaspersky.

      Adresa sursei de actualizare trebuie să se potrivească cu adresa pe care ai specificat-o în câmpul **Folder for storing updates** atunci când ai configurat descărcarea actualizărilor în spațiul de stocare al serverului (activitatea *Download updates to the Administration Server repository*).

   b. Fă clic pe **Selectează**.

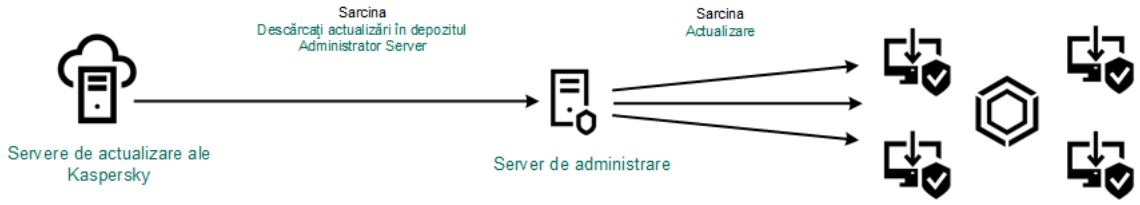
   Puteți exclude sursa de actualizare fără a o elimina din lista de surse de actualizare. Pentru aceasta, setați comutatorul de lângă acesta în poziția oprit.

6. Configurați prioritățile surselor de actualizări folosind butoanele **Sus** și **Jos**.

   Dacă o actualizare nu poate fi efectuată din prima sursă de actualizare, Kaspersky Endpoint Security comută automat la sursa următoare.

   Dacă un computer este gestionat de Kaspersky Security Center, nu este posibil să configurați modul de executare pentru activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor*. Puteți executa activitatea doar manual.

7. Salvați-vă modificările.



Actualizarea din depozitul unui server

Actualizarea dintr-un director partajat

Pentru a conserva traficul pe Internet, poți configura actualizări ale bazelor de date și modulelor aplicației pe computere din rețeaua locală a organizației dintr-un director partajat. În acest scop, unul dintre computerele din rețeaua locală a organizației trebuie să primească pachete de actualizare de la Serverul de administrare Kaspersky Security Center sau de la servere de actualizare Kaspersky și apoi să copieze pachetul de actualizare primit într-un director partajat. Alte computere din rețeaua locală a organizației vor putea primi pachetul de actualizare din acest director partajat.

Versiunea și localizarea aplicației Kaspersky Endpoint Security care copiază pachetul de actualizare într-un director partajat trebuie să se potrivească cu versiunea și localizarea aplicației care actualizează bazele de date din directorul partajat. Dacă versiunile sau localizările aplicațiilor nu se potrivesc, actualizarea bazei de date se poate termina cu o eroare.

Configurarea actualizărilor pentru bazele de date și modulele aplicației dintr-un director partajat constă din următorii pași:

1. Configurarea actualizărilor bazei de date și a modulului de aplicații din depozitul unui server.
2. Permiterea copierii unui pachet de actualizare într-un director partajat de pe unul dintre computerele din rețeaua locală.

   Cum se activează copierea pachetului de actualizare în directorul partajat în Consola de administrare (MMC)

   1. Deschide Consolă de administrare a Kaspersky Security Center.
   2. În arborele consolei, selectați **Tasks**.

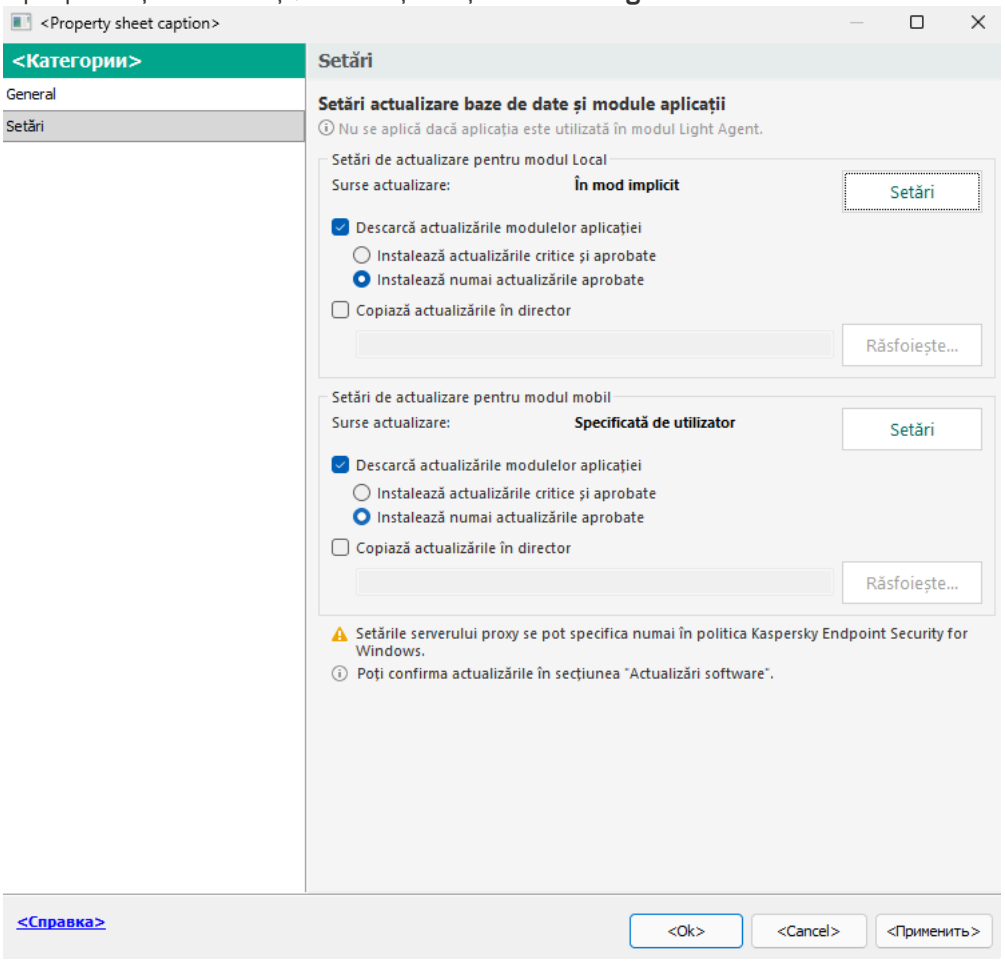
      Activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* trebuie atribuită unui computer care va servi drept sursă de actualizări.

   3. Faceți clic pe activitatea **Actualizarea modulelor bazelor de date și ale aplicațiilor** a Kaspersky Endpoint Security.

      Se va deschide fereastra de proprietăți a activității.

      Activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* este creată automat de Expertul de pornire rapidă a Serverului de administrare. Pentru a crea activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor*, instalați plug-inul Kaspersky Endpoint Security for Windows Management în timp ce executați Expertul.

4. În fereastra cu proprietățile activității, selectați secțiunea **Settings**.



Setări activitate Actualizarea modulelor bazelor de date și ale aplicațiilor

5. În blocul **Setări de actualizare pentru modul Local**, fă clic pe butonul **Setări**.

6. Configurarea surselor de actualizări.

   Sursele de actualizări pot fi servere de actualizare Kaspersky, Serverul de administrare Kaspersky Security Center, alte servere FTP sau HTTP, directoare locale sau directoare de rețea.

7. Bifați caseta de selectare **Copiază actualizările în director**.

8. În câmpul **Cale către director**, introduceți calea UNC către directorului partajat (de exemplu, `\\<server name>\KLSHARE\Updates`).

   În cazul în care câmpul este lăsat necompletat, Kaspersky Endpoint Security va copia pachetul de actualizare în directorul `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

9. Salvați-vă modificările.

Cum se activează copierea pachetului de actualizare în directorul partajat în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

> Activitatea *Update* trebuie atribuită unui computer care va servi drept sursă de actualizări.

2. Faceți clic pe activitatea **Update** a Kaspersky Endpoint Security.

   Se va deschide fereastra de proprietăți a activității.

   Activitatea *Update* este creată automat de Expertul de pornire rapidă a Serverului de administrare. Pentru a crea activitatea *Update*, instalați plug-inul Kaspersky Endpoint Security for Windows Management în timp ce executați Expertul.

3. Selectează fila **Application settings** → **Local mode**.

4. Configurarea surselor de actualizări.

   Sursele de actualizări pot fi servere de actualizare Kaspersky, Serverul de administrare Kaspersky Security Center, alte servere FTP sau HTTP, directoare locale sau directoare de rețea.

5. Bifați caseta de selectare **Copy updates to folder**.

6. În câmpul **Path**, introduceți calea UNC către directorului partajat (de exemplu, `\\<server name>\KLSHARE\Updates`).

   În cazul în care câmpul este lăsat necompletat, Kaspersky Endpoint Security va copia pachetul de actualizare în directorul `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

7. Salvați-vă modificările.

Cum se activează copierea pachetului de actualizare în directorul partajat în interfața aplicației

Nu puteți configura activitatea de grup *Actualizarea modulelor bazelor de date și ale aplicațiilor* în interfața aplicației. Doar o activitate de actualizare locală, *Actualizarea modulelor bazelor de date și ale aplicațiilor*, este disponibilă pentru utilizator. Dacă activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* nu este afișată, înseamnă că administratorul a interzis utilizarea activităților locale în politică.

1. În fereastra principală a aplicației, accesați secțiunea **Actualizare**.



Activitate de actualizare locală

2. Se deschide lista de activități; selectați activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* și faceți clic pe ⚙.

   Se va deschide fereastra de proprietăți a activității.

3. În blocul **Se distribuie actualizările**, bifați caseta de selectare **Copiază actualizările în director**.

4. Introduceți calea UNC către directorului partajat (de exemplu, `\\<server name>\KLSHARE\Updates`).

5. Salvați-vă modificările.

3. Configurarea actualizărilor pentru bazele de date și modulele aplicației din directorul partajat specificat pe celelalte computere din rețeaua locală a organizației.

Cum se configurează actualizările din directorul partajat în Consola de administrare (MMC)

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **Add**.

   Expertul de activitate pornește.

3. Configurați setările pentru activitate:

   a. În lista verticală **Application**, selectează **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. În lista verticală **Task type**, selectează **Actualizarea modulelor bazelor de date și ale aplicațiilor**.

4. În arborele Consolei de administrare Kaspersky Security Center, selectează **Tasks**.

   Lista activităților se deschide.

5. Fă clic pe **New task**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Selectarea tipului activității

Selectați **Kaspersky Endpoint Security for Windows (14.1)** → **Actualizarea modulelor bazelor de date și ale aplicațiilor**.

Pasul 2. Selectarea surselor de actualizare

Adăugați o nouă sursă de actualizare: un director partajat. Adresa sursei trebuie să se potrivească cu adresa specificată anterior de dvs. în câmpul **Cale către director**, atunci când ați configurat copierea pachetului de actualizare în directorul partajat. Configurați prioritățile surselor de actualizări folosind butoanele **Sus** și **Jos**.

Pasul 3. Selectarea dispozitivelor cărora le va fi atribuită activitatea

Selectați computerele pe care se va efectua activitatea. Sunt disponibile următoarele opțiuni:

- Atribuirea activității unui grup de administrare. În acest caz, activitatea este atribuită computerelor incluse într-un grup de administrare creat anterior.
- Selectare computere detectate în rețea de Serverul de administrare: *dispozitive neatribuite*. Dispozitivele specifice pot include dispozitive din grupuri de administrare, precum și dispozitive neatribuite.
- Specificarea manuală a adreselor computerelor sau importarea adreselor dintr-o listă. Poți specifica nume NetBIOS, adrese IP și subrețele IP ale dispozitivelor cărora dorești să le atribui activitatea.

Activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* trebuie atribuită computerelor din rețeaua locală a organizației, exceptând computerul care servește drept sursă de actualizări.

Pasul 4. Selectarea contului pentru executarea activității

Selectați un cont pentru a executa activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor*. În mod implicit, Kaspersky Endpoint Security începe activitatea cu drepturile unui cont de utilizator local.

Pasul 5. Configurarea unei planificări de pornire a activității

Configurați o planificare pentru începerea unei activități, de exemplu, manual sau după ce bazele de date antivirus sunt descărcate în depozit.

Pasul 6. Definirea numelui activității

Introduceți numele activității, de exemplu *Actualizare dintr-un director partajat*.

Pasul 7. Finalizarea creării activității

Ieșiți din Expert. Dacă este necesar, bifați caseta de selectare **Run the task after the wizard finishes**. Puteți monitoriza progresul activității în proprietățile activității. Ca rezultat, activitatea de actualizare va fi executată pe computerele utilizatorilor în conformitate cu planificarea specificată.

Cum se configurează actualizările din directorul partajat în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectează **Tasks**.
   Lista activităților se deschide.
2. Fă clic pe **Add**.
   Expertul de activitate pornește.
3. Configurați setările pentru activitate:
   a. În lista verticală **Application**, selectează **Kaspersky Endpoint Security for Windows 14.1.0**.
   b. În lista verticală **Task type**, selectează **Update**.
   c. În câmpul **Task name**, introduceți o descriere succintă, de exemplu *Actualizare dintr-un director partajat*.
   d. În blocul **Devices to which the task will be assigned**, selectați domeniul activității.

   > Activitatea *Update* trebuie atribuită computerelor din rețeaua locală a organizației, exceptând computerul care servește drept sursă de actualizări.

4. Selectează dispozitive în funcție de opțiunea selectată pentru domeniul activității și treci la pasul următor.

5. Ieșiți din Expert.

   Se va afișa o activitate nouă în tabelul cu activități.

6. Faceți clic pe activitatea *Update* nou creată.

   Se va deschide fereastra de proprietăți a activității.

7. Selectează fila **Application settings** → **Local mode**.

8. În blocul **Update sources**, fă clic pe butonul **Add**.

9. În fereastra care se deschide, introduceți calea către directorul partajat.

   > Adresa sursă trebuie să se potrivească cu adresa specificată anterior de dvs. în câmpul **Path**, atunci când ați configurat copierea pachetului de actualizare în directorul partajat (consultați instrucțiunile de mai sus).

10. Fă clic pe **OK**.

11. Configurați prioritățile surselor de actualizări folosind butoanele **Up** și **Down**.

12. Salvați-vă modificările.

Cum se configurează actualizările din directorul partajat în interfața aplicației

Nu puteți configura activitatea de grup *Actualizarea modulelor bazelor de date și ale aplicațiilor* în interfața aplicației. Doar o activitate de actualizare locală, *Actualizarea modulelor bazelor de date și ale aplicațiilor*, este disponibilă pentru utilizator. Dacă activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* nu este afișată, înseamnă că administratorul a interzis utilizarea activităților locale în politică.

1. În fereastra principală a aplicației, accesați secțiunea **Actualizare**.



Activitate de actualizare locală

2. Se deschide lista de activități; selectați activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* și faceți clic pe ⚙.

   Se va deschide fereastra de proprietăți a activității.

3. Fă clic pe **Selectează sursele de actualizare**.

4. În fereastra care se deschide, faceți clic pe butonul **Adaugă**.

5. În fereastra care se deschide, introduceți calea către directorul partajat.

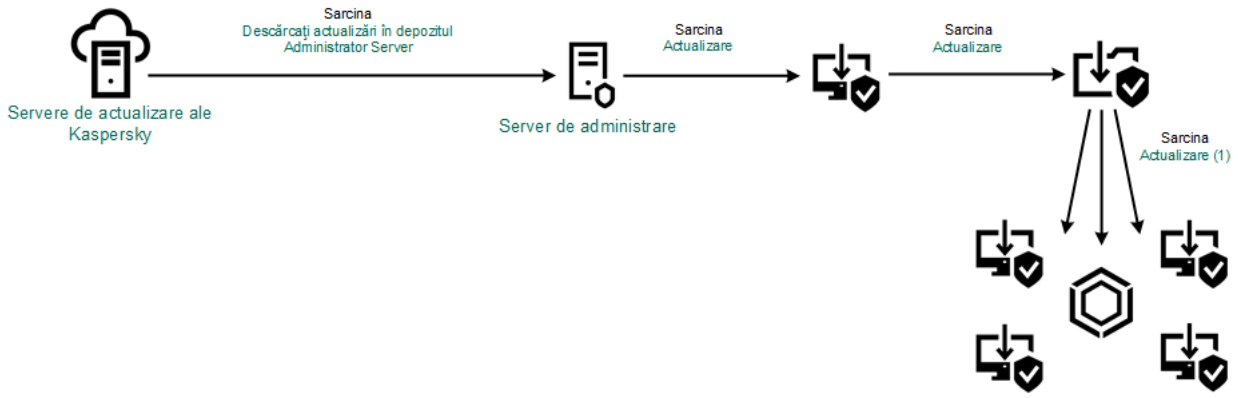
   Adresa sursă trebuie să se potrivească cu adresa specificată anterior de dvs., atunci când ați configurat copierea pachetului de actualizare în directorul partajat (consultați instrucțiunile de mai sus).

6. Fă clic pe **Selectează**.

7. Configurați prioritățile surselor de actualizări folosind butoanele **Sus** și **Jos**.

   Dacă o actualizare nu poate fi efectuată din prima sursă de actualizare, Kaspersky Endpoint Security comută automat la sursa următoare.

8. Salvați-vă modificările.



Actualizarea dintr-un director partajat

Actualizarea folosind Utilitarul de actualizare Kaspersky

Pentru a conserva traficul pe Internet, puteți configura actualizări ale bazelor de date și modulelor aplicației pe computere din rețeaua locală a organizației dintr-un director partajat utilizând Utilitarul de actualizare Kaspersky. În acest scop, unul dintre computerele din rețeaua locală a organizației trebuie să primească pachete de actualizare de la Serverul de administrare Kaspersky Security Center sau de la serverele de actualizare Kaspersky și apoi să copieze pachetul de actualizare primit în directorul partajat, utilizând utilitarul. Alte computere din rețeaua locală a organizației vor putea primi pachetul de actualizare din acest director partajat.

Versiunea și localizarea aplicației Kaspersky Endpoint Security care copiază pachetul de actualizare într-un director partajat trebuie să se potrivească cu versiunea și localizarea aplicației care actualizează bazele de date din directorul partajat. Dacă versiunile sau localizările aplicațiilor nu se potrivesc, actualizarea bazei de date se poate termina cu o eroare.

Configurarea actualizărilor pentru bazele de date și modulele aplicației dintr-un director partajat constă din următorii pași:

1. Configurarea actualizărilor bazei de date și a modulului de aplicații din depozitul unui server.
2. Instalați Utilitarul Kaspersky Update pe unul din computerele rețelei locale a organizației.
3. Configurați copierea pachetului de actualizare în directorul partajat din setările Utilitarului de actualizare Kaspersky.

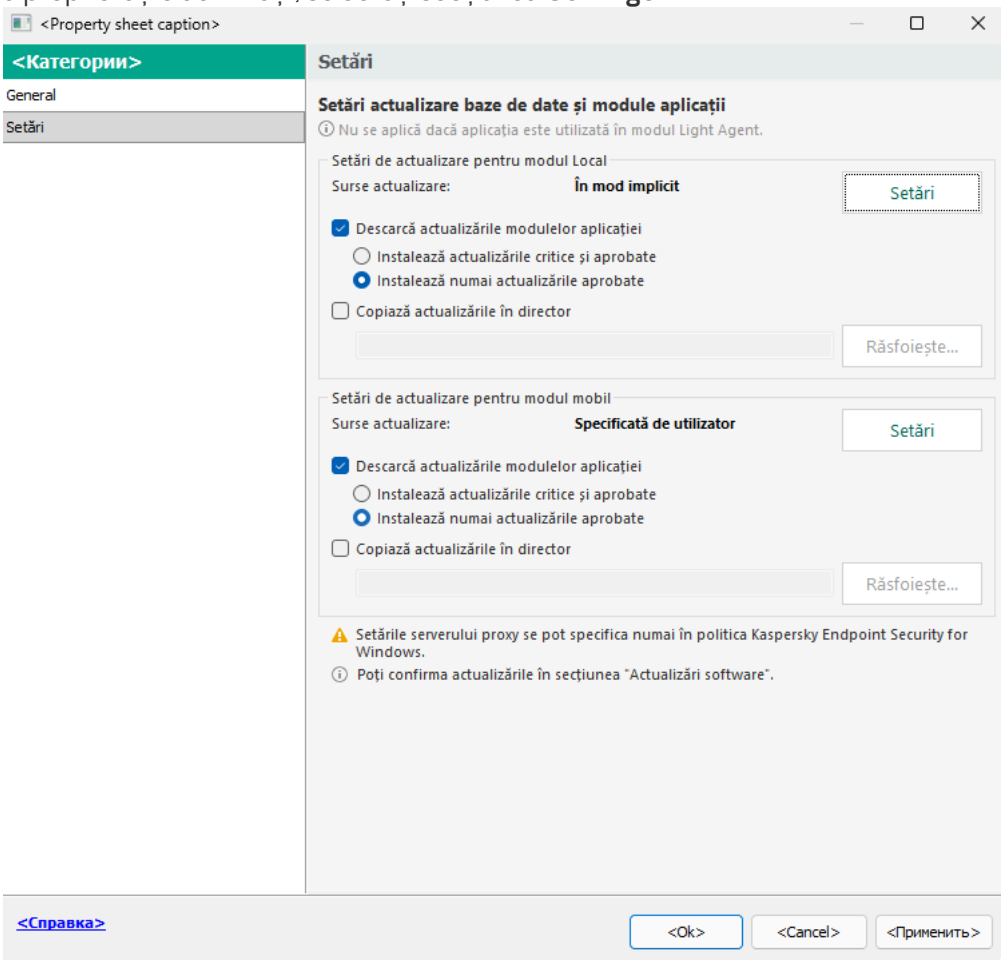
   Puteți descărca pachetul de distribuție pentru Utilitarul de actualizare Kaspersky de pe site-ul web al Serviciului de asistență tehnică Kaspersky. După instalarea utilitarului, selectați sursa de actualizare (de exemplu, depozitul Serverului de administrare) și directorul partajat în care Utilitarul de actualizare Kaspersky va copia pachetele de actualizare. Pentru informații detaliate despre utilizarea Utilitarului de actualizare Kaspersky, consultați Baza de cunoștințe Kaspersky.
4. Configurarea actualizărilor pentru bazele de date și modulele aplicației din directorul partajat specificat pe celelalte computere din rețeaua locală a organizației.

Cum se configurează actualizările din directorul partajat în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați **Tasks**.
3. Faceți clic pe activitatea **Actualizarea modulelor bazelor de date și ale aplicațiilor** a Kaspersky Endpoint Security.

   Se va deschide fereastra de proprietăți a activității.

   Activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* este creată automat de Expertul de pornire rapidă a Serverului de administrare. Pentru a crea activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor*, instalați plug-inul Kaspersky Endpoint Security for Windows Management în timp ce executați Expertul.
4. În fereastra cu proprietățile activității, selectați secțiunea **Settings**.



Setări activitate Actualizarea modulelor bazelor de date și ale aplicațiilor

5. În blocul **Setări de actualizare pentru modul Local**, fă clic pe butonul **Setări**.
6. În lista de surse de actualizări, faceți clic pe butonul **Adaugă**.
7. În fereastra care se deschide, introdu calea UNC către directorul partajat (de exemplu, `\\<server name>\KLSHARE\Updates`).

   Adresa sursă trebuie să se potrivească cu adresa indicată în setările Utilitarului de actualizare Kaspersky.
8. Fă clic pe **OK**.

9. Configurați prioritățile surselor de actualizări folosind butoanele **Sus** și **Jos**.

   Dacă o actualizare nu poate fi efectuată din prima sursă de actualizare, Kaspersky Endpoint Security comută automat la sursa următoare.

10. Salvați-vă modificările.

Cum se configurează actualizările din directorul partajat în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe activitatea **Update** a Kaspersky Endpoint Security.

   Se va deschide fereastra de proprietăți a activității.

   Activitatea *Update* este creată automat de Expertul de pornire rapidă a Serverului de administrare. Pentru a crea activitatea *Update*, instalați plug-inul Kaspersky Endpoint Security for Windows Management în timp ce executați Expertul.

3. Selectează fila **Application settings** → **Local mode**.

4. În lista de surse de actualizări, faceți clic pe butonul **Add**.

5. În fereastra care se deschide, introdu calea UNC către directorul partajat (de exemplu, `\\<server name>\KLSHARE\Updates`).

   > Adresa sursă trebuie să se potrivească cu adresa indicată în setările Utilitarului de actualizare Kaspersky.

6. Fă clic pe **OK**.

7. Configurați prioritățile surselor de actualizări folosind butoanele **Sus** și **Jos**.

   Dacă o actualizare nu poate fi efectuată din prima sursă de actualizare, Kaspersky Endpoint Security comută automat la sursa următoare.

8. Salvați-vă modificările.

Cum se configurează actualizările din directorul partajat în interfața aplicației

Nu puteți configura activitatea de grup *Actualizarea modulelor bazelor de date și ale aplicațiilor* în interfața aplicației. Doar o activitate de actualizare locală, *Actualizarea modulelor bazelor de date și ale aplicațiilor*, este disponibilă pentru utilizator. Dacă activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* nu este afișată, înseamnă că administratorul a interzis utilizarea activităților locale în politică.

1. În fereastra principală a aplicației, accesați secțiunea **Actualizare**.



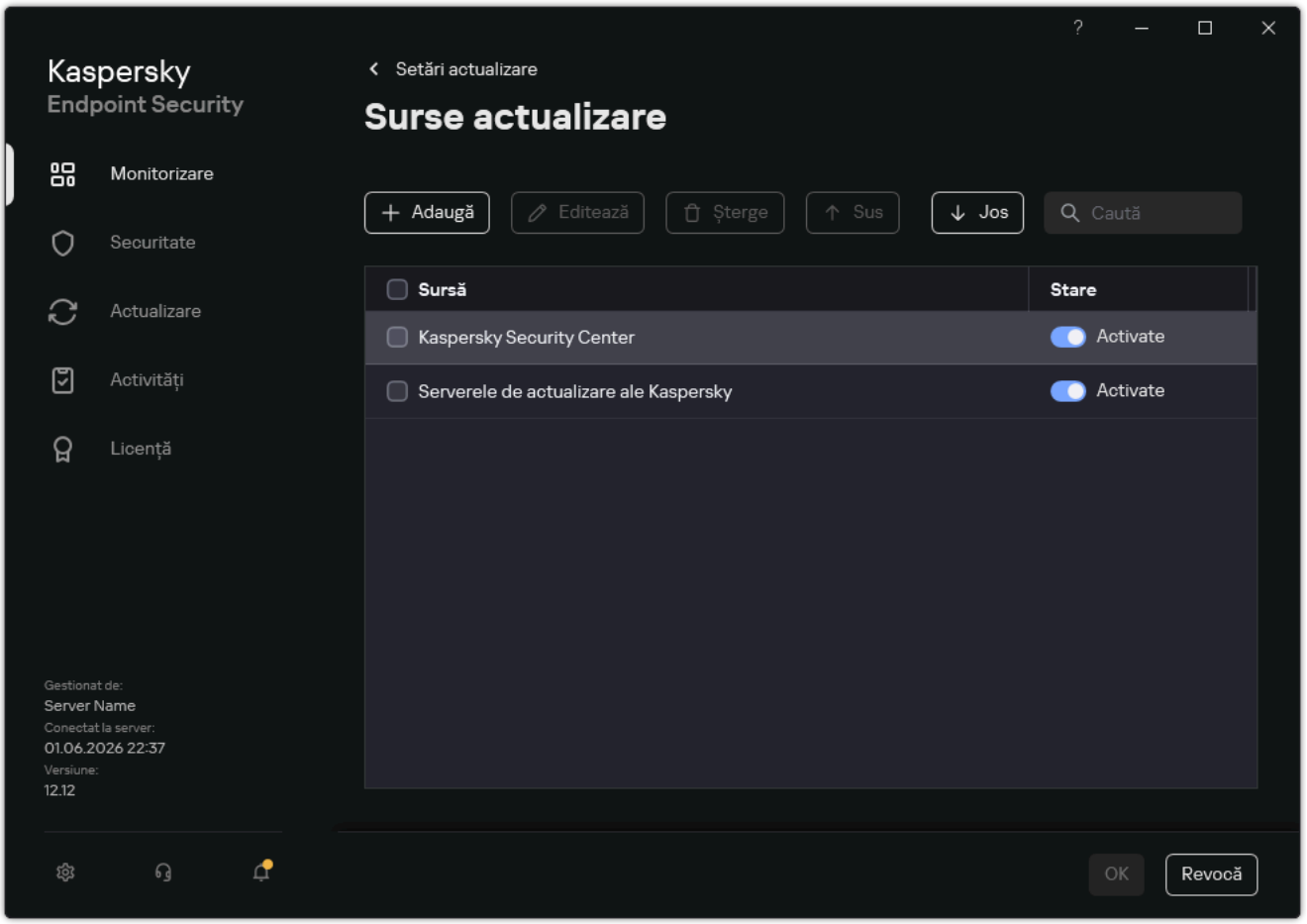
Activitate de actualizare locală

2. Se deschide lista de activități; selectați activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* și faceți clic pe ⚙.

   Se va deschide fereastra de proprietăți a activității.

3. În fereastra cu proprietățile activității faceți clic pe **Selectează sursele de actualizare**.

4. În lista de surse de actualizări, faceți clic pe butonul **Adaugă**.



Surse de actualizare

5. Introduceți calea UNC către directorului partajat (de exemplu, `\\<server name>\KLSHARE\Updates`).

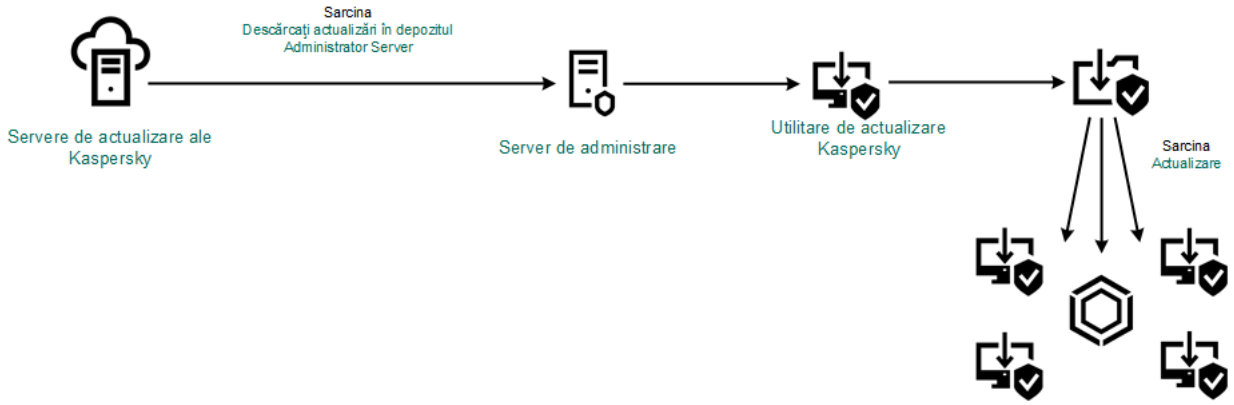
Adresa sursă trebuie să se potrivească cu adresa indicată în setările Utilitarului de actualizare Kaspersky.

6. Fă clic pe **Selectează**.

7. Configurați prioritățile surselor de actualizări folosind butoanele **Sus** și **Jos**.

   Dacă o actualizare nu poate fi efectuată din prima sursă de actualizare, Kaspersky Endpoint Security comută automat la sursa următoare.

8. Salvați-vă modificările.



Actualizarea folosind Utilitarul de actualizare Kaspersky

Actualizarea în modul Mobil

Modul Mobil este modul de operare al aplicației Kaspersky Endpoint Security atunci când un computer părăsește perimetrul rețelei organizației (*computer offline*). Pentru mai multe detalii despre lucrul cu computere offline și utilizatori absenți de la birou, consultați Ajutor pentru Kaspersky Security Center.

Un computer offline aflat în afara rețelei organizației nu se poate conecta la Serverul de administrare pentru a actualiza bazele de date și modulele de aplicații. În mod implicit, în modul Mobil, numai serverele de actualizare Kaspersky sunt utilizate ca sursă de actualizare pentru actualizarea bazelor de date și a modulelor aplicației. Utilizarea unui server proxy pentru conectarea la Internet este determinată de o politică Absent de la birou specială. Politica Absent de la birou trebuie creată separat. Atunci când aplicația Kaspersky Endpoint Security este comutată la modul Mobil, activitatea de actualizare este pornită la fiecare două ore.

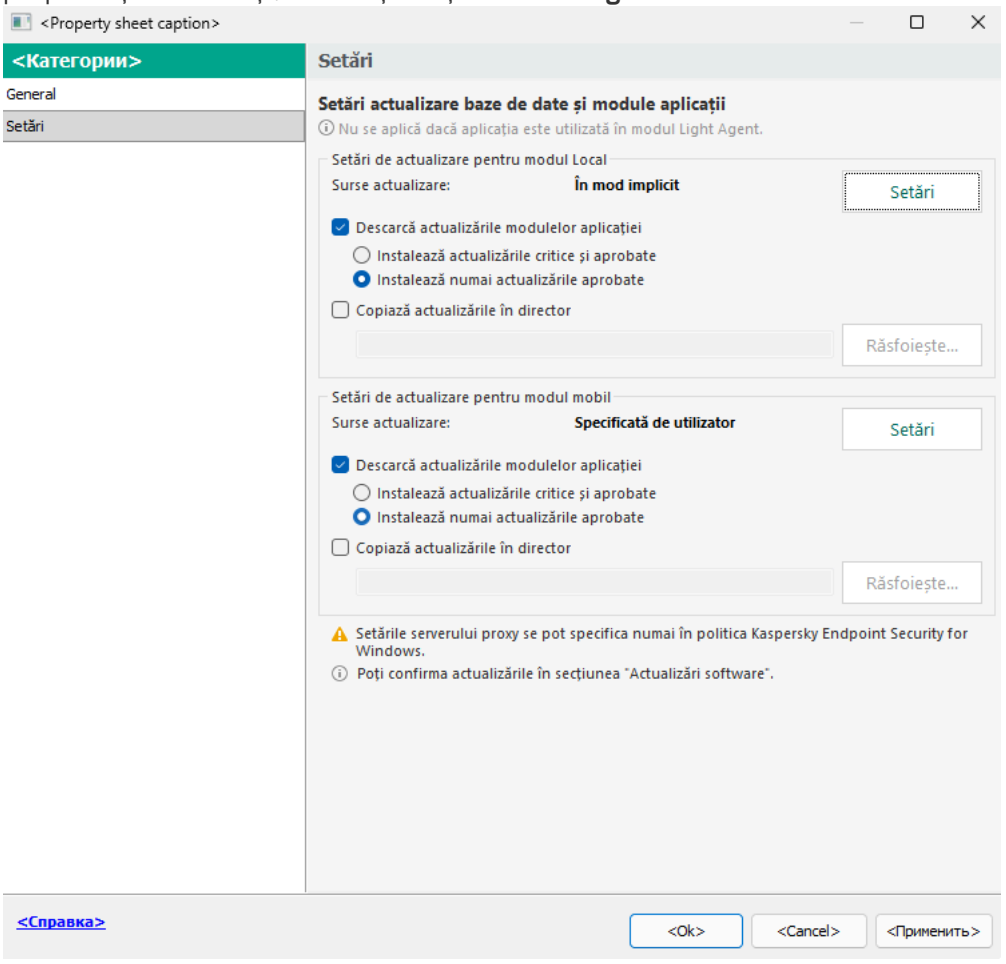
Cum se configurează setările de actualizare pentru modul mobil în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați **Tasks**.
3. Faceți clic pe activitatea **Actualizarea modulelor bazelor de date și ale aplicațiilor** a Kaspersky Endpoint Security.

   Se va deschide fereastra de proprietăți a activității.

   Activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* este creată automat de Expertul de pornire rapidă a Serverului de administrare. Pentru a crea activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor*, instalați plug-inul Kaspersky Endpoint Security for Windows Management în timp ce executați Expertul.

4. În fereastra cu proprietățile activității, selectați secțiunea **Settings**.



Setări activitate Actualizarea modulelor bazelor de date și ale aplicațiilor

5. În blocul **Setări de actualizare pentru modul mobil**, fă clic pe butonul **Setări**.

6. Configurarea surselor de actualizări. Sursele de actualizări pot fi servere de actualizare Kaspersky, alte servere FTP și HTTP, directoare locale sau directoare de rețea.

7. Salvați-vă modificările.

Cum se configurează setările de actualizare pentru modul mobil în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe activitatea **Update** a Kaspersky Endpoint Security.

   Se va deschide fereastra de proprietăți a activității.

   Activitatea *Update* este creată automat de Expertul de pornire rapidă a Serverului de administrare. Pentru a crea activitatea *Update*, instalați plug-inul Kaspersky Endpoint Security for Windows Management în timp ce executați Expertul.

3. Selectează fila **Application settings** → **Mobile mode**.

4. Configurarea surselor de actualizări. Sursele de actualizări pot fi servere de actualizare Kaspersky, alte servere FTP și HTTP, directoare locale sau directoare de rețea.

5. Salvați-vă modificările.

Ca rezultat, bazele de date și modulele aplicației vor fi actualizate pe computerele utilizatorilor atunci când aceștia comută la modul Mobil.

Pornirea și oprirea unei activități de actualizare

Indiferent de modul de executare a activității de actualizare pe care îl selectezi, poți porni sau opri oricând o activitate de actualizare a aplicației Kaspersky Endpoint Security.

Pentru a porni sau a opri o activitate de actualizare:

1. În fereastra principală a aplicației, accesați secțiunea **Actualizare**.
2. În dala **Actualizarea modulelor bazelor de date și ale aplicațiilor**, faceți clic pe butonul **Actualizează** dacă doriți să începeți activitatea de actualizare.

   Kaspersky Endpoint Security va începe să actualizeze modulele aplicației și bazele de date. Aplicația va afișa progresul activității, dimensiunea fișierelor descărcate și sursa de actualizare. Puteți opri activitatea în orice moment făcând clic pe butonul **Oprire actualizare**.

Pentru a începe sau a opri activitatea actualizare atunci când este afișată interfața aplicației simplificată:

1. Faceți clic dreapta pe pictograma aplicației din zona de notificare a barei de activități pentru a se afișa meniul contextual.
2. În lista verticală **Activități**, în meniul contextual, procedează într-unul din modurile următoare:
   - selectați o activitate de actualizare care nu se execută pentru a o porni
   - selectați o activitate de actualizare care se execută pentru a o opri
   - selectați o activitate de actualizare în pauză pentru a o relua sau a o porni

Pornirea unei activități de actualizare utilizând drepturile altui cont de utilizator

În mod implicit, activitatea de actualizare a aplicației Kaspersky Endpoint Security este pornită din partea utilizatorului al cărui cont l-ai utilizat pentru a face Log in la sistemul de operare. Totuși, aplicația Kaspersky Endpoint Security poate fi actualizată și dintr-o sursă de actualizare la care utilizatorul nu are acces din cauza lipsei drepturilor necesare (de exemplu, dintr-un director partajat care conține un pachet de actualizare) sau dintr-o sursă de actualizare pentru care autentificarea serverului proxy nu este configurată. În setările aplicației, poți specifica un utilizator care are astfel de drepturi și poți porni activitatea de actualizare a aplicației Kaspersky Endpoint Security din contul utilizatorului respectiv.

Pentru a porni o activitate de actualizare din alt cont de utilizator:

Nu puteți configura activitatea de grup *Actualizarea modulelor bazelor de date și ale aplicațiilor* în interfața aplicației. Doar o activitate de actualizare locală, *Actualizarea modulelor bazelor de date și ale aplicațiilor*, este disponibilă pentru utilizator. Dacă activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* nu este afișată, înseamnă că administratorul a interzis utilizarea activităților locale în politică.

1. În fereastra principală a aplicației, accesați secțiunea **Actualizare**.



Activitate de actualizare locală

2. Se deschide lista de activități; selectați activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* și faceți clic pe ⚙.

   Se va deschide fereastra de proprietăți a activității.

3. Fă clic pe **Execută actualizările bazei de date cu drepturi de utilizator**.

4. În fereastra care se deschide, selectați **Alt utilizator**.

5. Introduceți acreditările de cont ale unui utilizator cu permisiunile necesare pentru a accesa sursa de actualizare.

6. Salvați-vă modificările.

Selectarea modului de executare a activității de actualizare

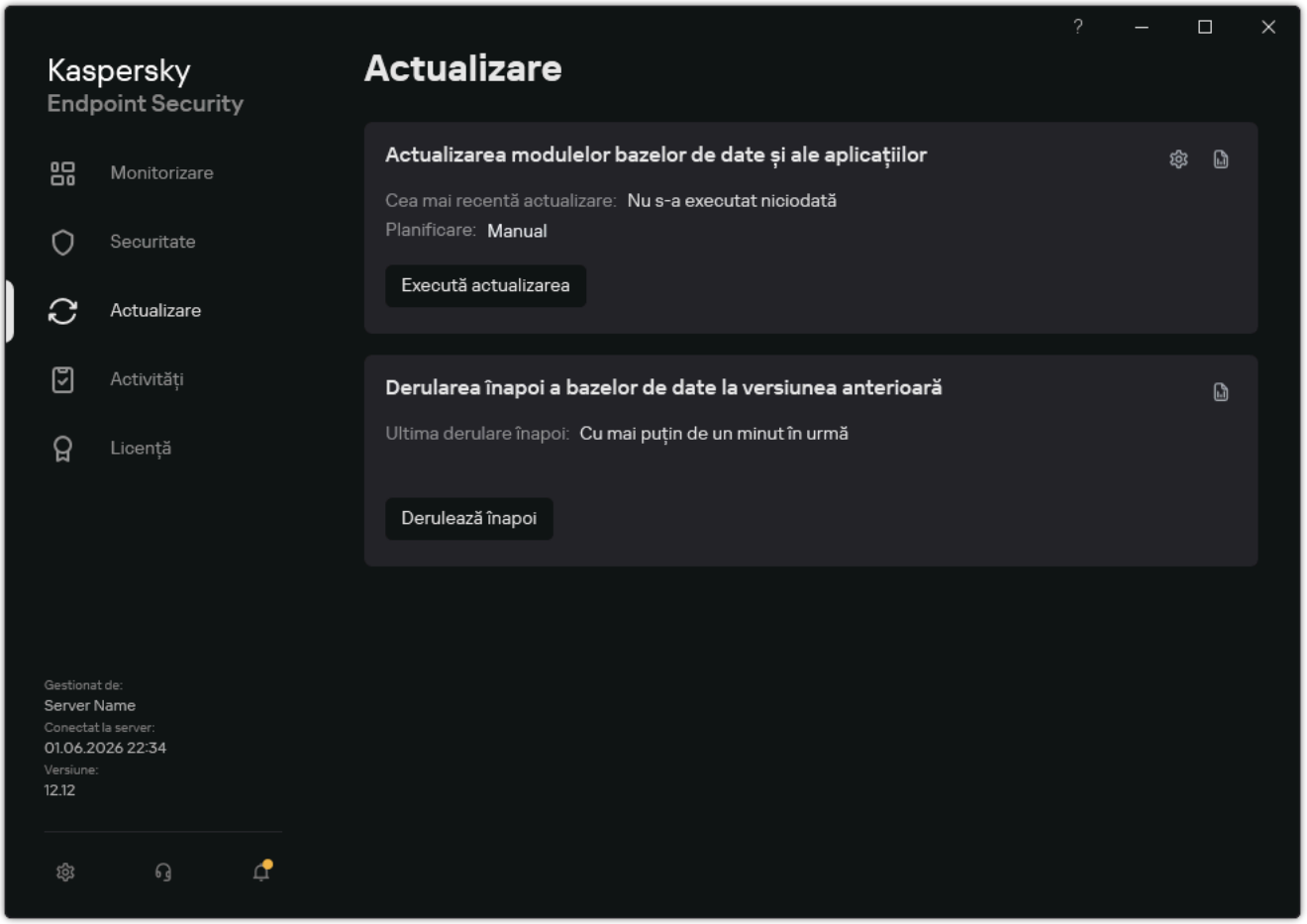
Dacă nu se poate executa acțiunea de actualizare dintr-un anumit motiv (de exemplu, computerul nu este pornit la momentul respectiv), poți configura activitatea omisă pentru pornire automată atunci când este posibil.

Poți amâna lansarea activității de actualizare după pornirea aplicației, dacă selectezi modul de executare **Conform planificării** pentru activitatea de actualizare și dacă ora de pornire a Kaspersky Endpoint Security corespunde planificării pornirii activității de actualizare. Activitatea de actualizare se poate executa numai după scurgerea intervalului de timp specificat de la pornirea aplicației Kaspersky Endpoint Security.

Pentru a selecta modul de executare a activității de actualizare:

Nu puteți configura activitatea de grup *Actualizarea modulelor bazelor de date și ale aplicațiilor* în interfața aplicației. Doar o activitate de actualizare locală, *Actualizarea modulelor bazelor de date și ale aplicațiilor*, este disponibilă pentru utilizator. Dacă activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* nu este afișată, înseamnă că administratorul a interzis utilizarea activităților locale în politică.

1. În fereastra principală a aplicației, accesați secțiunea **Actualizare**.



Activitate de actualizare locală

2. Se deschide lista de activități; selectați activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* și faceți clic pe ⚙.

   Se va deschide fereastra de proprietăți a activității.

3. Fă clic pe **Mod executare**.

4. În fereastra care se deschide, selectați modul de executare a activității de actualizare:

   - Dacă dorești ca aplicația Kaspersky Endpoint Security să execute activitatea de actualizare în funcție de disponibilitatea pachetului de actualizare în sursa de actualizare, selectați **Automat**. Frecvența cu care aplicația Kaspersky Endpoint Security verifică existența pachetelor de actualizare crește în timpul epidemiilor de viruși și scade în absența acestora.

   - Dacă dorești să pornești manual o activitate de actualizare, selectați **Manual**.

   - Dacă doriți să configurați o planificare pentru executarea activității de actualizare, selectați alte opțiuni. Configurați setările avansate pentru a începe activitatea de actualizare:

     - În câmpul **Amână executarea după pornirea aplicației timp de N minute**, introduceți intervalul de timp cu care doriți să amânați începutul activității de actualizare după pornirea Kaspersky Endpoint Security.

     - Selectați **Execută scanarea planificată în ziua următoare dacă computerul este închis** dacă doriți ca Kaspersky Endpoint Security să execute sarcini de actualizare ratate cu prima ocazie. Când aplicația are ocazia să execute activitățile omise, aceasta le execută aleatoriu într-un anumit interval de timp pentru a distribui încărcarea pe computer.

5. Salvați-vă modificările.

Adăugarea unei surse de actualizare

O *sursă de actualizare* este o resursă care conține actualizări pentru bazele de date și modulele aplicației Kaspersky Endpoint Security.

Sursele de actualizare includ serverul Kaspersky Security Center, serverele de actualizare ale Kaspersky și directoare de rețea sau locale.

În cazul în care serverele de actualizare Kaspersky nu sunt disponibile, Kaspersky Endpoint Security poate utiliza domenii alternative pentru a-și actualiza bazele de date și modulele software ale aplicației. Pentru informații detaliate, consultați Baza de cunoștințe pentru suport tehnic.

Lista implicită de surse de actualizare include Kaspersky Security Center și servere de actualizare ale Kaspersky. Poți adăuga la listă alte surse de actualizare. Potț specifica drept surse de actualizare servere HTTP/FTP și directoare partajate.

Kaspersky Endpoint Security nu acceptă actualizări de la servere HTTPS decât dacă sunt servere de actualizare ale Kaspersky.

Dacă mai multe resurse sunt selectate drept surse de actualizare, Kaspersky Endpoint Security încearcă să se conecteze la ele pe rând, începând cu prima din listă și efectuează acțiunea de actualizare preluând pachetul de actualizare de la prima sursă disponibilă.

În mod implicit, Kaspersky Endpoint Security utilizează serverul Kaspersky Security Center ca primă sursă de actualizare. Acest lucru ajută la conservarea traficului]n timpul actualizării. Dacă o politică nu este aplicată computerului, serverele Kaspersky sunt selectate ca primă sursă de actualizare în setările activității locale *Actualizarea modulelor bazelor de date și ale aplicațiilor*, deoarece este posibil ca aplicația să nu aibă acces la serverul Kaspersky Security Center.

Dacă aplicația se execută în modul Light Agent, un director pe SVM este selectat ca sursă de actualizare.

Cum se adăugă o sursă de actualizare în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.

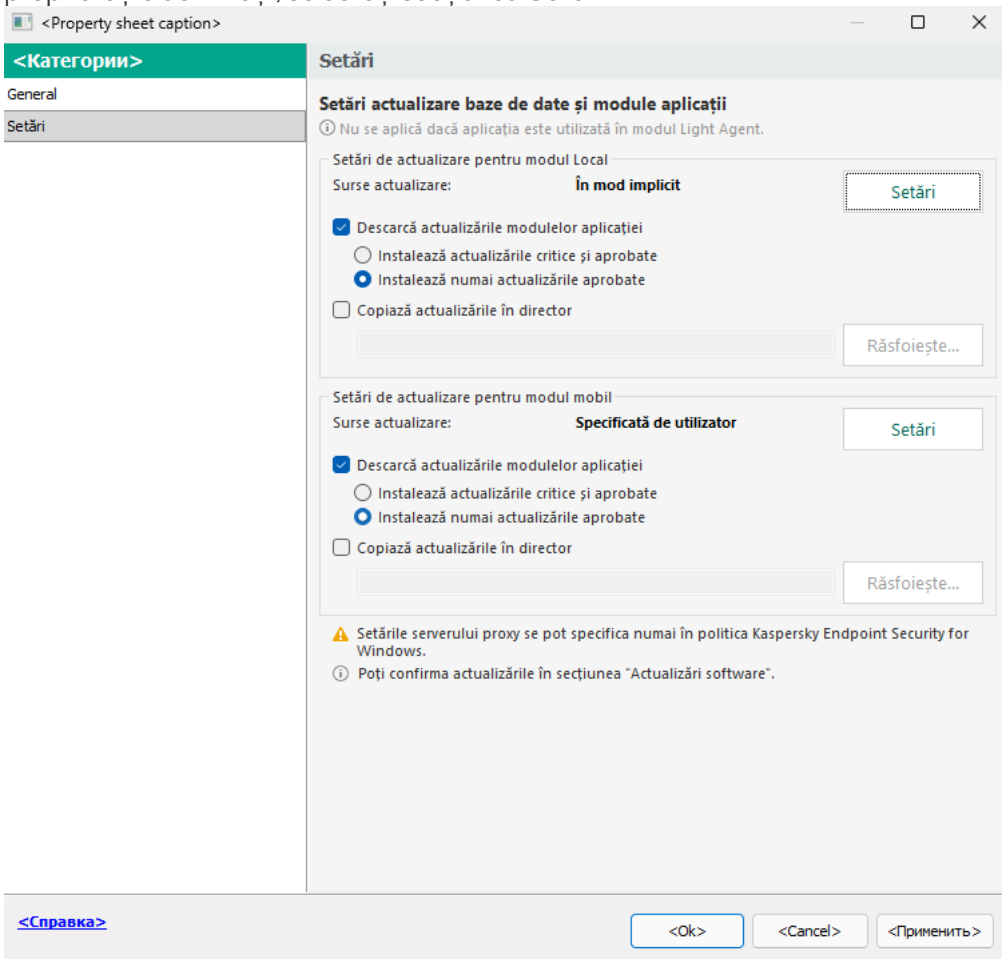
   În arborele consolei, selectați **Tasks**.

2. Faceți clic pe activitatea **Actualizarea modulelor bazelor de date și ale aplicațiilor** a Kaspersky Endpoint Security.

   Se va deschide fereastra de proprietăți a activității.

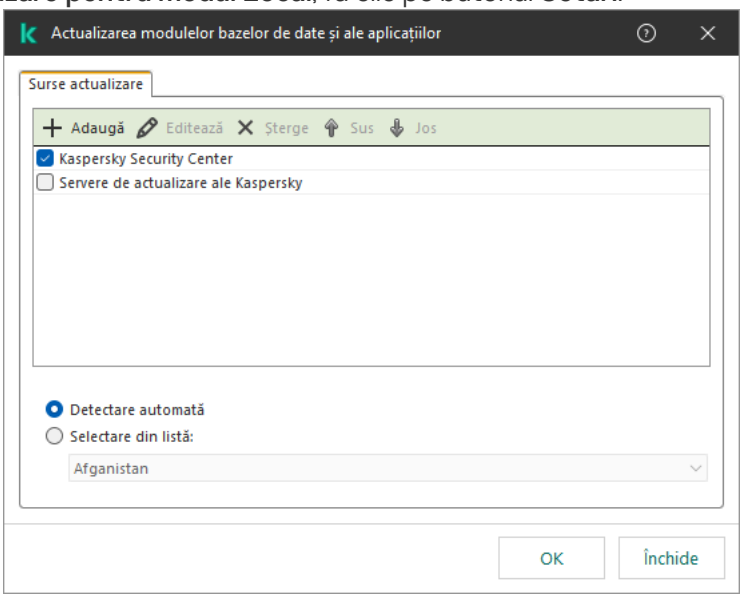
   Activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* este creată automat de Expertul de pornire rapidă a Serverului de administrare. Pentru a crea activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor*, instalați plug-inul Kaspersky Endpoint Security for Windows Management în timp ce executați Expertul.

3. În fereastra cu proprietățile activității, selectați secțiunea **Setări**.



Setări activitate Actualizarea modulelor bazelor de date și ale aplicațiilor

4. În blocul **Setări de actualizare pentru modul Local**, fă clic pe butonul **Setări**.



Surse de actualizare

5. În lista de surse de actualizări, faceți clic pe butonul **Adaugă**.

6. În câmpul **Surse actualizare**, specificați adresa serverului FTP sau HTTP, directorul de rețea sau directorul local care conține pachetul de actualizare.

   Pentru sursa de actualizare se utilizează următorul format de cale:

   - Pentru un server FTP sau HTTP, introdu adresa sa Web sau IP.

     De exemplu, `http://dnl-01.geo.kaspersky.com/` sau `93.191.13.103`.

     Pentru un server FTP, puteți specifica setările de autentificare în adresă în următorul format: `ftp://<user name>:<password>@<node>:<port>`.

   - Pentru un director de rețea, introduceți calea UNC.

     De exemplu, `\\Server\Share\Update distribution`.

   - Pentru un director local, introdu calea completă către acel director.

     De exemplu, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

   Puteți exclude sursa de actualizare fără a o elimina din lista de surse de actualizare. Pentru aceasta, debifați caseta de selectare de lângă obiect.

7. Fă clic pe **OK**.

8. Configurați prioritățile surselor de actualizări folosind butoanele **Sus** și **Jos**.

   Dacă o actualizare nu poate fi efectuată din prima sursă de actualizare, Kaspersky Endpoint Security comută automat la sursa următoare.

9. Daca este necesar, adăugați o sursă de actualizare pentru modul mobil. *Modul Mobil* este modul de operare al aplicației Kaspersky Endpoint Security atunci când un computer părăsește perimetrul rețelei organizației (*computer offline*).

10. Salvați-vă modificările.

Cum se adaugă o sursă de actualizare în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectează **Tasks**.

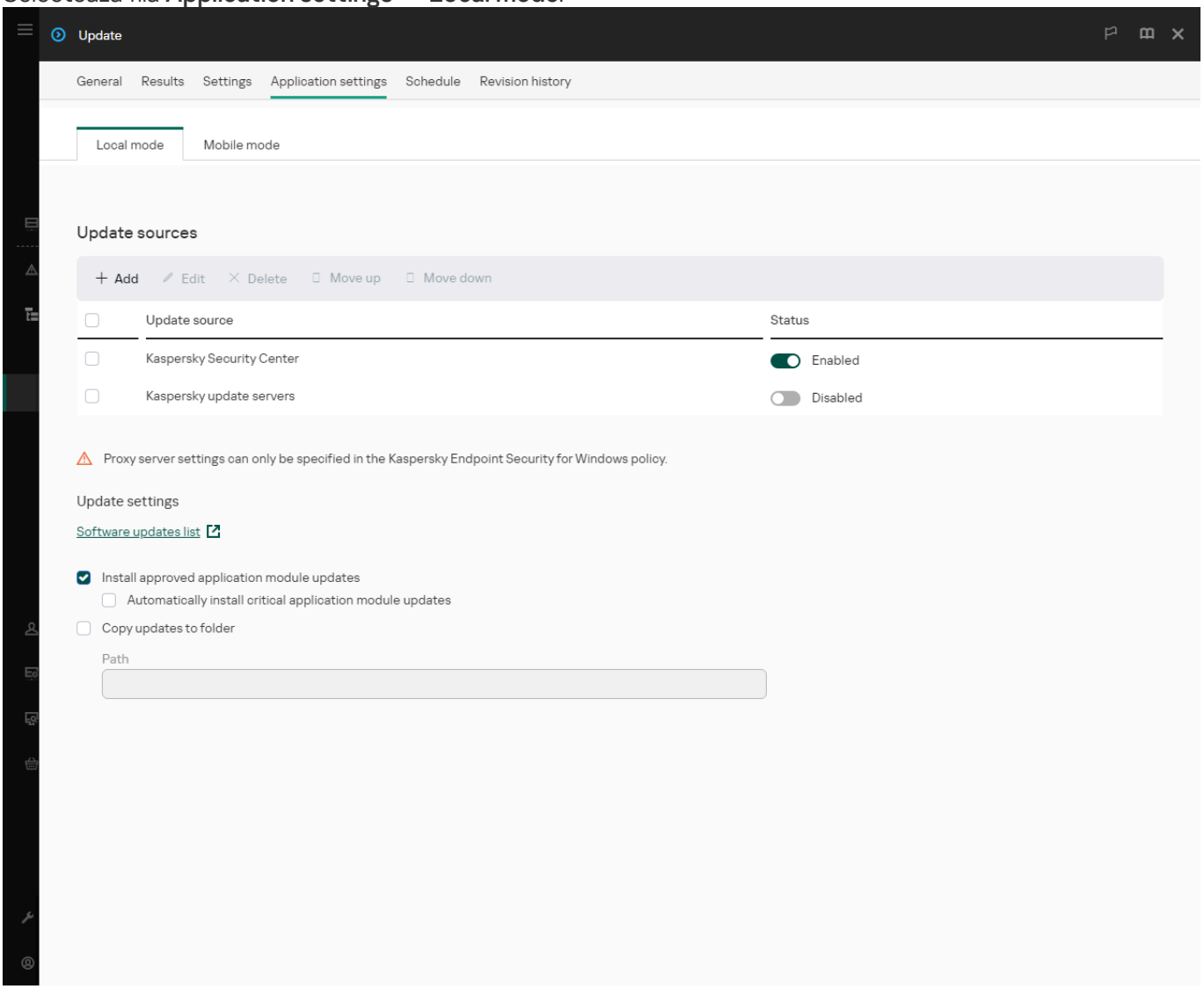
   Lista activităților se deschide.

2. Faceți clic pe activitatea **Update** a Kaspersky Endpoint Security.

   Se va deschide fereastra de proprietăți a activității.

   Activitatea *Update* este creată automat de Expertul de pornire rapidă a Serverului de administrare. Pentru a crea activitatea *Update*, instalați plug-inul Kaspersky Endpoint Security for Windows Management în timp ce executați Expertul.

3. Selectează fila **Application settings** → **Local mode**.



Surse de actualizare

4. În lista de surse de actualizări, faceți clic pe butonul **Add**.

5. În fereastra care se deschide, specificați adresa serverului FTP sau HTTP, directorul de rețea sau directorul local care conține pachetul de actualizare.

   Pentru sursa de actualizare se utilizează următorul format de cale:

   - Pentru un server FTP sau HTTP, introdu adresa sa Web sau IP.

     De exemplu, `http://dnl-01.geo.kaspersky.com/` sau `93.191.13.103`.

Pentru un server FTP, puteți specifica setările de autentificare în adresă în următorul format: `ftp://<user name>:<password>@<node>:<port>`.

- Pentru un director de rețea, introduceți calea UNC.

  De exemplu, `\\Server\Share\Update distribution`.

- Pentru un director local, introdu calea completă către acel director.

  De exemplu, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

Puteți exclude sursa de actualizare fără a o elimina din lista de surse de actualizare. Pentru aceasta, setați comutatorul de lângă acesta în poziția oprit.

6. Fă clic pe **OK**.
7. Configurați prioritățile surselor de actualizări folosind butoanele **Up** și **Down**.

   Dacă o actualizare nu poate fi efectuată din prima sursă de actualizare, Kaspersky Endpoint Security comută automat la sursa următoare.

8. Daca este necesar, adăugați o sursă de actualizare pentru modul mobil. *Modul Mobil* este modul de operare al aplicației Kaspersky Endpoint Security atunci când un computer părăsește perimetrul rețelei organizației (*computer offline*).
9. Salvați-vă modificările.

Cum se adaugă o sursă de actualizare în interfața aplicației

Nu puteți configura activitatea de grup *Actualizarea modulelor bazelor de date și ale aplicațiilor* în interfața aplicației. Doar o activitate de actualizare locală, *Actualizarea modulelor bazelor de date și ale aplicațiilor*, este disponibilă pentru utilizator. Dacă activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* nu este afișată, înseamnă că administratorul a interzis utilizarea activităților locale în politică.

1. În fereastra principală a aplicației, accesați secțiunea **Actualizare**.



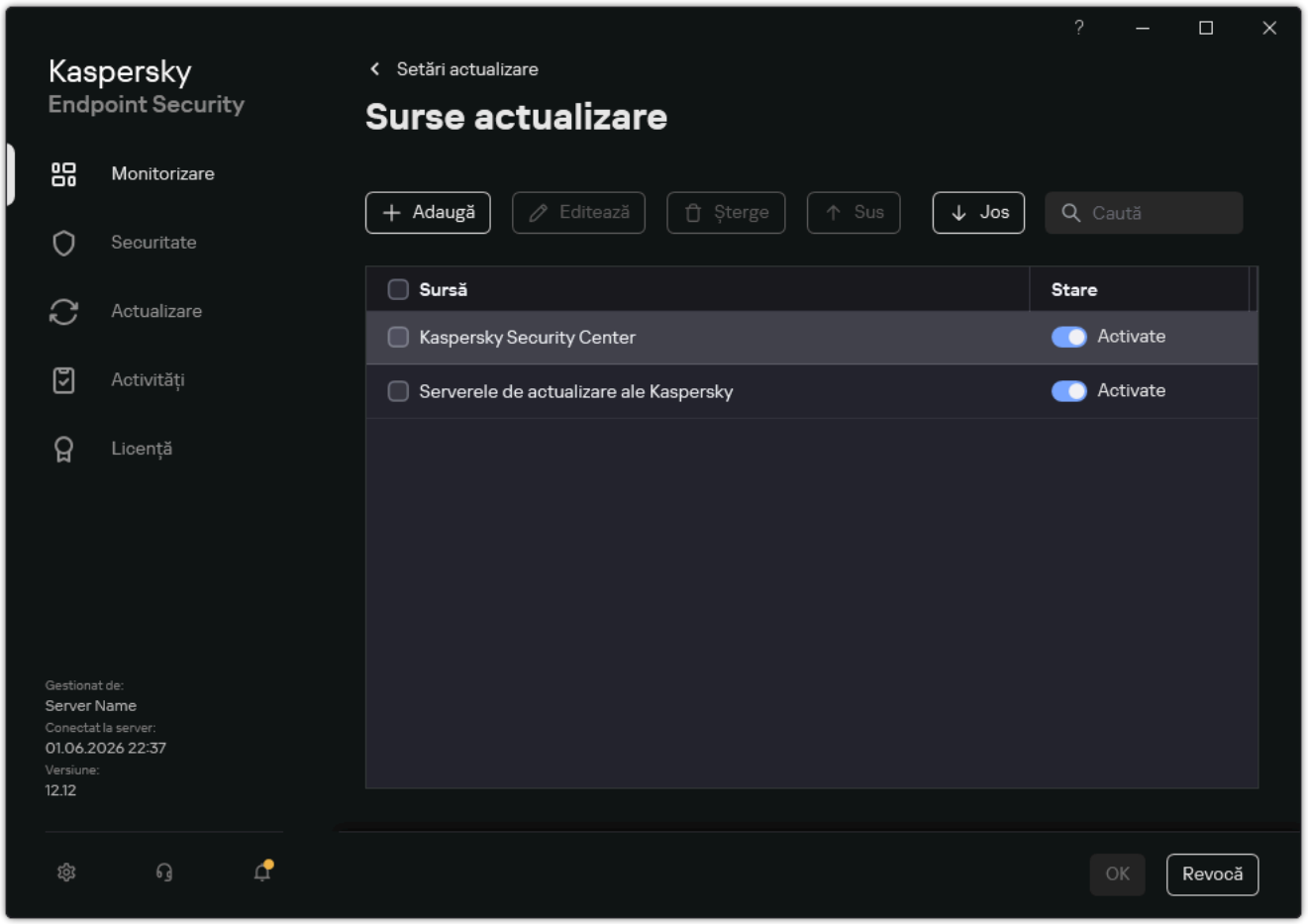
Activitate de actualizare locală

2. Se deschide lista de activități; selectați activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* și faceți clic pe ⚙.

   Se va deschide fereastra de proprietăți a activității.

3. Fă clic pe **Selectează sursele de actualizare**.

4. În fereastra care se deschide, faceți clic pe butonul **Adaugă**.



Surse de actualizare

5. În fereastra care se deschide, specificați adresa serverului FTP sau HTTP, directorul de rețea sau directorul local care conține pachetul de actualizare.

   Pentru sursa de actualizare se utilizează următorul format de cale:

   - Pentru un server FTP sau HTTP, introdu adresa sa Web sau IP.

     De exemplu, `http://dnl-01.geo.kaspersky.com/` sau `93.191.13.103`.

     Pentru un server FTP, puteți specifica setările de autentificare în adresă în următorul format: `ftp://<user name>:<password>@<node>:<port>`.

   - Pentru un director de rețea, introduceți calea UNC.

     De exemplu, `\\Server\Share\Update distribution`.

   - Pentru un director local, introdu calea completă către acel director.

     De exemplu, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

6. Fă clic pe **Selectează**.

7. Configurați prioritățile surselor de actualizări folosind butoanele **Sus** și **Jos**.

8. Salvați-vă modificările.

Actualizarea modulelor aplicației

Actualizările modulelor aplicației remediază erorile, îmbunătățesc performanța și adaugă noi funcții. Când devine disponibilă o nouă actualizare a modulelor aplicației, trebuie să confirmați instalarea actualizării. Puteți confirma instalarea unei actualizări a modulelor aplicației fie în interfața aplicației, fie în Kaspersky Security Center. Ori de câte ori este disponibilă o actualizare, aplicația afișează o notificare în fereastra principală a Kaspersky Endpoint Security: . Dacă actualizările modulelor aplicației necesită revizuirea și acceptarea Acordului de licență pentru utilizatorul final, aplicația instalează actualizările numai după acceptarea termenilor Acordului de licență pentru utilizatorul final.

După instalarea unei actualizări a aplicației, este posibil să vi se solicite să reporniți computerul.

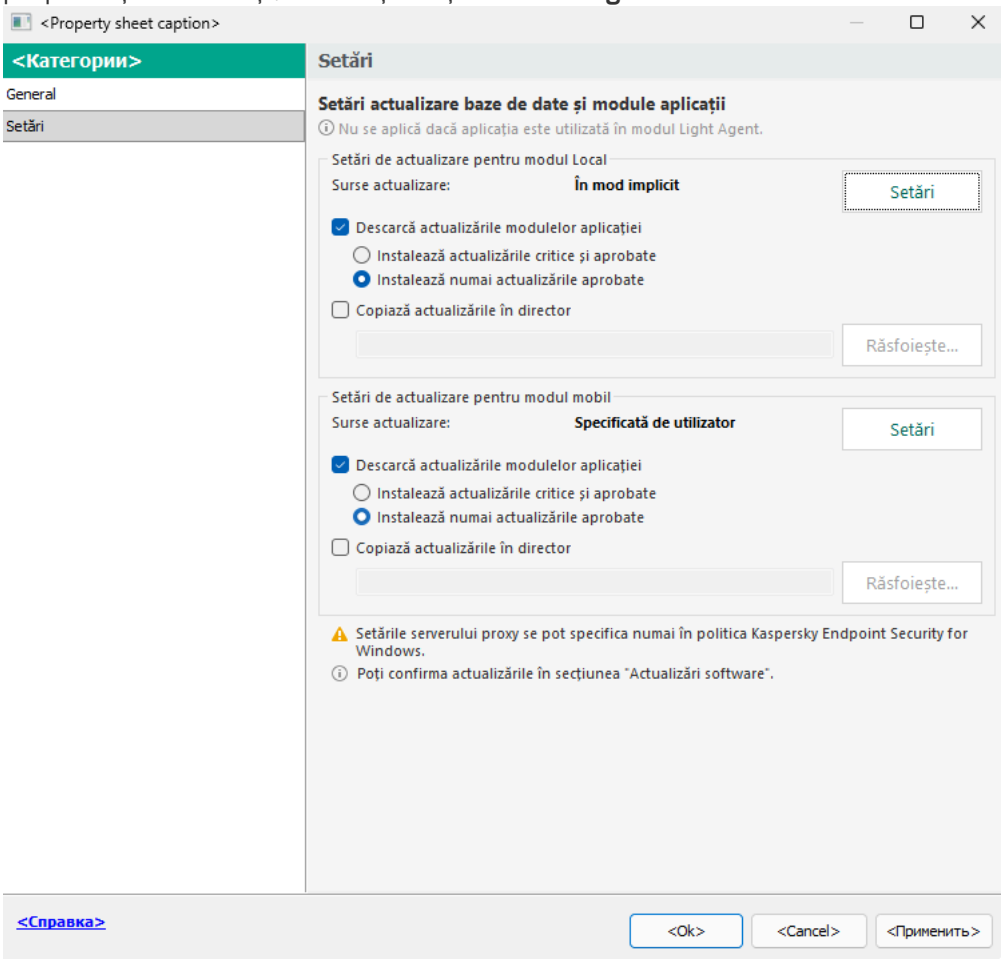
Cum se configurează actualizările modulelor aplicației în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați **Tasks**.
3. Faceți clic pe activitatea **Actualizarea modulelor bazelor de date și ale aplicațiilor** a Kaspersky Endpoint Security.

   Se va deschide fereastra de proprietăți a activității.

   Activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* este creată automat de Expertul de pornire rapidă a Serverului de administrare. Pentru a crea activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor*, instalați plug-inul Kaspersky Endpoint Security for Windows Management în timp ce executați Expertul.

4. În fereastra cu proprietățile activității, selectați secțiunea **Settings**.



Setări activitate Actualizarea modulelor bazelor de date și ale aplicațiilor

5. În blocul **Setări de actualizare pentru modul Local**, bifați caseta de selectare **Descarcă actualizările modulelor aplicației**.

   Dacă dorești să împiedici descărcarea actualizărilor modulelor aplicațiilor, debifează caseta de selectare **Descarcă actualizările modulelor aplicației** și interzice utilizarea activităților locale de către utilizator.

6. Selectați actualizările modulelor aplicației pe care doriți să le instalați.

   - **Instalează actualizările critice și aprobate**. Dacă este selectată această opțiune, atunci când sunt disponibile actualizări ale modulelor aplicației, Kaspersky Endpoint Security instalează automat actualizările critice și orice altă actualizare a modulelor aplicației numai după ce instalarea lor este aprobată local prin interfața aplicației sau în Kaspersky Security Center.

   - **Instalează numai actualizările aprobate**. Dacă este selectată această opțiune, atunci când sunt disponibile actualizări ale modulelor aplicației, Kaspersky Endpoint Security le instalează numai după ce instalarea lor este aprobată local prin interfața aplicației sau în Kaspersky Security Center. Această opțiune este selectată în mod implicit.

7. Daca este necesar, configurează actualizările modulelor aplicațiilor pentru modul mobil. *Modul Mobil* este modul de operare al aplicației Kaspersky Endpoint Security atunci când un computer părăsește perimetrul rețelei organizației (*computer offline*).

8. Salvați-vă modificările.

Cum se configurează actualizările modulelor alicațiilor în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectează **Tasks**.

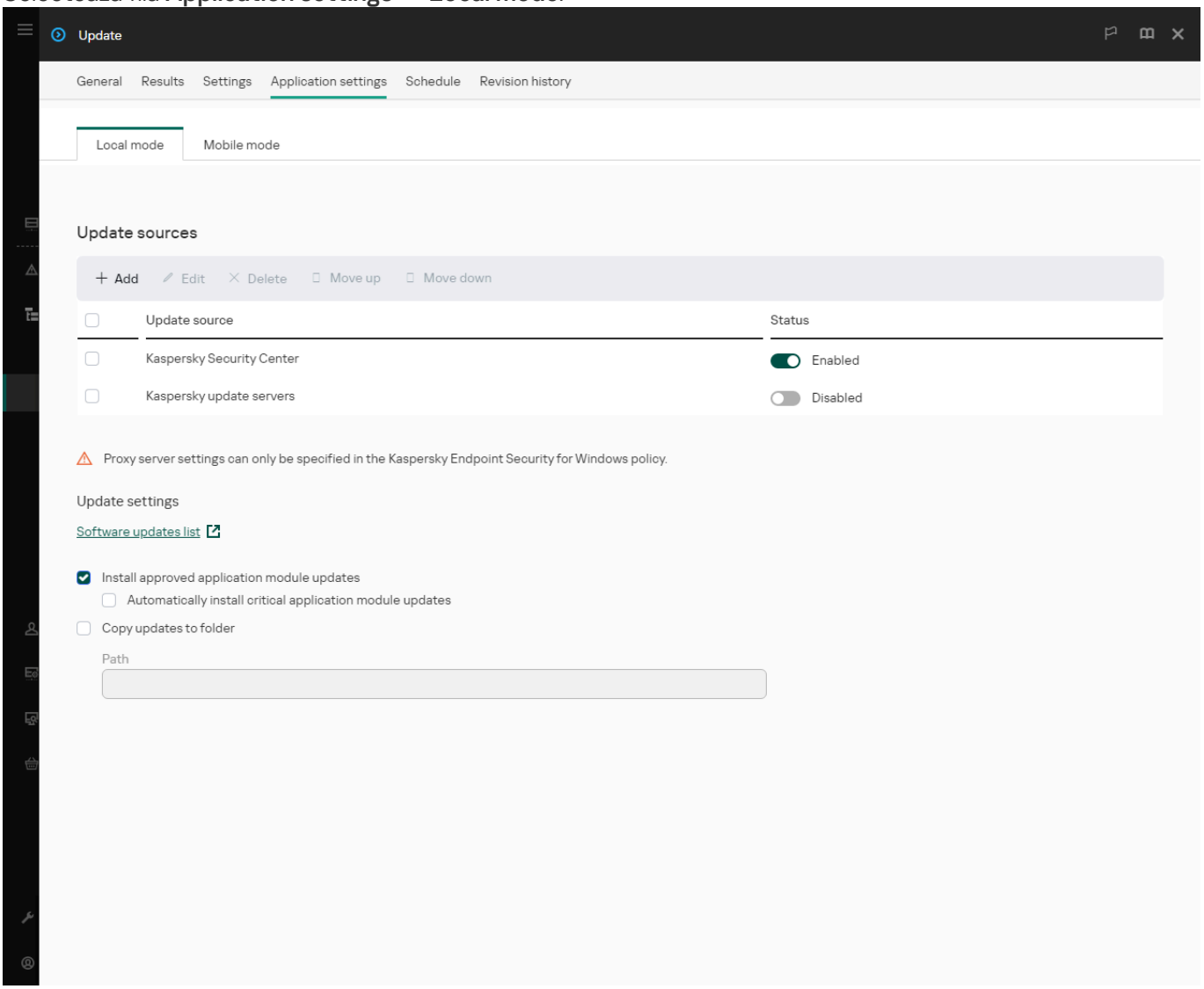
   Lista activităților se deschide.

2. Faceți clic pe activitatea **Actualizarea modulelor bazelor de date și ale aplicațiilor** a Kaspersky Endpoint Security.

   Se va deschide fereastra de proprietăți a activității.

   Activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* este creată automat de Expertul de pornire rapidă a Serverului de administrare. Pentru a crea activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor*, instalați plug-inul Kaspersky Endpoint Security for Windows Management în timp ce executați Expertul.

3. Selectează fila **Application settings** → **Local mode**.



Setări activitate Update

4. În **Update settings**, selectează actualizările modulelor aplicației pe care dorești să le instalezi:

   - **Install approved application module updates**. Dacă este selectată această opțiune, atunci când sunt disponibile actualizări ale modulelor aplicației, Kaspersky Endpoint Security le instalează numai după ce instalarea lor este aprobată local prin interfața aplicației sau în Kaspersky Security Center. Această opțiune este selectată în mod implicit.

   - **Automatically install critical application module updates**. Dacă este selectată această opțiune, atunci când sunt disponibile actualizări ale modulelor aplicației, Kaspersky Endpoint Security instalează automat actualizările critice și orice altă actualizare a modulelor aplicației numai după ce instalarea lor este aprobată local prin interfața aplicației sau în Kaspersky Security Center.

Dacă dorești să împiedici descărcarea actualizărilor modulelor aplicațiilor, debifează casetele de selectare **Install approved application module updates** și **Automatically install critical application module updates** și interzice utilizarea activităților locale de către utilizator.

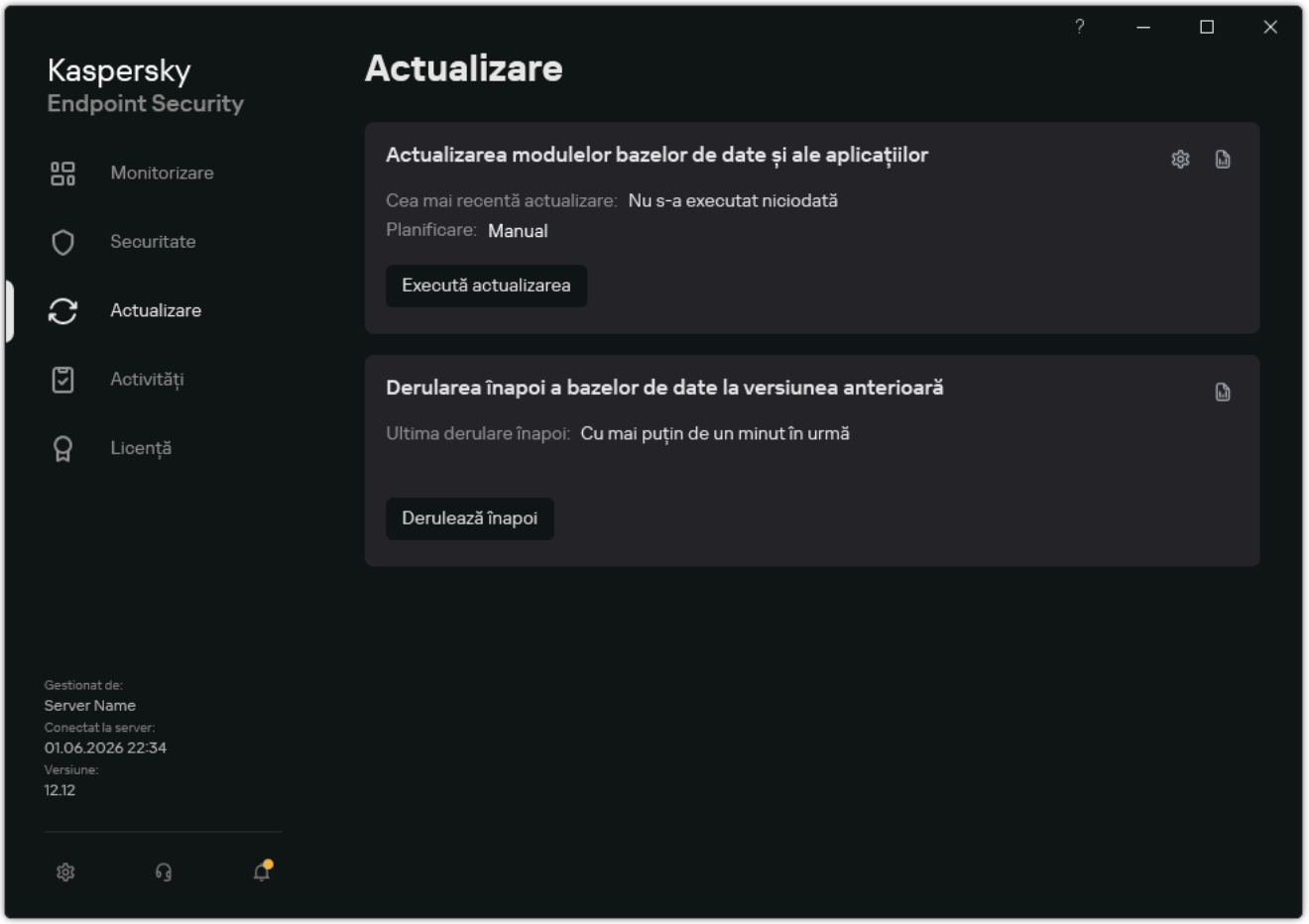
5. Daca este necesar, configurează actualizările modulelor aplicațiilor pentru modul mobil. *Modul Mobil* este modul de operare al aplicației Kaspersky Endpoint Security atunci când un computer părăsește perimetrul rețelei organizației (*computer offline*).

6. Salvați-vă modificările.

Cum se configurează actualizările modulelor aplicației în interfața aplicației

Nu puteți configura activitatea de grup *Actualizarea modulelor bazelor de date și ale aplicațiilor* în interfața aplicației. Doar o activitate de actualizare locală, *Actualizarea modulelor bazelor de date și ale aplicațiilor*, este disponibilă pentru utilizator. Dacă activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* nu este afișată, înseamnă că administratorul a interzis utilizarea activităților locale în politică.

1. În fereastra principală a aplicației, accesați secțiunea **Actualizare**.



Activitate de actualizare locală

2. Se deschide lista de activități; selectați activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* și faceți clic pe ⚙.

   Se va deschide fereastra de proprietăți a activității.

3. În blocul **Descărcarea și instalarea actualizărilor modulelor aplicației**, bifați caseta de selectare **Descarcă actualizările modulelor aplicației**.

4. Selectați actualizările modulelor aplicației pe care doriți să le instalați.

   - **Instalează actualizările critice și aprobate**. Dacă este selectată această opțiune, atunci când sunt disponibile actualizări ale modulelor aplicației, Kaspersky Endpoint Security instalează automat actualizările critice și orice altă actualizare a modulelor aplicației numai după ce instalarea lor este aprobată local prin interfața aplicației sau în Kaspersky Security Center.

   - **Instalează numai actualizările aprobate**. Dacă este selectată această opțiune, atunci când sunt disponibile actualizări ale modulelor aplicației, Kaspersky Endpoint Security le instalează numai după ce instalarea lor este aprobată local prin interfața aplicației sau în Kaspersky Security Center. Această opțiune este selectată în mod implicit.

5. Salvați-vă modificările.

Utilizarea unui server proxy pentru actualizări

Este posibil să ți se solicite să specifici setările pentru serverul proxy pentru a descărca actualizări pentru baza de date și modulele aplicației din sursa de actualizare. Dacă există mai multe surse de actualizare, setările pentru serverul proxy se aplică pentru toate sursele. Dacă nu este necesar un server proxy pentru unele surse de actualizare, poți dezactiva utilizarea unui server proxy în proprietățile politicii. Kaspersky Endpoint Security va folosi, de asemenea, un server proxy pentru a accesa Kaspersky Security Network și serverele de activare.

Pentru a configura o conexiune la surse de actualizare printr-un server proxy:

1. În fereastra principală a Web Console, faceți clic pe ⚙.

   Se deschide fereastra de proprietăți a Serverului de administrare.

2. Accesează secțiunea **Configuring internet access**.

3. Bifați caseta de selectare **Use proxy server**.

4. Configurați setările pentru conexiunea la serverul proxy: adresa serverului proxy, portul și setările de autentificare (numele de utilizator și parola).

5. Salvați-vă modificările.

Pentru a dezactiva utilizarea unui server proxy pentru un anumit grup de administrare:

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **General Settings** → **Network Settings**.

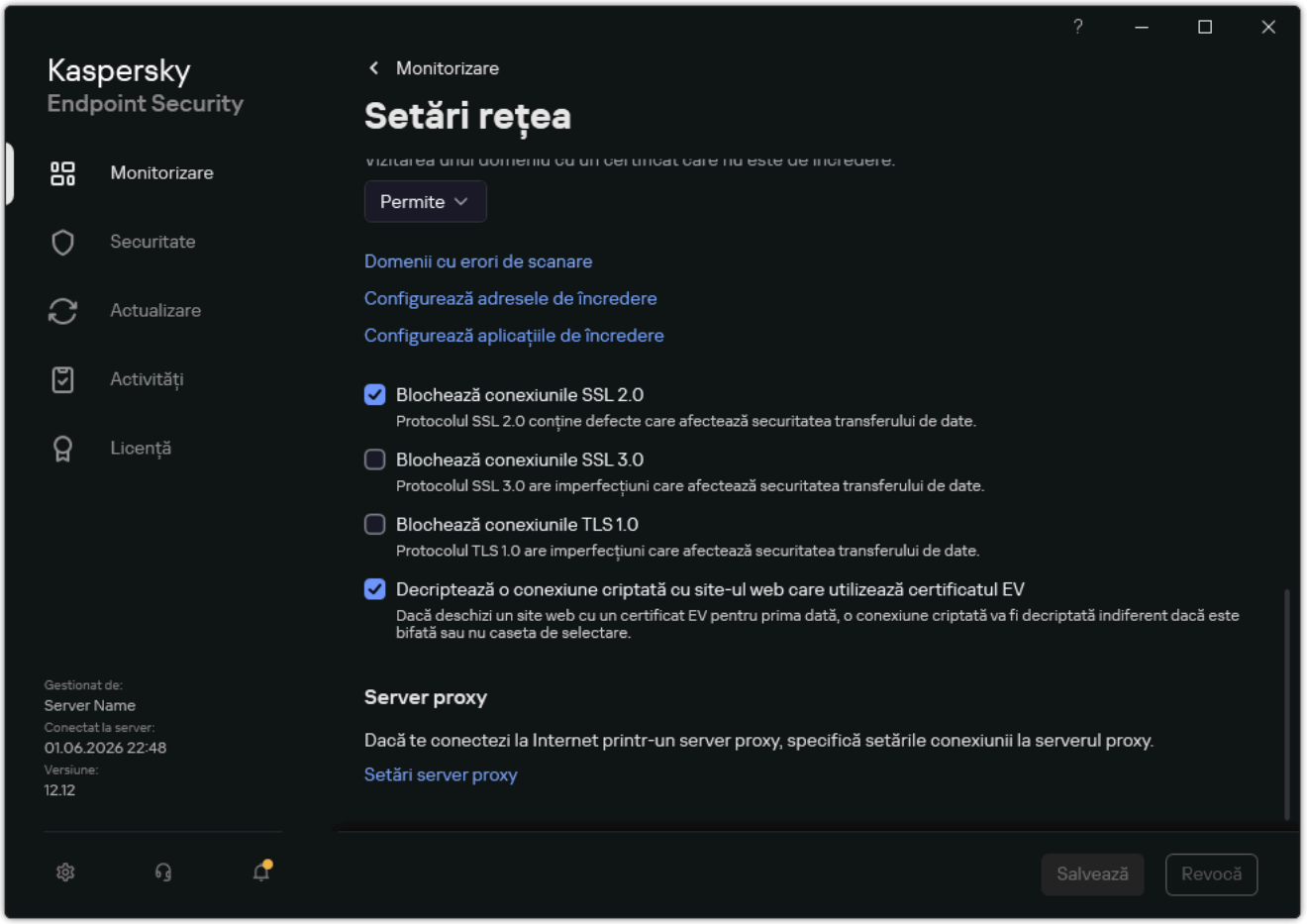
5. În blocul **Proxy server**, fă clic pe butonul **Settings**.

6. În fereastra care se deschide, bifați caseta de selectare **Bypass a proxy server for local addresses**.

7. Salvați-vă modificările.

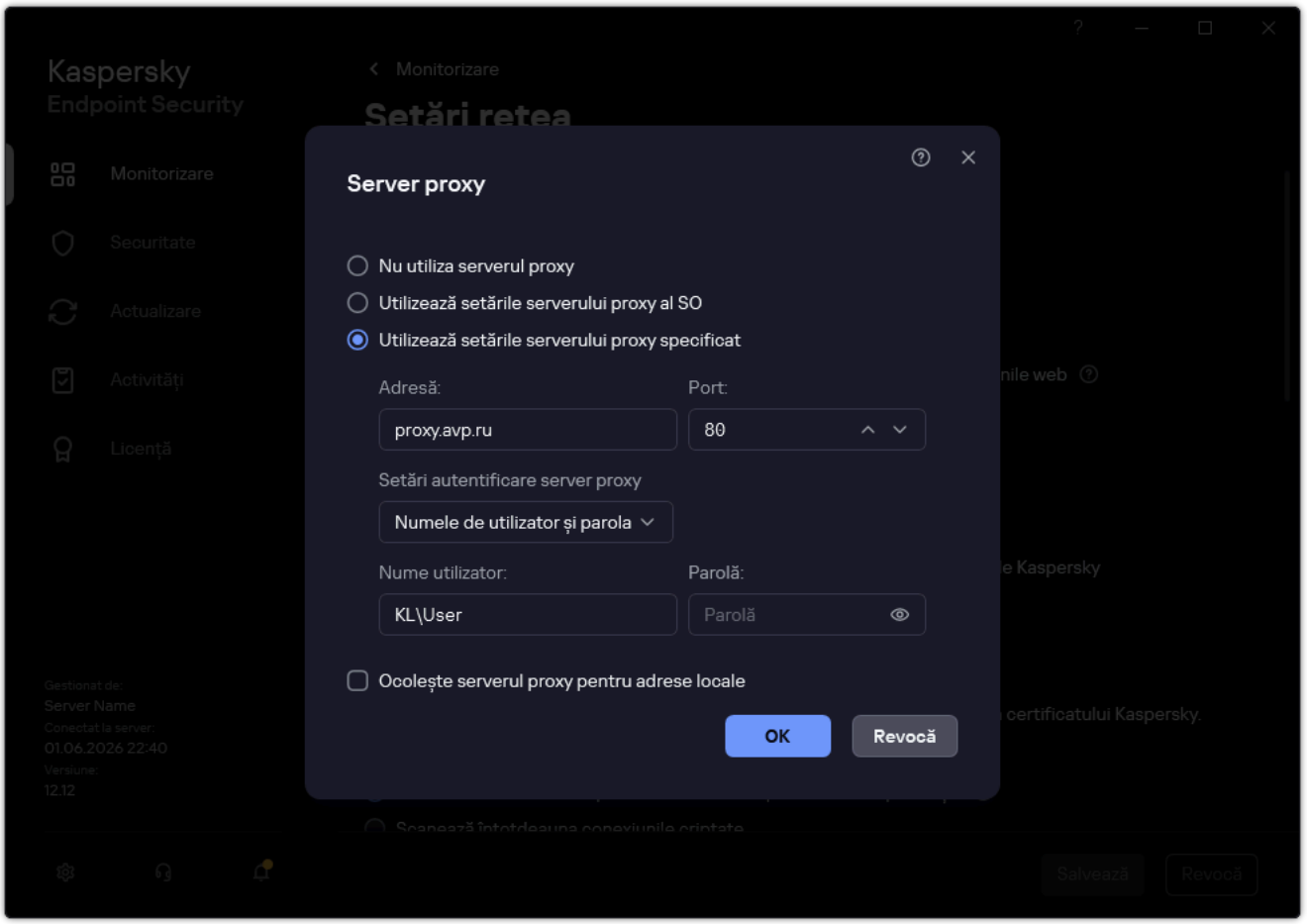
Pentru a configura setările serverului proxy în interfața aplicației:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Setări generale** → **Setări rețea**.



Setări de rețea pentru aplicație

3. În blocul **Server proxy**, faceți clic pe linkul **Setări server proxy**.



Setări conectare server proxy

4. În fereastra care se deschide, selectați una dintre opțiunile următoare pentru a determina adresa serverului proxy:

   - **Utilizează setările serverului proxy al SO**.

     Această opțiune este selectată în mod implicit. Kaspersky Endpoint Security utilizează setările serverului proxy definite în setările sistemului de operare.

   - **Utilizează setările serverului proxy specificat**.

     Dacă ați selectat această opțiune, configurați setările pentru conectarea la serverul proxy: adresa și portul serverului proxy.

5. Selectează modul în care dorești să se autentifice aplicația pe serverul proxy. În mod implicit, aplicația folosește autentificarea NTLM la domeniu a utilizatorului curent.

6. Dacă doriți să dezactivați utilizarea serverului proxy atunci când actualizați bazele de date și modulele aplicațiilor dintr-un director partajat, bifați caseta de selectare **Ocolește serverul proxy pentru adrese locale**.

7. Salvați-vă modificările.

Ca urmare, Kaspersky Endpoint Security va utiliza serverul proxy pentru a descărca actualizările modulului de aplicații și a bazei de date. Kaspersky Endpoint Security va utiliza, de asemenea, serverul proxy pentru a accesa serverele KSN și serverele de activare Kaspersky. Dacă este necesară autentificarea pe serverul proxy, dar acreditările contului de utilizator nu au fost introduse sau sunt incorecte, Kaspersky Endpoint Security vă va solicita numele de utilizator și parola.

Derulare înapoi ultima actualizare

După prima actualizare a bazelor de date și modulelor aplicației, devine disponibilă funcția de derulare înapoi a bazelor de date și modulelor aplicației la versiunile lor anterioare.

De fiecare dată când utilizatorul pornește procesul de actualizare, aplicația Kaspersky Endpoint Security creează o copie de rezervă a bazelor de date și modulelor actuale ale aplicației. Acest lucru îți permite, atunci când este necesar, să derulezi înapoi bazele de date și modulele aplicației la versiunile lor anterioare. Derularea înapoi a celei mai recente actualizări este utilă, de exemplu, dacă o versiunea nouă a bazei de date generează un fals pozitiv care determină Kaspersky Endpoint Security să blocheze o aplicație sigură.

Kaspersky Endpoint Security în modul Light Agent nu acceptă activitatea *Derulare înapoi actualizare*.

Cum se derulează înapoi ultima actualizare în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **New task**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Selectarea tipului activității

1. Selectați **Kaspersky Endpoint Security for Windows (14.1)** → **Derulare înapoi actualizare**.

Pasul 2. Selectarea dispozitivelor cărora le va fi atribuită activitatea

Selectați computerele pe care se va efectua activitatea. Sunt disponibile următoarele opțiuni:

- Atribuirea activității unui grup de administrare. În acest caz, activitatea este atribuită computerelor incluse într-un grup de administrare creat anterior.
- Selectare computere detectate în rețea de Serverul de administrare: *dispozitive neatribuite*. Dispozitivele specifice pot include dispozitive din grupuri de administrare, precum și dispozitive neatribuite.
- Specificarea manuală a adreselor computerelor sau importarea adreselor dintr-o listă. Poți specifica nume NetBIOS, adrese IP și subrețele IP ale dispozitivelor cărora dorești să le atribui activitatea.

Pasul 3. Configurarea unei planificări de pornire a activității

Configurează planificarea activității, de exemplu, manual.

Pasul 4. Definirea numelui activității

Introdu un nume pentru activitate.

Pasul 7. Finalizarea creării activității

Ieșiți din Expert. Dacă este necesar, bifați caseta de selectare **Run the task after the wizard finishes**. Puteți monitoriza progresul activității în proprietățile activității.

Cum se derulează înapoi ultima actualizare în Web Console

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **Add**.

   Expertul de activitate pornește.

3. Configurați setările pentru activitate:

   a. În lista verticală **Application**, selectează **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. În lista verticală **Task type**, selectează **Update rollback**.

   c. În câmpul **Task name**, introdu o descriere succintă, de exemplu *Derulare înapoi actualizare*.

   d. În blocul **Devices to which the task will be assigned**, selectați domeniul activității.

4. Selectați dispozitive în funcție de opțiunea selectată pentru domeniul activității. Mergeți la pasul următor.

5. Selectează un cont pentru a executa activitatea. În mod implicit, Kaspersky Endpoint Security începe activitatea cu drepturile unui cont de utilizator local.

6. Ieșiți din Expert.

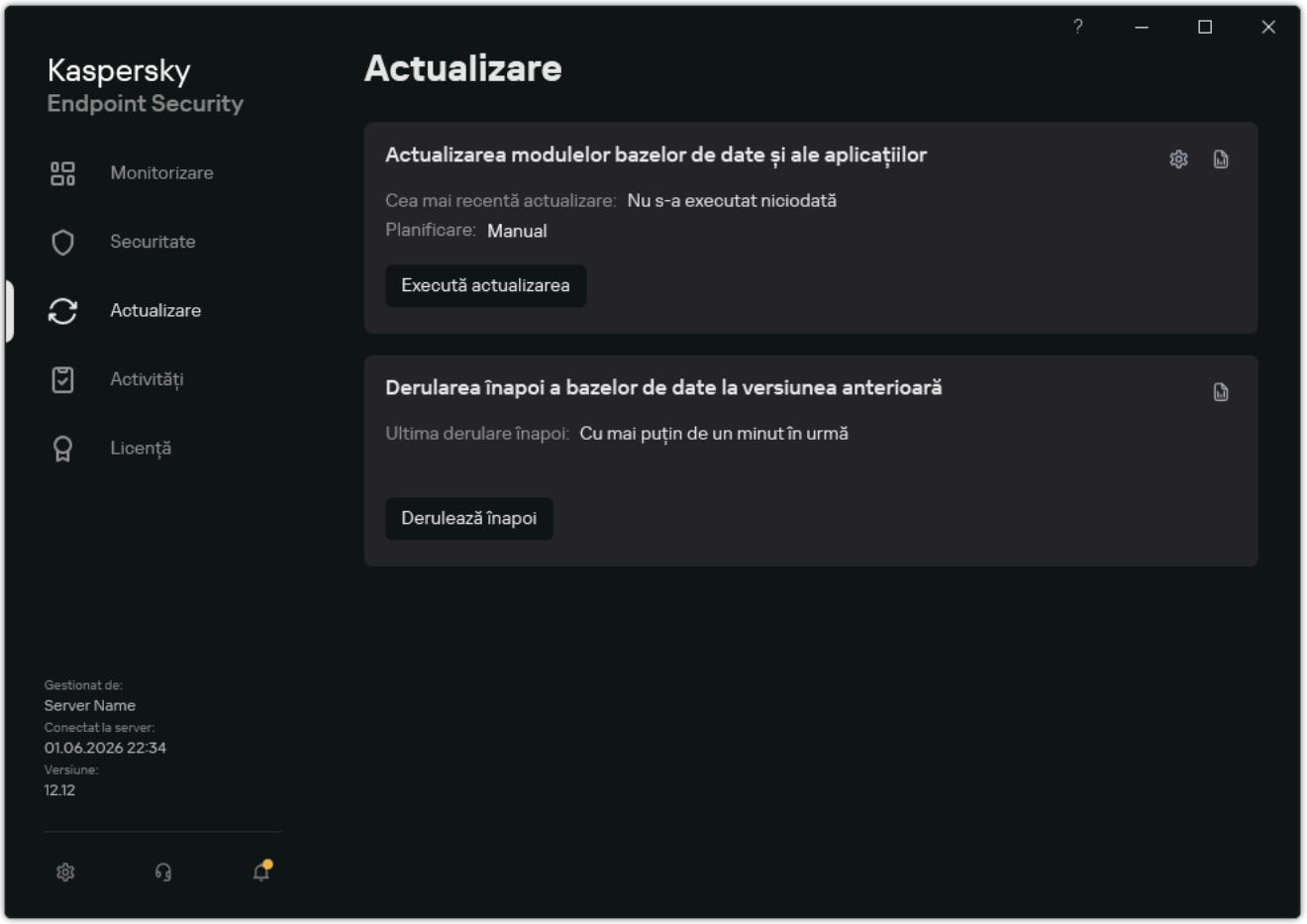
7. Se va afișa o activitate nouă în lista de activități.

8. Bifați caseta de selectare de lângă activitate.

9. Fă clic pe **Start**.

Cum se derulează înapoi ultima actualizare în interfața aplicației

1. În fereastra principală a aplicației, accesați secțiunea **Actualizare**.



Activitate de actualizare locală

2. În dala **Derularea înapoi a bazelor de date la versiunea anterioară**, fă clic pe butonul **Derulează înapoi**.

Kaspersky Endpoint Security va începe să anuleze ultima actualizare a bazei de date. Aplicația va afișa progresul de anulare, dimensiunea fișierelor descărcate și sursa de actualizare. Puteți opri activitatea în orice moment făcând clic pe butonul **Oprire actualizare**.

Tehnologia de dezinfectare avansată

Kaspersky Endpoint Security utilizează tehnologia Dezinfectare avansată pentru a lucra cu amenințările active. Tehnologia Dezinfectare avansată funcționează diferit în cazul serverelor și stațiilor de lucru. Poți configura dezinfectarea avansată în setările activității *Scanare malware* și în setările aplicației.

Dacă Kaspersky Endpoint Security nu poate opri din rulare o aplicație rău intenționată, puteți utiliza tehnologia Dezinfectare avansată. Pentru computerele care fac obiectul politicii, dezinfectarea avansată este dezactivată în mod implicit deoarece această tehnologie utilizează o cantitate semnificativă de resurse de procesare. Pentru computerele care nu fac obiectul unei politici, dezinfectarea avansată este activată în mod implicit.

Tehnologia Dezinfectare avansată funcționează diferit în cazul serverelor și stațiilor de lucru. Pentru a utiliza tehnologia pe servere, este necesar să activezi Dezinfectarea avansată imediată în proprietățile activității *Scanare malware*. Această cerință nu este necesară pentru a putea utiliza tehnologia pe stațiile de lucru.

Cum se activează sau dezactivează tehnologia Dezinfectare avansată în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Setări generale** → **Setări aplicație**.
4. În blocul **General**, bifați sau debifați caseta de selectare **Activează tehnologia Dezinfectare avansată** pentru a activa sau dezactiva tehnologia Dezinfectare avansată.
5. Salvați-vă modificările.

Cum se activează sau dezactivează componenta Dezinstalare avansată în Web Console și Cloud Console

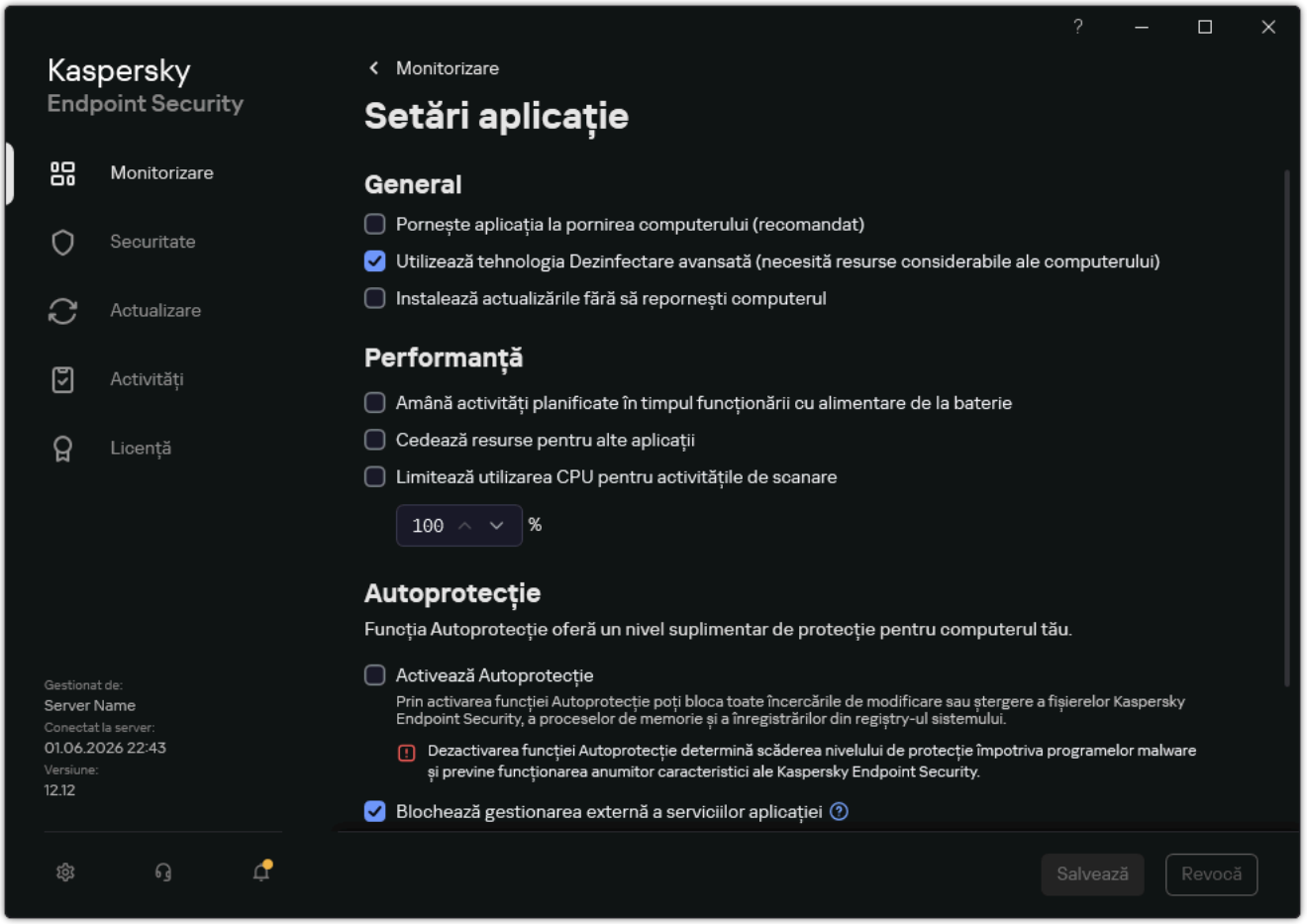
1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Selectați **General Settings** → **Detection Settings**.
5. În blocul **Advanced Disinfection Technology**, activează sau dezactivează comutatorul **Advanced Disinfection Technology ENABLED** pentru a activa sau dezactiva tehnologia Dezinfectare avansată.
6. Salvați-vă modificările.

Cum se activează sau dezactivează tehnologia Dezinfectare avansată în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Setări generale** → **Setări aplicație**.



Setări Kaspersky Endpoint Security for Windows

3. În blocul **General**, bifați sau debifați caseta de selectare **Utilizează tehnologia Dezinfectare avansată (necesită resurse considerabile ale computerului)** pentru a activa sau dezactiva tehnologia Dezinfectare avansată.

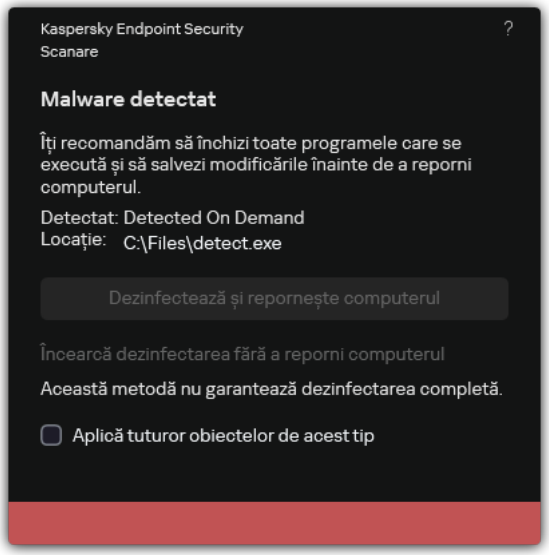
4. Salvați-vă modificările.

În concluzie, utilizatorul nu poate folosi majoritatea funcțiilor sistemului de operare, cât timp se desfășoară Dezinfectarea avansată. Când activitatea de dezinfectare este finalizată, computerul va fi repornit.

Dezinfectarea amenințărilor active pe stațiile de lucru

Pentru a lucra cu amenințările active pe stațiile de lucru, activați tehnologia Dezinfectare avansată în setările aplicației. În continuare, configurați experiența utilizatorului în proprietățile activității *Scanare malware*. Există o casetă de selectare **Execută Dezinfectare avansată imediat** în proprietățile activității. Dacă această casetă este bifată, Kaspersky Endpoint Security va realiza activitatea de dezinfectare, fără a notifica utilizatorul. Când activitatea de dezinfectare este finalizată, computerul va fi repornit. Dacă această casetă nu este bifată, Kaspersky Endpoint Security va afișa o notificare cu privire la amenințările active (vizualizați imaginea de mai jos). Nu puteți închide această notificare fără să procesați fișierul.

Dezinfectarea avansată în timpul unei activități de scanare de viruși pe computer se efectuează doar dacă este activată caracteristica Dezinfectare avansată în proprietățile politicii aplicate pe acest computer.



Notificare cu privire la amenințarea activă

Dezinfectarea amenințărilor active de pe servere

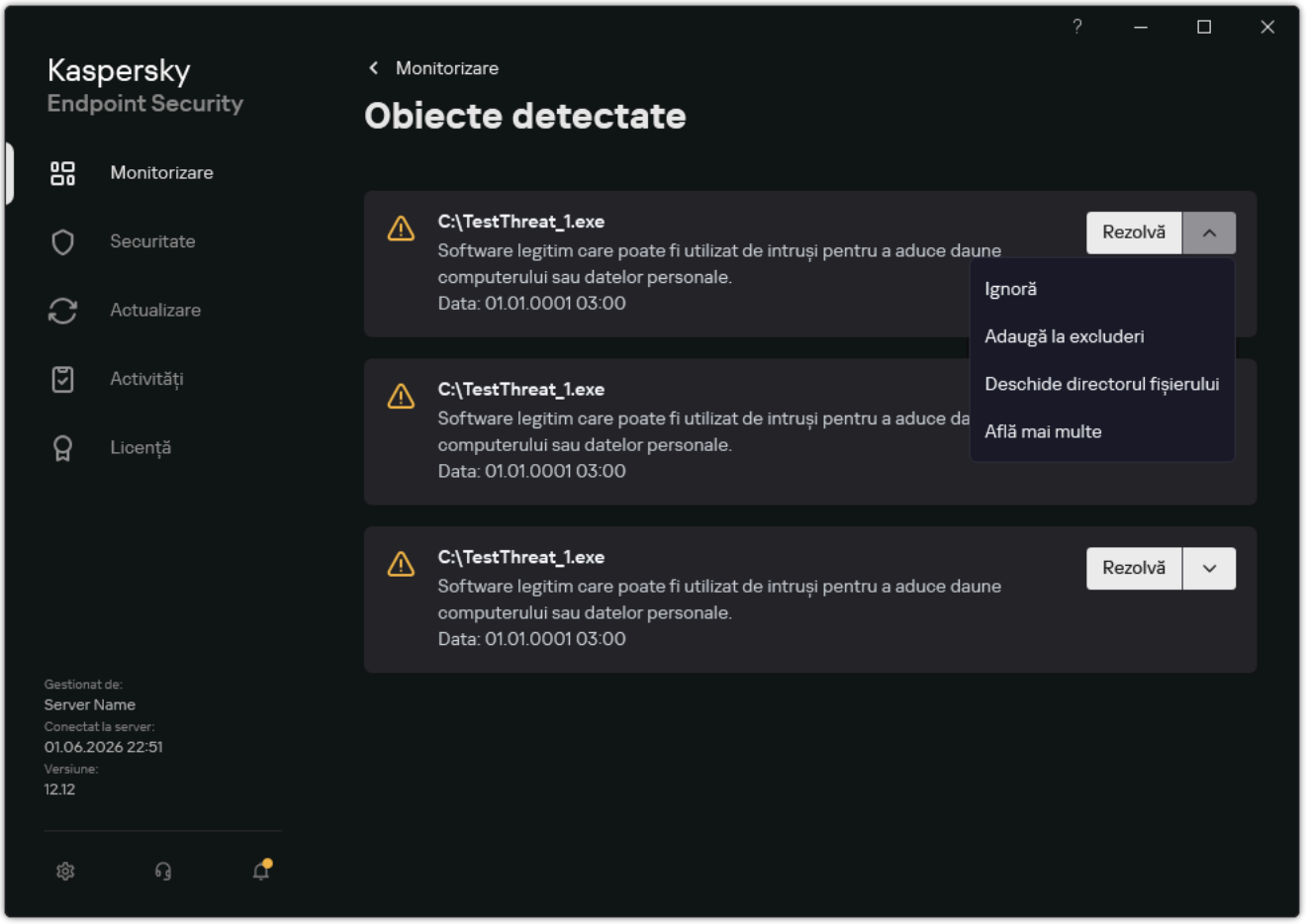
Pentru a lucra cu amenințările active de pe servere, trebuie să realizați următoarele:

- activați tehnologia Dezinfectare automată în setările aplicației;
- activați Dezinfectarea avansată imediată în proprietățile activității *Scanare malware*.

Dacă Kaspersky Endpoint Security este instalat pe un computer care rulează Windows Server, Kaspersky Endpoint Security nu va afișa notificarea. Prin urmare, nu poți selecta o acțiune pentru a dezinfecta o amenințare activă. Pentru a neutraliza o amenințare, este necesar să activați tehnologia Dezinfectare avansată în setările aplicației și să activați imediat Dezinfectarea avansată din proprietățile activității *Scanare malware*. Apoi, este necesar să porniți activitatea *Scanare malware*.

Eliminarea amenințărilor neprocesate

Kaspersky Endpoint Security înregistrează în jurnal informațiile despre fișierele neprocesate dintr-un anumit motiv. Aceste informații sunt înregistrate sub forma unor evenimente în lista de amenințări active (consultați figura de mai jos).



O listă de amenințări active

Un fișier infectat este considerat *procesat* dacă Kaspersky Endpoint Security a dezinfectat fișierul sau a eliminat amenințarea ca parte a scanării computerului pentru viruși și alte programe malware.

Kaspersky Endpoint Security mută fișierul în lista de amenințări active dacă, indiferent de motiv, Kaspersky Endpoint Security nu reușește să efectueze o acțiune asupra acestui fișier, în conformitate cu setările de aplicație specificate atunci când scanează computerul după viruși și alte amenințări.

Această situație este posibilă în următoarele cazuri:

- Fișierul scanat este indisponibil (de exemplu, este localizat pe o unitate de rețea sau pe o unitate amovibilă, fără privilegii de scriere).
- În setările activității *Scanare malware*, acțiunea la detectarea amenințărilor este setată la **Informează**. Apoi, când notificarea fișierului infectat a fost afișată pe ecran, utilizatorul a selectat **Ignoră**.

Dacă nu există amenințări neprocesate, Kaspersky Endpoint Security schimbă pictograma în . În fereastra principală a aplicației, este afișată notificarea privind amenințarea (consultați figura de mai jos). În consola Kaspersky Security Center, starea computerului este schimbată în *Critical* – .

Cum se procesează o amenințare în Consola de administrare (MMC)

1. În Consola de administrare, accesați directorul **Administration Server** → **Advanced** → **Repositories** → **Active threats**.

   Se deschide lista amenințărilor active.

2. Selectați obiectul pe care doriți să îl procesați.

3. Alegeți cum doriți să gestionați amenințarea:

   - **Disinfect**. Dacă selectezi această opțiune, aplicația încearcă automat să dezinfecteze fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, aplicația șterge fișierul.

   - **Delete**. Dacă această opțiune este selectată, aplicația șterge fișierele infectate detectate din depozitul de amenințări active. În acest caz, aplicația păstrează fișierul detectat în memoria computerului. Pentru a elimina amenințarea din computer, selectează **Disinfect**.

Cum se procesează o amenințare în Web Console și Cloud Console

1. În fereastra principală a componentei Web Console, selectați **Operations** → **Repositories** → **Active threats**.

   Se deschide lista amenințărilor active.

2. Selectați obiectul pe care doriți să îl procesați.

3. Alegeți cum doriți să gestionați amenințarea:

   - **Disinfect**. Dacă selectezi această opțiune, aplicația încearcă automat să dezinfecteze fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, aplicația șterge fișierul.

   - **Delete**. Dacă această opțiune este selectată, aplicația șterge fișierele infectate detectate din depozitul de amenințări active. În acest caz, aplicația păstrează fișierul detectat în memoria computerului. Pentru a elimina amenințarea din computer, selectează **Disinfect**.

Cum se procesează o amenințare în interfața aplicației

1. În fereastra principală a aplicației, în secțiunea **Monitorizare**, faceți clic pe dala **Protecția este în pericol**.

   Se deschide lista amenințărilor active.

2. Selectați obiectul pe care doriți să îl procesați.

3. Alegeți cum doriți să gestionați amenințarea:

   - **Rezolvă**. Dacă selectezi această opțiune, aplicația încearcă automat să dezinfecteze fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, aplicația șterge fișierul.

   - **Adaugă la excluderi**. Dacă această acțiune este selectată, Kaspersky Endpoint Security sugerează adăugarea fișierului la lista de excluderi de la scanare. Setările excluderii sunt configurate automat. Dacă adăugarea unei excluderi nu este disponibilă, înseamnă că administratorul a dezactivat adăugarea de excluderi în setările politicii.

   - **Ignoră**. Dacă selectați această opțiune, Kaspersky Endpoint Security șterge intrarea din lista de amenințări active. Dacă în listă nu mai rămâne nicio amenințare activă, starea computerului se va schimba în *OK*. Dacă obiectul este detectat din nou, Kaspersky Endpoint Security va adăuga o nouă intrare în lista de amenințări active.

- **Deschide directorul fișierului**. Dacă este selectată această opțiune, Kaspersky Endpoint Security deschide directorul care conține obiectul din managerul de fișiere. Puteți apoi șterge manual obiectul sau îl puteți muta într-un director care nu se află în domeniul de protecție.

- **Află mai multe**. Dacă este selectată această opțiune, Kaspersky Endpoint Security deschide site-ul web Baza de date Kaspersky pentru vulnerabilități și amenințări.

Pentru a procesa amenințările active în consola Kaspersky Security Center, trebuie să activezi transferul informațiilor despre fișierele neprocesate către Serverul de administrare. Transferul de date este activat în mod implicit.

Cum se activează transferul datelor fișierelor neprocesate în Consola de administrare (MMC)

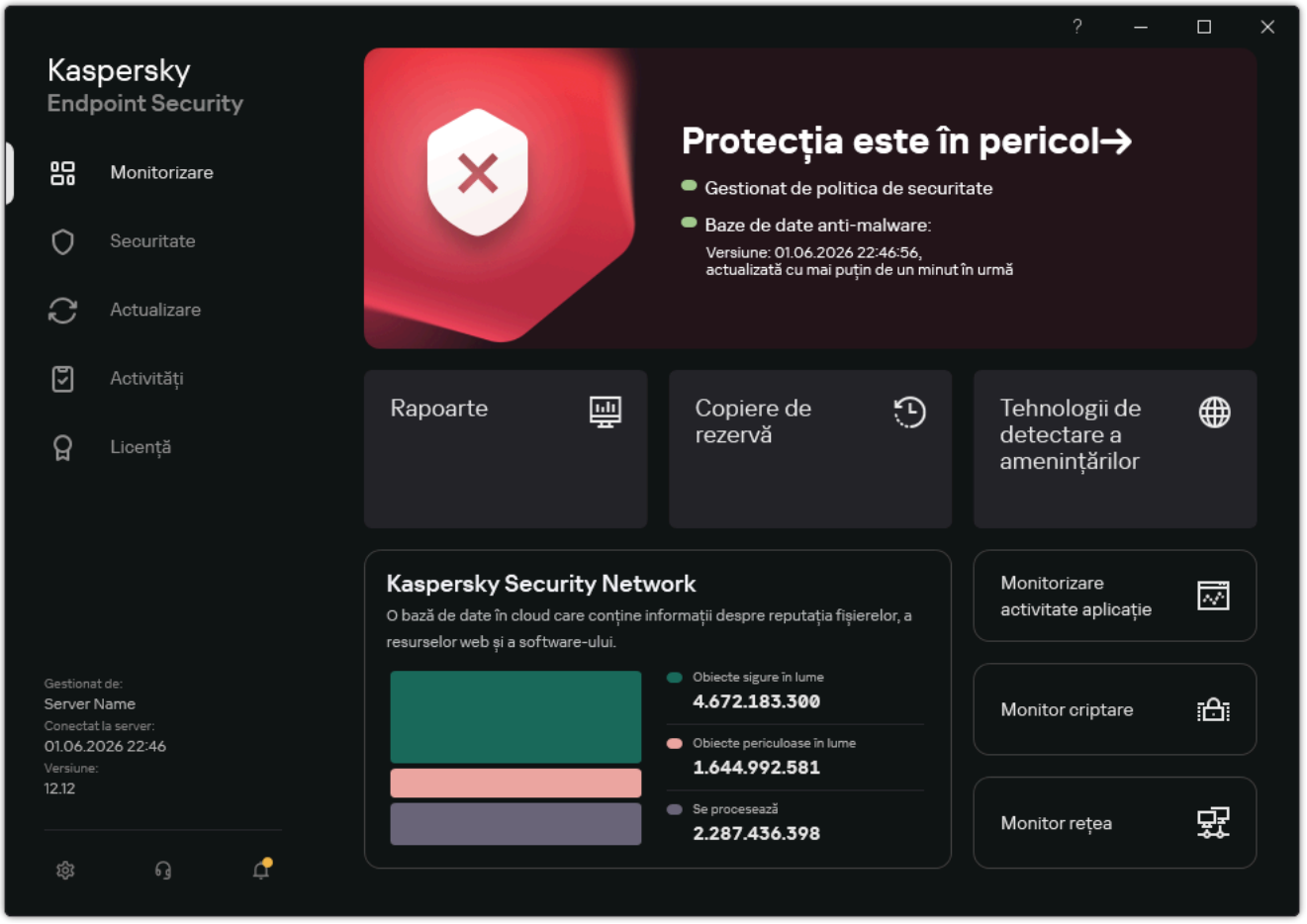
1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Setări generale** → **Rapoarte și Spații de stocare**.
4. În blocul **Transfer de date pe serverul de administrare**, fă clic pe butonul **Setări**.
5. Bifați caseta de selectare **Fișiere neprocesate**.
6. Salvați-vă modificările.

Cum se activează transferul datelor fișierelor neprocesate în Web Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.
   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **General Settings** → **KSC Integration**.

5. În blocul **Data transfer to Administration Server**, bifați caseta de selectare **About unprocessed files**.

6. Salvați-vă modificările.



Fereastra principală a aplicației când este detectată o amenințare

Protecția computerului

File Threat Protection

Componenta File Threat Protection îți permite să previi infectarea sistemului de fișiere al unui computer. În mod implicit, componenta File Threat Protection se află permanent în memoria RAM a computerului și scanează în timp real toate fișierele deschise, salvate sau executate. Componenta scanează fișierele de pe toate unitățile computerului, inclusiv de pe unitățile conectate. Componenta oferă protecție computerului cu ajutorul bazelor de date antivirus, a serviciului cloud Kaspersky Security Network și a analizei euristice.

Componenta scanează fișierele accesate de un utilizator sau de o aplicație. Dacă este detectat un fișier periculos, Kaspersky Endpoint Security blochează utilizarea fișierului. Aplicația apoi dezinfectează sau șterge fișierul periculos, în funcție de setările componentei File Threat Protection.

Atunci când se încearcă accesarea unui fișier al cărui conținut este stocat în spațiul de stocare cloud OneDrive, Kaspersky Endpoint Security descarcă și scanează conținutul fișierului.

Activarea și dezactivarea componentei File Threat Protection

În mod implicit, componenta File Threat Protection este activată și se execută în modul recomandat de experții Kaspersky. Pentru File Threat Protection, Kaspersky Endpoint Security poate aplica diferite grupuri de setări. Aceste grupuri de setări care sunt stocate în aplicație sunt denumite *niveluri de securitate*: **Ridicat**, **Recomandat**, **Redus**. Setările pentru nivelul de securitate **Recomandat** sunt considerate a fi setările optime recomandate de către experții de la Kaspersky (consultați tabelul de mai jos). Poți să selectezi unul dintre nivelurile de securitate presetate sau să configurezi manual setările pentru nivelul de securitate. Dacă modifici setările pentru nivelul de securitate, poți reveni oricând la setările recomandate pentru nivelul de securitate.

Componenta File Threat Protection utilizează datele primite de la alte componente ale aplicației. Activarea acelor componente este opțională. Printre componentele care furnizează date suplimentare se numără:

- Kaspersky Security Network.
- Host Intrusion Prevention.
- Behavior Detection.

Cum se activează sau dezactivează componenta File Threat Protection în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Essential Threat Protection → File Threat Protection**.
4. Utilizează caseta de selectare **File Threat Protection** pentru a activa sau a dezactiva componenta.

5. Dacă ați activat componenta, efectuați una dintre următoarele acțiuni în blocul **Nivel de securitate**:

   - Dacă doriți să aplicați unul dintre nivelurile de securitate presetate, selectați-l folosind glisorul:

     - **Ridicat**. Atunci când este selectat acest nivel de securitate pentru fișiere, componenta File Threat Protection efectuează controlul cel mai strict asupra tuturor fișierelor deschise, salvate și pornite. Componenta File Threat Protection scanează toate tipurile de fișiere, de pe toate unitățile de hard disk, de pe toate unitățile amovibile și de pe toate unitățile de rețea ale computerului. De asemenea, componenta Antivirus pentru fișiere scanează arhivele, pachetele de instalare și obiectele OLE încorporate.

     - **Recomandat**. Acest nivel de securitate pentru fișiere este recomandat de specialiștii Kaspersky Lab. Componenta File Threat Protection scanează doar tipurile de fișiere specificate, de pe toate unitățile de hard disk, de pe toate unitățile amovibile și de pe toate unitățile de rețea ale computerului, precum și obiectele OLE încorporate. Componenta File Threat Protection nu scanează arhivele și pachetele de instalare.

     - **Redus**. Setările acestui nivel de securitate pentru fișiere asigură viteza de scanare maximă. Componenta File Threat Protection scanează numai fișierele cu extensiile specificate, de pe toate unitățile de hard disk, de pe toate unitățile amovibile și de pe toate unitățile de rețea ale computerului. Componenta File Threat Protection nu scanează fișierele compuse.

   - Dacă doriți să configurați un nivel de securitate personalizat, faceți clic pe butonul **Setări** și definiți propriile setări pentru componentă.

     Puteți restabili valorile nivelurilor de securitate prestabilite făcând clic pe butonul **În mod implicit**.

6. În blocul **Acțiune la detectarea amenințării**, selectează acțiunea pe care aplicația Kaspersky Endpoint Security trebuie să o efectueze asupra obiectelor rău intenționate:

   - **Dezinfectează; șterge dacă dezinfectarea nu reușește**. Dacă selectezi această opțiune, aplicația încearcă automat să dezinfecteze fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, aplicația șterge fișierul.

   - **Dezinfectează; blochează dacă dezinfectarea nu reușește**. Dacă selectezi această opțiune, aplicația încearcă automat să dezinfecteze fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, aplicația blochează fișierul.

   - **Blochează**. Dacă este selectată această opțiune, aplicația blochează automat fișierul infectat fără a încerca să îl dezinfecteze sau să îl șteargă.

   - **Informează**. Dacă este selectată această opțiune, Kaspersky Endpoint Security adaugă informațiile despre fișierele infectate în lista de amenințări active la detectarea acestor fișiere.

   Înainte de a încerca să dezinfectați sau să ștergeți un fișier infectat, aplicația creează o copie de rezervă a fișierului în cazul în care trebuie să restaurați fișierul sau dacă acesta poate fi dezinfectat în viitor.

7. Salvați-vă modificările.

Cum se activează sau dezactivează componenta Fileb Threat Protection în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesează **Host Threat Protection** → **File Threat Protection**.

5. Utilizați comutatorul **File Threat Protection ENABLED** pentru a activa sau a dezactiva componenta.

6. Dacă doriți să adăugați un obiect nou la domeniul de protecție:

   a. În **Advanced settings**, selectează fila **Protection scope**.

   b. Fă clic pe **Add**.

   c. Astfel, se deschide o fereastră; în acea fereastră, selectează obiectele pe care dorești să le adaugi la domeniul de protecție.

   Folosiți măști:

   - Caracterul `*` (asterisc) ține locul oricărui set de caractere, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\*\*.txt` va include toate căile către fișierele cu extensia TXT din directoarele de pe unitatea C:, dar nu și din subdirectoare.

   - Două caractere `*` consecutive țin locul oricărui set de caractere (inclusiv un set gol) din numele de fișier sau director, inclusiv caracterele `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\**\*.txt` va include toate căile către fișierele cu extensia TXT localizată în directoarele imbricate în `Folder`, cu excepția `Folder` în sine. Masca trebuie să includă cel puțin un nivel de imbricare. Masca `C:\**\*.txt` nu este o mască validă.

   - `?` (semn de întrebare) ține locul oricărui caracter individual, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\???.txt` va include căi pentru toate fișierele din directorul denumit `Folder` care au extensia TXT și un nume format din trei caractere.

   Puteți utiliza măști oriunde într-o cale de fișier sau director. De exemplu, dacă doriți ca domeniul de scanare să includă directorul Descărcări pentru toate conturile de utilizator de pe computer, introduceți masca `C:\Users\*\Downloads\`.

   Poți exclude un obiect din protecție fără a-l șterge din lista de obiecte din domeniul de protecție. Pentru aceasta, setați comutatorul de lângă acesta în poziția oprit.

   d. Salvați-vă modificările.

7. În blocul **Action on threat detection**, selectează acțiunea pe care aplicația Kaspersky Endpoint Security trebuie să o efectueze asupra obiectelor rău intenționate:

   - **Disinfect, delete if disinfection fails**. Dacă selectezi această opțiune, aplicația încearcă automat să dezinfecteze fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, aplicația șterge fișierul.

   - **Disinfect, block if disinfection fails**. Dacă selectezi această opțiune, aplicația încearcă automat să dezinfecteze fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, aplicația blochează fișierul.

   - **Block**. Dacă este selectată această opțiune, aplicația blochează automat fișierul infectat fără a încerca să îl dezinfecteze sau să îl șteargă.

Înainte de a încerca să dezinfectați sau să ștergeți un fișier infectat, aplicația creează o copie de rezervă a fișierului în cazul în care trebuie să restaurați fișierul sau dacă acesta poate fi dezinfectat în viitor.

8. Dacă este necesar, editează setările avansate ale componentei File Threat Protection.

9. Salvați-vă modificările.

Cum se activează sau dezactivează componenta File Threat Protection în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **File Threat Protection**.

3. Utilizați comutatorul **File Threat Protection** pentru a activa sau a dezactiva componenta.

4. Dacă ați activat componenta, efectuați una dintre următoarele acțiuni în blocul **Nivel de securitate**:

   - Dacă doriți să aplicați unul dintre nivelurile de securitate presetate, selectați-l folosind glisorul:

     - **Ridicat**. Atunci când este selectat acest nivel de securitate pentru fișiere, componenta File Threat Protection efectuează controlul cel mai strict asupra tuturor fișierelor deschise, salvate și pornite. Componenta File Threat Protection scanează toate tipurile de fișiere, de pe toate unitățile de hard disk, de pe toate unitățile amovibile și de pe toate unitățile de rețea ale computerului. De asemenea, componenta Antivirus pentru fișiere scanează arhivele, pachetele de instalare și obiectele OLE încorporate.

     - **Recomandat**. Acest nivel de securitate pentru fișiere este recomandat de specialiștii Kaspersky Lab. Componenta File Threat Protection scanează doar tipurile de fișiere specificate, de pe toate unitățile de hard disk, de pe toate unitățile amovibile și de pe toate unitățile de rețea ale computerului, precum și obiectele OLE încorporate. Componenta File Threat Protection nu scanează arhivele și pachetele de instalare.

     - **Redus**. Setările acestui nivel de securitate pentru fișiere asigură viteza de scanare maximă. Componenta File Threat Protection scanează numai fișierele cu extensiile specificate, de pe toate unitățile de hard disk, de pe toate unitățile amovibile și de pe toate unitățile de rețea ale computerului. Componenta File Threat Protection nu scanează fișierele compuse.

   - Dacă dorești să configurezi un nivel de securitate personalizat, fă clic pe butonul **Setări avansate** și definește propriile setări pentru componentă.

     Puteți restabili valorile nivelurilor de securitate prestabilite făcând clic pe butonul **Restaurare nivel recomandat de securitate**.

5. În blocul **Acțiune la detectarea amenințării**, selectează acțiunea pe care aplicația Kaspersky Endpoint Security trebuie să o efectueze asupra obiectelor rău intenționate:

   - **Dezinfectează; șterge dacă dezinfectarea nu reușește**. Dacă selectezi această opțiune, aplicația încearcă automat să dezinfecteze fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, aplicația șterge fișierul.

   - **Dezinfectează; blochează dacă dezinfectarea nu reușește**. Dacă selectezi această opțiune, aplicația încearcă automat să dezinfecteze fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, aplicația blochează fișierul.

- **Blochează**. Dacă este selectată această opțiune, aplicația blochează automat fișierul infectat fără a încerca să îl dezinfecteze sau să îl șteargă.

- **Informează**. Dacă este selectată această opțiune, Kaspersky Endpoint Security adaugă informațiile despre fișierele infectate în lista de amenințări active la detectarea acestor fișiere.

Înainte de a încerca să dezinfectați sau să ștergeți un fișier infectat, aplicația creează o copie de rezervă a fișierului în cazul în care trebuie să restaurați fișierul sau dacă acesta poate fi dezinfectat în viitor.

6. Salvați-vă modificările.

Setări File Threat Protection recomandate de experții Kaspersky (nivel de securitate recomandat)

Parametru	Valoare	Descriere
Tipuri de fișiere	**Fișiere scanate după format**	Dacă se activează această setare, aplicația scanează numai fișierele infectabile. Înainte de scanarea unui fișier pentru detectarea de cod rău intenționat, se analizează antetul intern al fișierului pentru a se determina formatul fișierului (de exemplu, .txt, .doc sau .exe). De asemenea, scanarea caută fișiere cu anumite extensii de fișiere.
Analiză euristică	**Scanare ușoară**	Tehnologia a fost dezvoltată pentru detectarea amenințărilor care nu se pot detecta utilizând versiunea curentă a bazelor de date ale aplicației Kaspersky. Aceasta detectează fișiere care este posibil să fie infectate cu un virus necunoscut sau cu o variație nouă a unui virus cunoscut. Când scanează fișierele pentru codul rău intenționat, analizatorul euristic execută instrucțiunile din fișierele executabile. Numărul de instrucțiuni executate de analizorul euristic depinde de nivelul specificat pentru analizorul euristic. Nivelul analizei euristice asigură un echilibru între gradul de detaliere a căutării de amenințări noi, gradul de solicitare a resurselor sistemului de operare și durata analizei euristice.
Scanează numai fișierele noi și modificate	**Pornit**	Scanează numai fișierele noi și acele fișiere care au fost modificate de la ultima dată când au fost scanate. Acest lucru reduce durata unei scanări. Acest mod se aplică atât fișierelor simple, cât și celor compuse.
Folosește tehnologia iSwift	**Pornit**	Această tehnologie permite creșterea vitezei de scanare excluzând de la scanare anumite fișiere. Fișierele sunt excluse de la scanări utilizând un algoritm special care ia în considerare data lansării bazelor de date Kaspersky Endpoint Security, data celei mai recente scanări a fișierului și orice modificare adusă setărilor scanării. Tehnologia iSwift reprezintă o versiune îmbunătățită a tehnologiei iChecker și este destinată sistemului de fișiere NTFS.
Folosește tehnologia iChecker	**Pornit**	Această tehnologie permite creșterea vitezei de scanare excluzând de la scanare anumite fișiere. Fișierele sunt excluse de la scanări utilizând un algoritm special care ia în considerare data lansării bazelor de date Kaspersky Endpoint Security, data celei mai recente scanări a fișierului și orice modificare adusă setărilor scanării. Există limitări ale tehnologiei iChecker: aceasta nu funcționează în cazul fișierelor mari și se aplică numai la fișierele cu o structură pe care aplicația o recunoaște (de exemplu, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP și RAR).
Scanează fișierele în formate Microsoft Office	**Pornit**	Scanează fișierele Microsoft Office (DOC, DOCX, XLS, PPT și alte extensii Microsoft). Fișierele în format Office includ și obiecte OLE. Aplicația scanează fișierele în format office mai mici de 1 MO, indiferent dacă această casetă de selectare este bifată sau nu.
Scanează fișierele în format de e-mail	**Pornit**	Scanează fișiere în format de e-mail. Aplicația scanează fișierele MSG și EML. Fișierele în format de e-mail includ obiecte OLE și fișiere MHT. Kaspersky Endpoint Security scanează fișierele în format de e-mail mai mici de 1 MO, indiferent dacă această casetă de selectare este bifată sau nu.
Mod de scanare	**Mod inteligent**	În acest mod, componenta File Threat Protection scanează un obiect pe baza analizei operațiilor efectuate asupra obiectului. De exemplu, atunci când se lucrează cu un document Microsoft Office, Kaspersky Endpoint Security scanează fișierul la prima deschidere și la ultima închidere a acestuia. Operațiunile intermediare care suprascriu fișierul nu determină scanarea acestuia.
Acțiune la detectarea amenințării	**Dezinfectează; șterge dacă dezinfectarea nu reușește**	Dacă selectezi această opțiune, aplicația încearcă automat să dezinfecteze fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, aplicația șterge fișierul.

Punerea automată în pauză a componentei File Threat Protection

Poți configura componenta File Threat Protection astfel încât să treacă automat în pauză la o oră specificată sau atunci când lucrezi cu anumite aplicații.

Componenta File Threat Protection ar trebui să fie trecută în pauză numai atunci când intră în conflict cu alte aplicații. Dacă apar conflicte în timp ce o componentă rulează, vă recomandăm să contactați Suportul tehnic Kaspersky. Experții în asistență te vor ajuta să configurezi componenta File Threat Protection astfel încât să se execute simultan cu alte aplicații pe computerul tău.

Pentru a configura trecerea automată în pauză a componentei File Threat Protection:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **File Threat Protection**.
3. Fă clic pe **Setări avansate**.
4. În blocul **Pune în pauză File Threat Protection**, faceți clic pe linkul **Pune în pauză File Threat Protection**.
5. În fereastra care se deschide, configurați setările pentru punerea în pauză a componentei File Threat Protection:
   a. Configurați un program pentru întreruperea automată a File Threat Protection.
   b. Creați o listă de aplicații a căror funcționare ar trebui să întrerupă activitățile File Threat Protection.
6. Salvați-vă modificările.

Modificarea acțiunii efectuate asupra fișierelor infectate de către componenta File Threat Protection

În mod implicit, componenta File Threat Protection încearcă automat să dezinfecteze toate fișierele infectate detectate. Dacă dezinfectarea nu reușește, componenta File Threat Protection șterge aceste fișiere.

Pentru a modifica acțiunea efectuată asupra fișierelor infectate de către componenta File Threat Protection:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **File Threat Protection**.

3. În secțiunea **Acțiune la detectarea amenințării**, selectați opțiunea relevantă:

   - **Dezinfectează; șterge dacă dezinfectarea nu reușește**. Dacă selectezi această opțiune, aplicația încearcă automat să dezinfecteze fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, aplicația șterge fișierul.

   - **Dezinfectează; blochează dacă dezinfectarea nu reușește**. Dacă selectezi această opțiune, aplicația încearcă automat să dezinfecteze fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, aplicația blochează fișierul.

   - **Blochează**. Dacă este selectată această opțiune, aplicația blochează automat fișierul infectat fără a încerca să îl dezinfecteze sau să îl șteargă.

   Înainte de a încerca să dezinfectați sau să ștergeți un fișier infectat, aplicația creează o copie de rezervă a fișierului în cazul în care trebuie să restaurați fișierul sau dacă acesta poate fi dezinfectat în viitor.

4. Salvați-vă modificările.

Specificarea domeniului de protecție al componentei File Threat Protection

Domeniul de protecție desemnează obiectele pe care componenta le scanează atunci când este activată. Proprietățile domeniilor de protecție diferă de la o componentă la alta. Locațiile și tipurile de fișiere care urmează a fi scanate reprezintă proprietățile domeniului de protecție al componentei File Threat Protection. În mod implicit, componenta File Threat Protection scanează numai fișierele potențial infectabile care sunt executate de pe unități de hard disk, unități amovibile și unități de rețea.

Când selectezi tipurile de fișiere de scanat, ia în calcul următoarele:

1. Există o probabilitatea redusă de introducere a codului periculos în fișiere cu anumite formate și în activitatea lor ulterioară (de exemplu, format TXT). În același timp, există formate de fișiere care conțin un cod executabil (precum .exe, .dll). Codul executabil poate fi inclus, de asemenea, în fișiere cu formate care nu sunt destinate acestui scop (de exemplu, formatul DOC). Riscul de pătrundere și de activare a codului rău intenționat în astfel de fișiere este ridicat.

2. Un intrus poate trimite pe computerul tău un virus sau o altă aplicație rău intenționată într-un fișier executabil care a fost redenumit cu extensia .txt. Dacă selectezi scanarea fișierelor după extensie, aplicația omite acest fișiere în cursul scanării. Dacă este selectată scanarea fișierelor după format, Kaspersky Endpoint Security analizează antetul fișierului indiferent de extensie. Dacă această analiză arată că fișierul are formatul unui fișier executabil (de exemplu, EXE), aplicația îl scanează.

Pentru a crea domeniul de protecție:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **File Threat Protection**.

3. Fă clic pe **Setări avansate**.

4. În blocul **Tipuri de fișiere**, specifică tipurile de fișiere pe care dorești să le scaneze componenta File Threat Protection:

   - **Toate fișierele**. Dacă se activează această setare, Kaspersky Endpoint Security verifică toate fișierele, fără excepție (toate formatele și toate extensiile).
   - **Fișiere scanate după format**. Dacă se activează această setare, aplicația scanează numai fișierele infectabile. Înainte de scanarea unui fișier pentru detectarea de cod rău intenționat, se analizează antetul intern al fișierului pentru a se determina formatul fișierului (de exemplu, .txt, .doc sau .exe). De asemenea, scanarea caută fișiere cu anumite extensii de fișiere.
   - **Fișiere scanate după extensie**. Dacă se activează această setare, aplicația scanează numai fișierele infectabile. Formatul fișierului se determină în funcție de extensia sa.

5. Faceți clic pe linkul **Editează domeniul de protecție**.

6. În fereastra care se deschide, selectează obiectele pe care dorești să le adaugi la domeniul de protecție sau să le excluzi din acesta.

   Nu puteți șterge sau edita obiecte care sunt incluse în domeniul de protecție implicit.

7. Dacă doriți să adăugați un obiect nou la domeniul de protecție:

   a. Fă clic pe **Adaugă**.

      Se deschide arborele de directoare.

   b. În câmpul **Cale**, introduceți calea către director sau fișier.

      Folosiți măști:

      - Caracterul `*` (asterisc) ține locul oricărui set de caractere, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\*\*.txt` va include toate căile către fișierele cu extensia TXT din directoarele de pe unitatea C:, dar nu și din subdirectoare.
      - Două caractere `*` consecutive țin locul oricărui set de caractere (inclusiv un set gol) din numele de fișier sau director, inclusiv caracterele `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\**\*.txt` va include toate căile către fișierele cu extensia TXT localizată în directoarele imbricate în `Folder`, cu excepția `Folder` în sine. Masca trebuie să includă cel puțin un nivel de imbricare. Masca `C:\**\*.txt` nu este o mască validă.
      - `?` (semn de întrebare) ține locul oricărui caracter individual, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\???.txt` va include căi pentru toate fișierele din directorul denumit `Folder` care au extensia TXT și un nume format din trei caractere.

      Puteți utiliza măști oriunde într-o cale de fișier sau director. De exemplu, dacă doriți ca domeniul de scanare să includă directorul Descărcări pentru toate conturile de utilizator de pe computer, introduceți masca `C:\Users\*\Downloads\`.

      Obiectul **Acest PC** din lista de resurse de fișiere a computerului include următoarele obiecte: **Toate unitățile de hard disk**, **Toate unitățile de rețea** și **Toate unitățile amovibile**.

   Puteți exclude un obiect din scanări fără a-l șterge din lista de obiecte din domeniul de scanare. Pentru aceasta, debifați caseta de selectare de lângă obiect.

8. Salvați-vă modificările.

Utilizarea metodelor de scanare

Kaspersky Endpoint Security folosește o tehnică de scanare denumită tehnologia Machine learning și analiza semnăturilor. La analiza semnăturii, Kaspersky Endpoint Security compară obiectul detectat cu înregistrările din bazele sale de date. În urma recomandărilor experților Kaspersky, tehnologia Machine learning și analiza semnăturilor este activată în permanență.

Pentru a spori eficiența protecției, poți utiliza analiza euristică. Când scanează fișierele pentru codul rău intenționat, analizatorul euristic execută instrucțiunile din fișierele executabile. Numărul de instrucțiuni executate de analizorul euristic depinde de nivelul specificat pentru analizorul euristic. Nivelul analizei euristice asigură un echilibru între gradul de detaliere a căutării de amenințări noi, gradul de solicitare a resurselor sistemului de operare și durata analizei euristice.

Pentru a configura folosirea analizei euristice în funcționarea componentei File Threat Protection:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **File Threat Protection**.
3. Fă clic pe **Setări avansate**.
4. Dacă doriți ca aplicația să utilizeze analiza euristică pentru protecția împotriva amenințărilor de fișiere, bifați caseta de selectare **Analiză euristică** din blocul **Metode de scanare**. Apoi utilizați glisorul pentru a seta nivelul analizei euristice: **Scanare ușoară**, **Scanare medie** sau **Scanare profundă**.
5. Salvați-vă modificările.

Folosirea tehnologiilor de scanare în funcționarea componentei File Threat Protection

Pentru a configura utilizarea tehnologiilor de scanare la funcționarea componentei File Threat Protection:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **File Threat Protection**.
3. Fă clic pe **Setări avansate**.

4. În blocul **Tehnologii de scanare**, bifați casetele de selectare de lângă numele tehnologiilor care doriți să fie utilizate pentru File Threat Protection:

   - **Folosește tehnologia iSwift**. Această tehnologie permite creșterea vitezei de scanare excluzând de la scanare anumite fișiere. Fișierele sunt excluse de la scanări utilizând un algoritm special care ia în considerare data lansării bazelor de date Kaspersky Endpoint Security, data celei mai recente scanări a fișierului și orice modificare adusă setărilor scanării. Tehnologia iSwift reprezintă o versiune îmbunătățită a tehnologiei iChecker și este destinată sistemului de fișiere NTFS.

   - **Folosește tehnologia iChecker**. Această tehnologie permite creșterea vitezei de scanare excluzând de la scanare anumite fișiere. Fișierele sunt excluse de la scanări utilizând un algoritm special care ia în considerare data lansării bazelor de date Kaspersky Endpoint Security, data celei mai recente scanări a fișierului și orice modificare adusă setărilor scanării. Există limitări ale tehnologiei iChecker: aceasta nu funcționează în cazul fișierelor mari și se aplică numai la fișierele cu o structură pe care aplicația o recunoaște (de exemplu, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP și RAR).

5. Salvați-vă modificările.

Optimizarea scanării de fișiere

Poți optimiza scanarea de fișiere efectuată de componenta File Threat Protection, reducând astfel durata de scanare și mărind viteza de funcționare a aplicației Kaspersky Endpoint Security. Acest lucru se obține prin scanarea numai a fișierelor noi și a celor care au fost modificate din momentul scanării ulterioare. Acest mod se aplică atât fișierelor simple, cât și celor compuse.

De asemenea, puteți activa utilizarea tehnologiilor iChecker și iSwift, care optimizează viteza de scanare a fișierelor excluzând fișierele care nu au fost modificate din momentul celei mai recente scanări.

Pentru a optimiza scanarea de fișiere:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **File Threat Protection**.

3. Fă clic pe **Setări avansate**.

4. În blocul **Optimizare**, bifați caseta de selectare **Scanează numai fișierele noi și modificate**.

5. Salvați-vă modificările.

Scanarea fișierelor compuse

O tehnică obișnuită de ascundere a virușilor și a altor programe malware o reprezintă introducerea acestora în fișiere compuse, precum arhive sau baze de date. Pentru a detecta virușii și celelalte programe malware ascunse în acest mod, fișierul compus trebuie dezarhivat, fapt care poate încetini scanarea. Poți limita tipurile de fișiere compuse de scanat, accelerând astfel scanarea.

Metoda folosită pentru procesarea unul fișier compus infectat (dezinfectare sau ștergere) depinde de tipul de fișier.

Componenta File Threat Protection dezinfectează fișiere compuse în formatele ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR și ICE și șterge fișierele în toate celelalte formate (exceptând bazele de date de e-mail).

Pentru a configura scanarea fișierelor compuse:

1. În fereastra principală a aplicației, faceți clic pe butonul .
2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **File Threat Protection**.
3. Fă clic pe **Setări avansate**.
4. În blocul **Scanarea fișierelor compuse**, specificați tipurile de fișiere compuse pe care doriți să le scanați: arhive, pachete de distribuție, fișiere în format de mail sau office.
5. Dacă scanarea numai a fișierelor noi și modificate este dezactivată, configurați setările pentru scanarea fiecărui tip de fișier compus: scanați toate fișierele de acest tip sau numai fișierele noi.

   Dacă scanarea numai a fișierelor noi și modificate este activată, Kaspersky Endpoint Security scanează numai fișierele noi și modificate ale tuturor tipurilor de fișiere compuse.
6. Configurați setările avansate pentru scanarea fișierelor compuse.

   - **Nu dezarhiva fișierele compuse mari**.

     Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security nu scanează fișierele compuse a căror dimensiune depășește valoarea specificată.

     În cazul în care această casetă de selectare este nebifată, Kaspersky Endpoint Security scanează fișierele compuse indiferent de dimensiuni.

     Kaspersky Endpoint Security scanează fișierele de dimensiuni mari extrase din arhive indiferent dacă este bifată sau nu caseta de selectare **Nu dezarhiva fișierele compuse mari**.

   - **Dezarhivează fișierele compuse în fundal**.

     În cazul în care caseta de selectare este selectată, Kaspersky Endpoint Security asigură acces la fișierele compuse care sunt mai mari decât valoarea specificată înainte de scanarea acestor fișiere. În acest caz, Kaspersky Endpoint Security despachetează și scanează fișierele compuse în fundal.

     Kaspersky Endpoint Security asigură acces la fișierele compuse care sunt mai mici decât această valoare doar după despachetarea și scanarea acestor fișiere.

În cazul în care caseta de selectare nu este selectată, Kaspersky Endpoint Security asigură acces la fișierele compuse numai după despachetarea și scanarea fișierelor de orice dimensiune.

7. Salvați-vă modificările.

Schimbarea modului de scanare

Secțiunea *Mod de scanare* se referă la condiția care declanșează scanarea fișierelor de către componenta File Threat Protection. În mod implicit, Kaspersky Endpoint Security scanează fișierele în modul inteligent. În acest mod de scanare a fișierelor, componenta File Threat Protection decide dacă scanează sau nu fișierele în urma operațiunilor de analiză a fișierelor efectuate de utilizator, de o aplicație desemnată de utilizator (din contul utilizat pentru Log in sau dintr-un alt cont de utilizator) sau de sistemul de operare. De exemplu, atunci când se lucrează cu un document Microsoft Office Word, Kaspersky Endpoint Security scanează fișierul la prima deschidere și la ultima închidere a acestuia. Operațiunile intermediare care suprascriu fișierul nu determină scanarea acestuia.

Pentru a schimba modul de scanare a fișierelor:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Essential Threat Protection → File Threat Protection**.
3. Fă clic pe **Setări avansate**.
4. În blocul **Mod de scanare**, selectați modul necesar:
   - **Mod inteligent**. În acest mod, componenta File Threat Protection scanează un obiect pe baza analizei operațiilor efectuate asupra obiectului. De exemplu, atunci când se lucrează cu un document Microsoft Office, Kaspersky Endpoint Security scanează fișierul la prima deschidere și la ultima închidere a acestuia. Operațiunile intermediare care suprascriu fișierul nu determină scanarea acestuia.
   - **La accesare și modificare**. În acest mod, componenta File Threat Protection scanează obiecte la fiecare încercare de deschidere sau modificare a acestora.
   - **La accesare**. În acest mod, File Threat Protection scanează obiecte doar la o încercare de deschidere/modificare a acestora.
   - **La executare**. În acest mod, File Threat Protection scanează obiecte numai la o încercare de executare a acestora.
5. Salvați-vă modificările.

Scanare containere

Un *container* este un mediu izolat în care o aplicație se poate executa fără a interacționa direct cu sistemul de operare. Utilizarea containerelor implică următoarele riscuri:

- Hackerii pot să exploateze vulnerabilitățile containerizării pentru a compromite aplicațiile din interiorul containerului.
- Hackerii pot exploata o configurație nesigură a mediului containerului, pentru a obține acces neautorizat la datele de pe computer sau pentru a compromite integritatea sistemului.

- Un atac reușit asupra unui container poate permite unui hacker să obțină acces la datele de pe computer.
- Hackerii pot exploata vulnerabilitățile rețelei pentru a intercepta traficul de rețea.

Kaspersky Endpoint Security scanează fișierele nu doar de pe discuri, ci și din interiorul containerelor. Adică, Kaspersky Endpoint Security este un instrument extern pentru detectarea activităților rău intenționate în interiorul containerelor. Acest lucru permite menținerea performanței containerelor și previne conflictele cu alte aplicații din interiorul containerului. Instalarea Kaspersky Endpoint Security în interiorul containerului nu este acceptată.

Pe lângă asigurarea securității containerelor, Kaspersky Endpoint Security permite gestionarea aplicațiilor din interiorul containerelor folosind Application Control. Componenta Application Control este configurată pentru containere în același mod ca și pentru aplicațiile instalate pe computer. Monitorizare integritate sistem acceptă și containere.

Cerințe pentru containere

- Containerul trebuie să fie un container Docker. Alte instrumente de containerizare nu sunt acceptate.
- Containerul trebuie să se execute în modul de izolare a procesului. Modul de izolare Hyper-V nu este acceptat.
- Containerul trebuie plasat pe un server Windows Server 2016, 2019 sau 2022 (Docker Host).
- Containerul trebuie să includă o imagine Windows (Docker Image). Windows 10 și 11 nu sunt acceptate. Imaginile Linux nu sunt acceptate.

Acțiune la detectarea amenințării

Dacă o amenințare este detectată în interiorul unui container, aplicația aplică acțiunea selectată pentru componenta File Threat Protection. Scanare containere are setări suplimentare (consultă instrucțiunile de mai jos). Dacă este detectată o amenințare, aplicația blochează activitatea rău intenționată și efectuează acțiunea selectată (de exemplu, încearcă să dezinfecteze obiectul). Kaspersky Endpoint Security poate opri containerul dacă obiectul detectat nu poate fi dezinfectat. În mod implicit, funcționalitatea de oprire a containerului este dezactivată.

Cum se configurează scanarea containerelor în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Essential Threat Protection** → **File Threat Protection**.
4. Fă clic pe **Setări**.
5. Se deschide o fereastră; în acea fereastră, selectați fila **Suplimentar**.

6. În blocul **Scanarea operațiunilor cu fișiere executate în containerele Windows**, configurează setările de scanare a containerelor:

   - **Oprește containerul dacă dezinfectarea eșuează**. Este posibil ca aplicația să nu aibă suficiente drepturi de citire și scriere pentru obiectul detectat. În acest caz, dezinfectarea sau ștergerea obiectului detectat este imposibilă. Dacă această casetă de selectare este bifată, aplicația blochează obiectul detectat și oprește containerul. Dacă această casetă de selectare este debifată, aplicația blochează doar obiectul detectat.

   - **Nu scana operațiunile cu fișiere executate în containerele Windows**. Dacă această casetă de selectare este bifată, aplicația scanează containerul numai la pornirea acestuia. Dacă această casetă de selectare este debifată, aplicația scanează continuu containerul în timp real.

7. Salvați-vă modificările.

Cum se configurează scaarea containerelor în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesează **Host Threat Protection** → **File Threat Protection**.

5. În **Advanced settings**, selectează fila **Performance**.

6. În blocul **Scan optimization**, configurează setările de scanare a containerelor:

   - **Stop container if disinfection fails**. Este posibil ca aplicația să nu aibă suficiente drepturi de citire și scriere pentru obiectul detectat. În acest caz, dezinfectarea sau ștergerea obiectului detectat este imposibilă. Dacă această casetă de selectare este bifată, aplicația blochează obiectul detectat și oprește containerul. Dacă această casetă de selectare este debifată, aplicația blochează doar obiectul detectat.

   - **Do not scan file operations executed in Windows containers**. Dacă această casetă de selectare este bifată, aplicația scanează containerul numai la pornirea acestuia. Dacă această casetă de selectare este debifată, aplicația scanează continuu containerul în timp real.

7. Salvați-vă modificările.

Cum se configurează scanarea containerelor în interfața aplicației.

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **File Threat Protection**.

3. În blocul **Scanarea operațiunilor cu fișiere executate în containerele Windows**, configurează setările de scanare a containerelor:

   - **Oprește containerul dacă dezinfectarea eșuează**. Este posibil ca aplicația să nu aibă suficiente drepturi de citire și scriere pentru obiectul detectat. În acest caz, dezinfectarea sau ștergerea obiectului detectat este imposibilă. Dacă această casetă de selectare este bifată, aplicația blochează obiectul detectat și oprește containerul. Dacă această casetă de selectare este debifată, aplicația blochează doar obiectul detectat.

   - **Nu scana operațiunile cu fișiere executate în containerele Windows**. Dacă această casetă de selectare este bifată, aplicația scanează containerul numai la pornirea acestuia. Dacă această casetă de selectare este debifată, aplicația scanează continuu containerul în timp real.

4. Salvați-vă modificările.

Host Intrusion Prevention

Această componentă este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Windows pentru stații de lucru. Această componentă nu este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Windows pentru servere.

Componenta Host Intrusion Prevention împiedică aplicațiile să execute acțiuni care ar putea fi periculoase pentru sistemul de operare și asigură controlul accesului la resursele sistemului de operare și la datele personale. Componenta oferă protecție computerului cu ajutorul bazelor de date antivirus și a serviciului cloud Kaspersky Security Network.

Componenta controlează funcționarea aplicațiilor folosind *drepturi de aplicație*. Drepturile de aplicație includ următorii parametri de acces:

- Acces la resursele sistemului de operare (de exemplu, opțiuni de pornire automată, chei de registru)
- Acces la date cu caracter personal (de exemplu, fișiere și aplicații)

Activitatea în rețea a aplicațiilor este controlată de componenta Firewall folosind *regulile de rețea*.

În timpul primei porniri a aplicației, componenta Host Intrusion Prevention realizează următoarele acțiuni:

1. Verifică securitatea aplicației folosind bazele de date antivirus descărcate.
2. Verifică securitatea aplicației în Kaspersky Security Network.

   Vă recomandăm să participați în Kaspersky Security Network pentru a ajuta componenta Host Intrusion Prevention să funcționeze mai eficient.

3. Pune aplicația într-unul dintre grupurile de încredere: *De încredere*, *Restricționat la nivel inferior*, *Restricționat la nivel superior*, *Nu este de încredere*.

   Un grup de încredere definește drepturile la care se referă Kaspersky Endpoint Security atunci când controlează activitatea aplicațiilor. Kaspersky Endpoint Security plasează o aplicație într-un grup de încredere în funcție de nivelul de pericol pe care îl poate prezenta această aplicație pentru computer.

Kaspersky Endpoint Security plasează o aplicație într-un grup de încredere pentru componentele Firewall și Host Intrusion Prevention. Nu poți schimba grupul de încredere numai pentru componentele Firewall sau Host Intrusion Prevention.

Dacă ați refuzat să participați la KSN sau nu există o rețea, Kaspersky Endpoint Security plasează aplicația într-un grup de încredere, în funcție de setările componentei Host Intrusion Prevention. După primirea reputației aplicației de la KSN, grupul de încredere poate fi schimbat automat.

4. Blochează acțiunile aplicației în funcție de grupul de încredere. De exemplu, aplicațiilor din grupul de încredere *Restricționat la nivel superior* le este refuzat accesul la modulele sistemului de operare.

La următoarea pornire a aplicației, Kaspersky Endpoint Security verifică integritatea aplicației. Dacă aplicația este nemodificată, componenta folosește pentru aceasta drepturile curente pentru aplicații. Dacă aplicația a fost modificată, Kaspersky Endpoint Security analizează aplicația ca și cum ar fi fost pornită pentru prima dată.

Activarea și dezactivarea componentei Host Intrusion Prevention

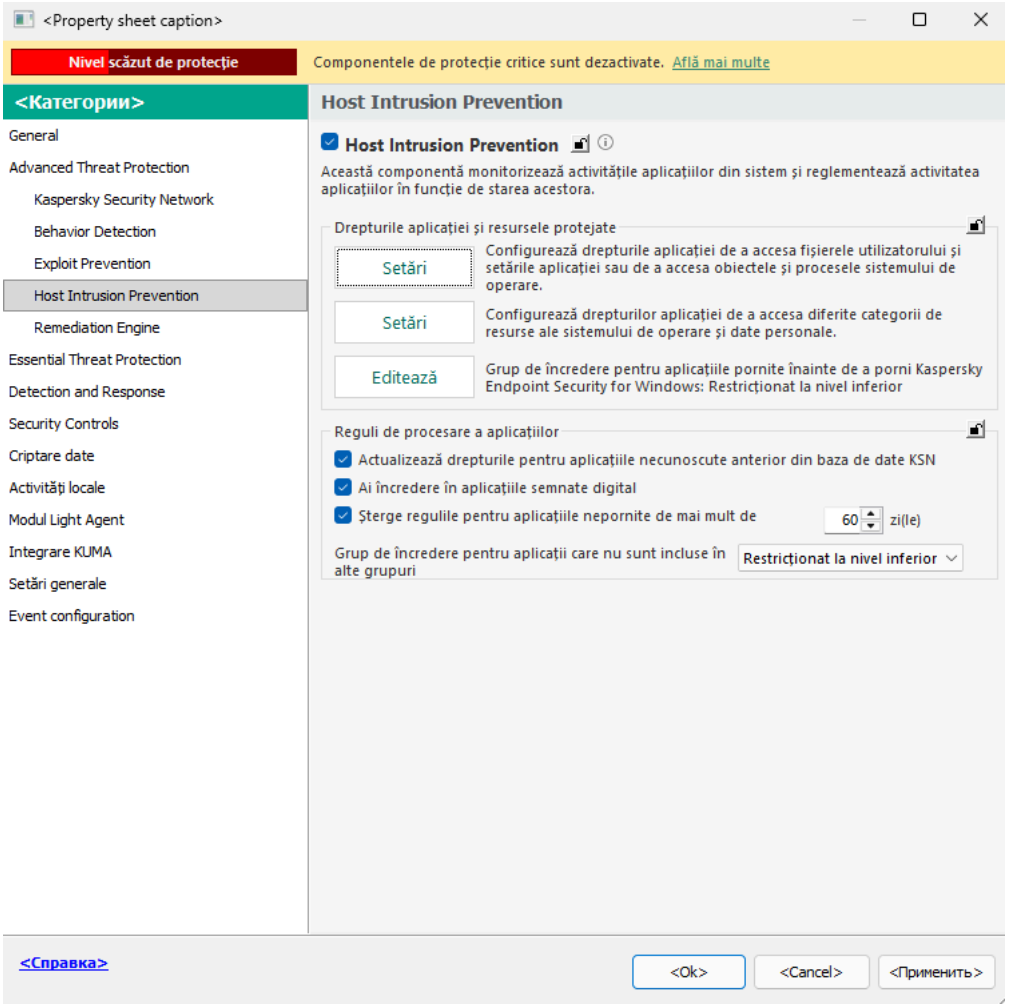
În mod implicit, componenta Host Intrusion Prevention este activată și se execută în modul recomandat de experții Kaspersky.

Cum se activează sau dezactivează componenta Host Intrusion Prevention în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.

2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

3. În fereastra politicii, selectați **Advanced Threat Protection → Host Intrusion Prevention**.



Setări Intrusion Prevention

4. Utilizează caseta de selectare **Host Intrusion Prevention** pentru a activa sau a dezactiva componenta.

5. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se activează sau dezactivează componenta Host Intrusion Prevention în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management → Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.
   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **Host Threat Protection → Host Intrusion Prevention**.

5. Utilizați comutatorul **Host Intrusion Prevention ENABLED** pentru a activa sau a dezactiva componenta.

6. Salvați-vă modificările.

Cum se activează sau dezactivează componenta Host Intrusion Prevention în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Advanced Threat Protection → Host Intrusion Prevention**.

3. Utilizați comutatorul **Host Intrusion Prevention** pentru a activa sau a dezactiva componenta.

4. Salvați-vă modificările.

În cazul în care componenta Host Intrusion Prevention este activată, Kaspersky Endpoint Security va plasa o aplicație într-un grup de încredere în funcție de nivelul de pericol pe care îl poate prezenta această aplicație pentru computer. Kaspersky Endpoint Security va bloca apoi acțiunile aplicației în funcție de grupul de încredere.

Administrarea grupurilor de încredere pentru aplicații

Atunci când o aplicație este pornită pentru prima dată, componenta Host Intrusion Prevention verifică securitatea aplicației și plasează aplicația într-unul dintre grupurile de încredere.

În prima etapă a scanării aplicației, Kaspersky Endpoint Security caută în baza de date internă de aplicații cunoscute o intrare corespunzătoare și, în același timp, trimite o solicitare către baza de date Kaspersky Security Network (dacă este disponibilă o conexiune la Internet). Pe baza rezultatelor căutării în baza de date internă și în baza de date Kaspersky Security Network, aplicația este plasată într-un grup de încredere. De fiecare dată când aplicația este repornită, Kaspersky Endpoint Security trimite o solicitare nouă către baza de date KSN și plasează aplicația într-un grup de încredere diferit, dacă reputația aplicației în baza de date KSN s-a modificat.

Poți selecta un grup de încredere în care dorești ca Kaspersky Endpoint Security să plaseze automat toate aplicațiile necunoscute. Aplicațiile care se executau înainte de a porni Kaspersky Endpoint Security sunt plasate automat în grupul de încredere. setat în setările componentei Host Intrusion Prevention.

Pentru aplicațiile care au fost pornite înainte de Kaspersky Endpoint Security, este controlată numai activitatea de rețea. Controlul se realizează conform regulilor de rețea definite în setările Firewall.

Modificarea grupului de încredere al unei aplicații

Atunci când o aplicație este pornită pentru prima dată, componenta Host Intrusion Prevention verifică securitatea aplicației și plasează aplicația într-unul dintre grupurile de încredere.

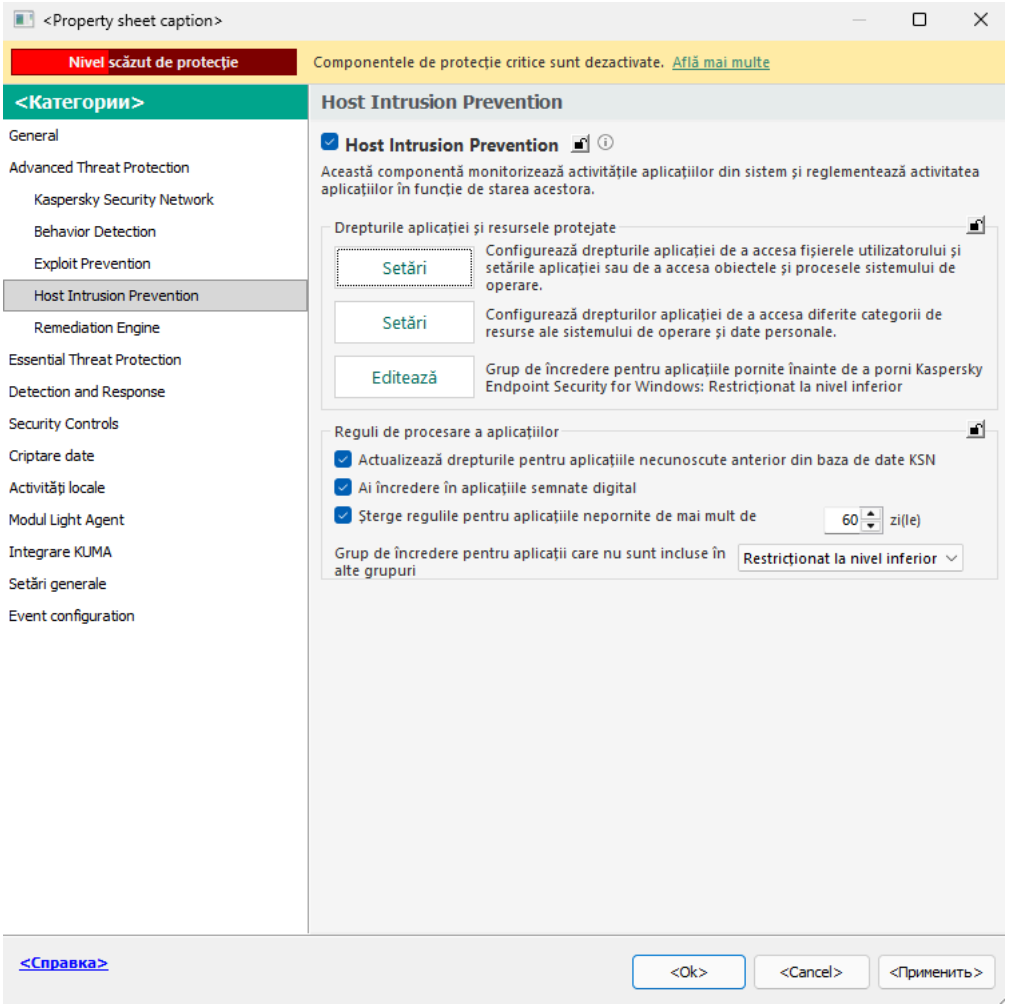
Specialiștii de la Kaspersky nu recomandă mutarea de aplicații din grupul de încredere atribuit în alt grup de încredere. În schimb, dacă este necesar, poți modifica drepturi pentru o aplicație individuală.

Cum se modifică grupul de încredere al unei aplicații în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.

2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

3. În fereastra politicii, selectați **Advanced Threat Protection → Host Intrusion Prevention**.



Setări Intrusion Prevention

4. În blocul **Drepturile aplicației și resursele protejate**, fă clic pe butonul **Setări**.

   Tastfel se deschide fereastra de configurare a drepturilor aplicațiilor și lista resurselor protejate.

5. Selectați fila **Drepturi aplicație**.

6. Fă clic pe **Adaugă**.

7. În fereastra care se deschide, introduceți criteriul de căutare pentru aplicația a cărui grup de încredere doriți să îl modificați.

   Puteți introduce numele aplicației sau numele producătorului. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști.

8. Fă clic pe **Împrospătează**.

   Kaspersky Endpoint Security va căuta aplicația în lista consolidată de aplicații instalate pe computerele gestionate. Kaspersky Endpoint Security va afișa o listă cu aplicațiile care satisfac criteriul dvs. de căutare.

9. Selectați aplicația necesară.

10. În lista verticală **Adaugă aplicații selectate la grupul de încredere**, selectați grupul de încredere necesar pentru aplicație.

11. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se modifică grupul de încredere al unei aplicații în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Host Threat Protection** → **Host Intrusion Prevention**.
5. În blocul **Application rights and protected resources**, faceți clic pe linkul **Application rights and protected resources**.

   Tastfel se deschide fereastra de configurare a drepturilor aplicațiilor și lista resurselor protejate.
6. Selectați fila **Application rights**.

   Veți vedea o listă cu grupurile de încredere în partea stângă a ferestrei, iar proprietățile acestora în partea dreaptă.
7. Fă clic pe **Add**.

   Aceasta pornește Expertul pentru adăugarea unei aplicații la un grup de încredere.
8. Selectați grupul de încredere relevant pentru aplicație.
9. Selectați **Application**. Mergeți la pasul următor.

   Dacă doriți să modificați grupul de încredere pentru mai multe aplicații, selectați **Group** și definiți un nume pentru grupul de aplicații.
10. În lista de aplicații deschisă, selectați aplicațiile al căror grup de încredere doriți să modificați.

    Utilizați un filtru. Puteți introduce numele aplicației sau numele producătorului. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști.
11. Ieșiți din Expert.

    Aplicația va fi adăugată în grupul de încredere.
12. Salvați-vă modificările.

Cum se modifică grupul de încredere al unei aplicații în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Advanced Threat Protection** → **Host Intrusion Prevention**.
3. Fă clic pe **Gestionează aplicațiile**.

   Acest lucru va deschide lista aplicațiilor instalate.
4. Selectați aplicația necesară.
5. În meniul contextual al aplicației, selectați **Restricții** → **<grup de încredere>**.
6. Salvați-vă modificările.

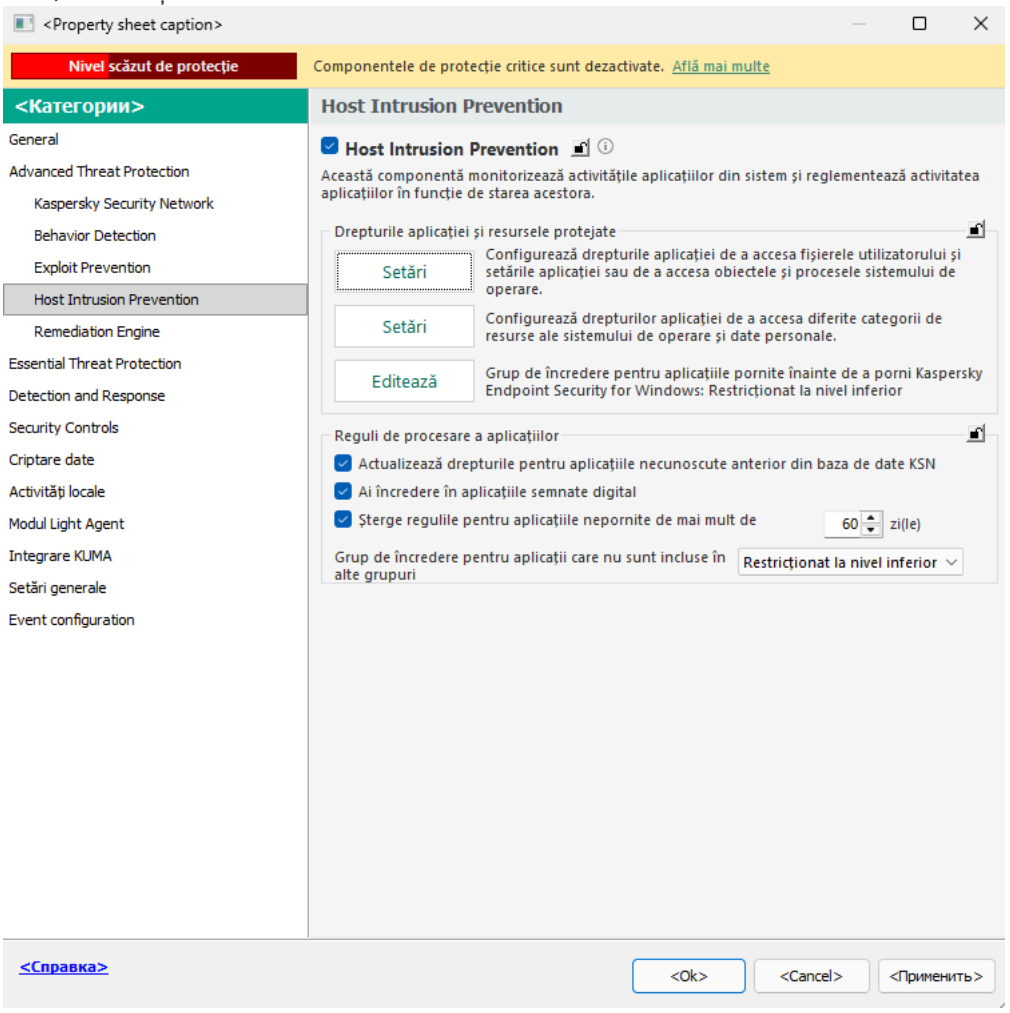
Ca rezultat, aplicația va fi introdusă în celălalt grup de încredere. Kaspersky Endpoint Security va bloca apoi acțiunile aplicației în funcție de grupul de încredere. Starea *(definit de utilizator)* va fi atribuită aplicației. Dacă reputația aplicația este modificată în Kaspersky Security Network, componenta Host Intrusion Prevention va lăsa grupul de încredere al acestei aplicații nemodificat.

Configurarea drepturilor grupului de încredere

Drepturi optime ale aplicației sunt create, în mod implicit, pentru diferite grupuri de încredere. Setările de drepturi pentru grupurile de aplicații dintr-un grup de încredere moștenesc valori din setările drepturilor grupului de încredere.

Cum se modifică drepturile grupului de încredere în Consola de administrare (MMC).

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Advanced Threat Protection → Host Intrusion Prevention**.



Setări Intrusion Prevention

4. În blocul **Drepturile aplicației și resursele protejate**, fă clic pe butonul **Setări**.

   Tastfel se deschide fereastra de configurare a drepturilor aplicațiilor și lista resurselor protejate.
5. Accesați fila **Drepturi aplicație**.
6. Selectați grupul de încredere necesar.

7. În meniul contextual al grupului de încredere, selectați **Drepturi pentru grup**.

   Aceasta deschide proprietățile grupului de încredere.

8. Efectuează una dintre următoarele acțiuni:

   - Dacă doriți să editați drepturile grupului de încredere care reglementează operațiile cu registry-ul sistemului de operare, fișierele utilizatorului și setările aplicațiilor, selectați **Fișiere și registry de sistem**.
   - Dacă doriți să editați drepturile grupului de încredere care reglementează accesul la procesele și obiectele sistemului de operare, selectați **Drepturi**.

   > Activitatea în rețea a aplicațiilor este controlată de componenta Firewall folosind *regulile de rețea*.

9. Pentru resursa relevantă, în coloana acțiunii corespunzătoare, faceți clic dreapta pentru a se deschide meniul contextual și selectați opțiunea necesară: **Moștenește**, **Permite** (✓) sau **Blochează** (⊘).

10. Dacă doriți să monitorizați utilizarea resurselor computerului, selectați **Înregistrează evenimentele în jurnal** (✓ / ⊘).

    Kaspersky Endpoint Security va înregistra informațiile despre funcționarea componentei Host Intrusion Prevention. Rapoartele conțin informații despre operațiile efectuate de aplicație cu resursele computerului (permise sau interzise). Rapoartele conțin, de asemenea, informații despre aplicațiile care utilizează fiecare resursă.

11. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se modifică drepturile grupului de încredere în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.
4. Accesați **Host Threat Protection** → **Host Intrusion Prevention**.
5. În blocul **Application rights and protected resources**, faceți clic pe linkul **Application rights and protected resources**.

   Tastfel se deschide fereastra de configurare a drepturilor aplicațiilor și lista resurselor protejate.

6. Accesați fila **Application rights**.

   Veți vedea o listă cu grupurile de încredere în partea stângă a ferestrei, iar proprietățile acestora în partea dreaptă.

7. În partea stângă a ferestrei, selectați grupul de încredere relevant.
8. În partea dreaptă a ferestrei, în lista verticală, efectuați una dintre următoarele acțiuni:

   - Dacă doriți să editați drepturile grupului de încredere care reglementează operațiile cu registry-ul sistemului de operare, fișierele utilizatorului și setările aplicațiilor, selectați **Files and system registry**.
   - Dacă doriți să editați drepturile grupului de încredere care reglementează accesul la procesele și obiectele sistemului de operare, selectați **Rights**.

Activitatea în rețea a aplicațiilor este controlată de componenta Firewall folosind *regulile de rețea*.

9. Pentru resursa relevantă, în coloana acțiunii corespunzătoare, selectați opțiunea necesară: **Inherit**, **Allow** (), **Block** ().

10. Dacă doriți să monitorizați utilizarea resurselor computerului, selectați **Log events** (/).

    Kaspersky Endpoint Security va înregistra informațiile despre funcționarea componentei Host Intrusion Prevention. Rapoartele conțin informații despre operațiile efectuate de aplicație cu resursele computerului (permise sau interzise). Rapoartele conțin, de asemenea, informații despre aplicațiile care utilizează fiecare resursă.

11. Salvați-vă modificările.

Cum se modifică drepturile grupului de încredere în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul .

2. În fereastra cu setările aplicației, selectați **Advanced Threat Protection** → **Host Intrusion Prevention**.

3. Fă clic pe **Gestionează aplicațiile**.

   Acest lucru va deschide lista aplicațiilor instalate.

4. Selectați grupul de încredere necesar.

5. În meniul contextual al grupului de încredere, selectați **Detalii și reguli**.

   Aceasta deschide proprietățile grupului de încredere.

6. Efectuează una dintre următoarele acțiuni:

   - Dacă doriți să editați drepturile grupului de încredere care reglementează operațiile cu registry-ul sistemului de operare, fișierele utilizatorului și setările aplicațiilor, selectați **Fișiere și registry de sistem**.
   - Dacă doriți să editați drepturile grupului de încredere care reglementează accesul la procesele și obiectele sistemului de operare, selectați **Drepturi**.

Activitatea în rețea a aplicațiilor este controlată de componenta Firewall folosind *regulile de rețea*.

7. Pentru resursa relevantă, în coloana acțiunii corespunzătoare, faceți clic dreapta pentru a se deschide meniul contextual și selectați opțiunea necesară: **Moștenește**, **Permite** () sau **Refuză** ().

8. Dacă doriți să monitorizați utilizarea resurselor computerului, selectați **Înregistrează evenimentele în jurnal** ().

   Kaspersky Endpoint Security va înregistra informațiile despre funcționarea componentei Host Intrusion Prevention. Rapoartele conțin informații despre operațiile efectuate de aplicație cu resursele computerului (permise sau interzise). Rapoartele conțin, de asemenea, informații despre aplicațiile care utilizează fiecare resursă.

9. Salvați-vă modificările.

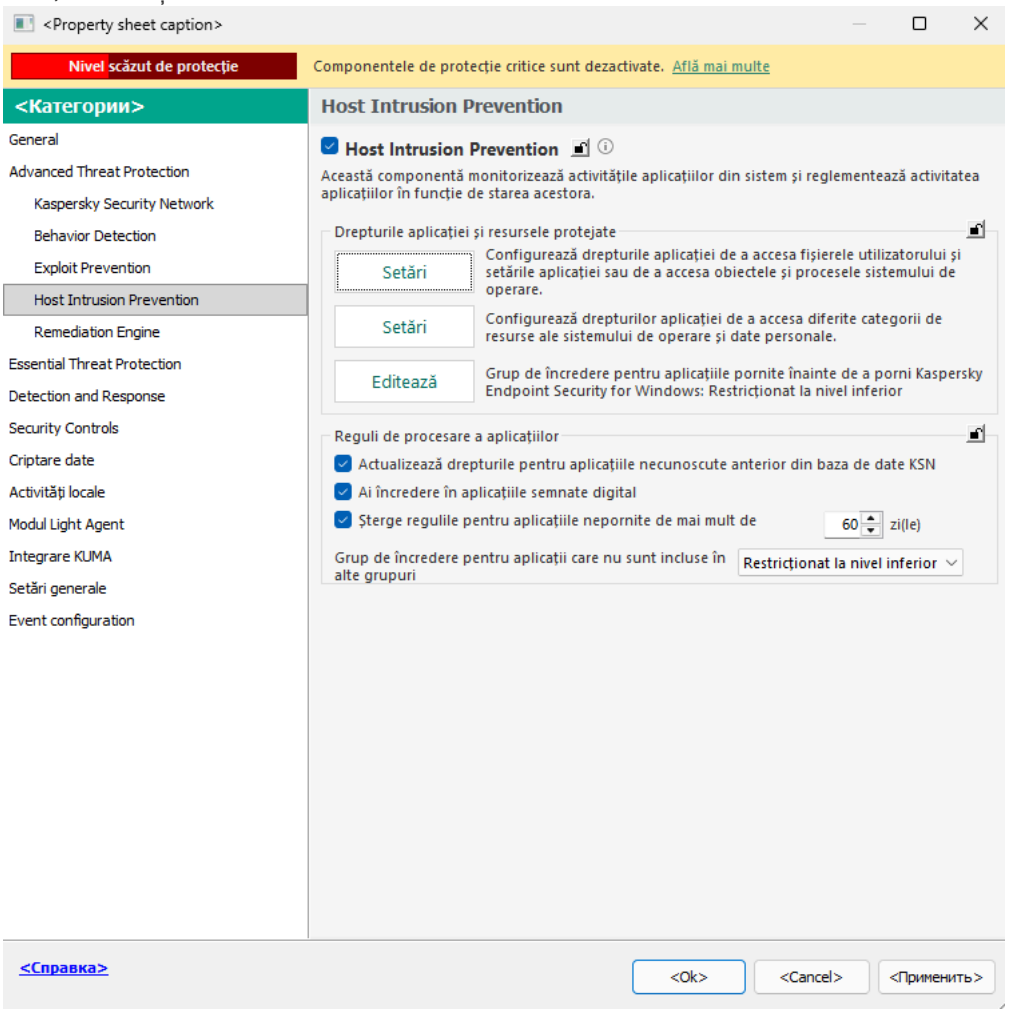
Drepturile grupului de încredere vor fi modificate. Kaspersky Endpoint Security va bloca apoi acțiunile aplicației în funcție de grupul de încredere. Starea (*Setări personalizate*) va fi alocată grupului de încredere.

Selectarea unui grup de încredere pentru aplicații lansate înainte de Kaspersky Endpoint Security

Pentru aplicațiile care au fost pornite înainte de Kaspersky Endpoint Security, este controlată numai activitatea de rețea. Controlul se realizează conform regulilor de rețea definite în setările Firewall. Pentru a preciza ce reguli de rețea trebuie aplicate monitorizării activității de rețea pentru aceste aplicații, trebuie să selectezi un grup de încredere.

Cum se selectează un grup de încredere pentru aplicații pornite înaintea componentei Kaspersky Endpoint Security în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Advanced Threat Protection → Host Intrusion Prevention**.



Setări Intrusion Prevention

4. În blocul **Drepturile aplicației și resursele protejate**, fă clic pe butonul **Editează**.
5. Pentru setarea opțiunii **Trust group for applications started before Kaspersky Endpoint Security**, selectați grupul de încredere corespunzător.
6. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se selectează un grup de încredere pentru aplicații pornite înaintea componentei Kaspersky Endpoint Security în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Host Threat Protection** → **Host Intrusion Prevention**.
5. Pentru setarea opțiunii **Trust group for applications started before Kaspersky Endpoint Security**, selectați grupul de încredere corespunzător.
6. Salvați-vă modificările.

Cum se selectează un grup de încredere pentru aplicații pornite înaintea componentei Kaspersky Endpoint Security în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul .
2. În fereastra cu setările aplicației, selectați **Advanced Threat Protection** → **Host Intrusion Prevention**.
3. În blocul **Grup de încredere pentru aplicațiile pornite înainte de a porni Kaspersky Endpoint Security**, selectați grupul de încredere corespunzător.
4. Salvați-vă modificările.

Ca rezultat, o aplicație pornită înaintea componentei Kaspersky Endpoint Security va fi introdusă în celălalt grup de încredere. Kaspersky Endpoint Security va bloca apoi acțiunile aplicației în funcție de grupul de încredere.

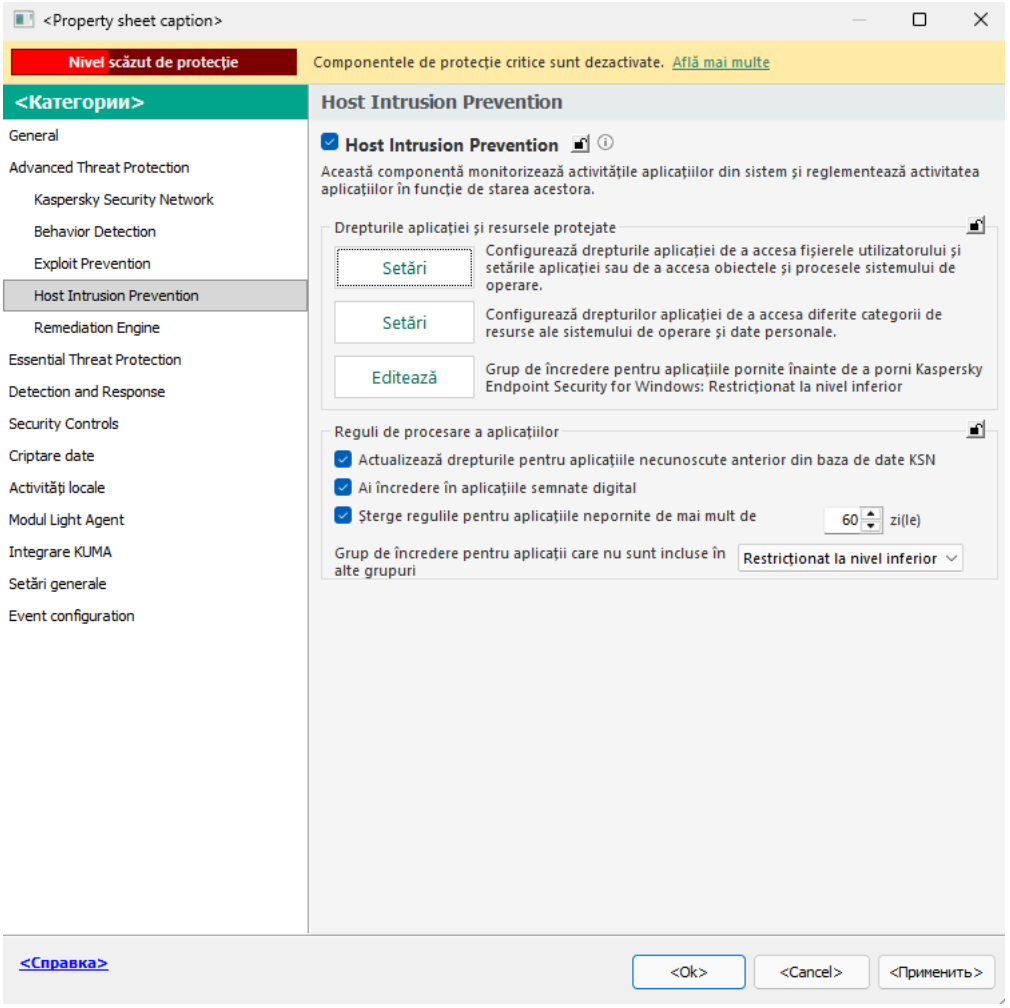
Selectarea unui grup de încredere pentru aplicații necunoscute

Atunci când o aplicație este pornită pentru prima dată, componenta Host Intrusion Prevention determină grupul de încredere pentru aplicație. Dacă nu aveți acces la Internet sau dacă Kaspersky Security Network nu deține nicio informație despre această aplicație, Kaspersky Endpoint Security va plasa în mod implicit aplicația în grupul *Restricționat la nivel inferior*. Atunci când sunt detectate informații despre o aplicație necunoscută anterior în KSN, Kaspersky Endpoint Security va actualiza drepturile acestei aplicații. Apoi poți edita manual drepturile pentru aplicații.

Cum se selectează un grup de încredere pentru aplicații necunoscute în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

3. În fereastra politicii, selectați **Advanced Threat Protection → Host Intrusion Prevention**.



Setări Intrusion Prevention

4. În blocul **Application processing rules**, utilizați lista verticală **Trust group for applications not included in other groups** pentru a selecta grupul de încredere necesar.

   Dacă participarea la Kaspersky Security Network este activată, Kaspersky Endpoint Security trimite către KSN o solicitare privind reputația unei aplicații de fiecare dată când aplicația este pornită. Pe baza răspunsului primit, aplicația poate fi mutată într-un grup de încredere diferit de cel specificat în setările componentei Host Intrusion Prevention.

5. Utilizați caseta de selectare **Update rights for previously unknown applications from KSN database** pentru a configura actualizarea automată a drepturilor pentru aplicațiile necunoscute.

6. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se selectează un grup de încredere pentru aplicații necunoscute în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management → Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **Host Threat Protection → Host Intrusion Prevention**.

5. În blocul **Application processing rules**, utilizați lista verticală **Trust group for applications not included in other groups** pentru a selecta grupul de încredere necesar.

   Dacă participarea la Kaspersky Security Network este activată, Kaspersky Endpoint Security trimite către KSN o solicitare privind reputația unei aplicații de fiecare dată când aplicația este pornită. Pe baza răspunsului primit, aplicația poate fi mutată într-un grup de încredere diferit de cel specificat în setările componentei Host Intrusion Prevention.

6. Utilizați caseta de selectare **Update rights for previously unknown applications from KSN database** pentru a configura actualizarea automată a drepturilor pentru aplicațiile necunoscute.

7. Salvați-vă modificările.

Cum se selectează un grup de încredere pentru aplicații necunoscute în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Advanced Threat Protection → Host Intrusion Prevention**.

3. În blocul **Reguli de procesare a aplicațiilor**, selectați grupul de încredere corespunzător.

   Dacă participarea la Kaspersky Security Network este activată, Kaspersky Endpoint Security trimite către KSN o solicitare privind reputația unei aplicații de fiecare dată când aplicația este pornită. Pe baza răspunsului primit, aplicația poate fi mutată într-un grup de încredere diferit de cel specificat în setările componentei Host Intrusion Prevention.

4. Utilizați caseta de selectare **Actualizează reguli pentru aplicațiile anterior necunoscute de la KSN** pentru a configura actualizarea automată a drepturilor pentru aplicațiile necunoscute.

5. Salvați-vă modificările.

Selectarea unui grup de încredere pentru aplicațiile semnate digital

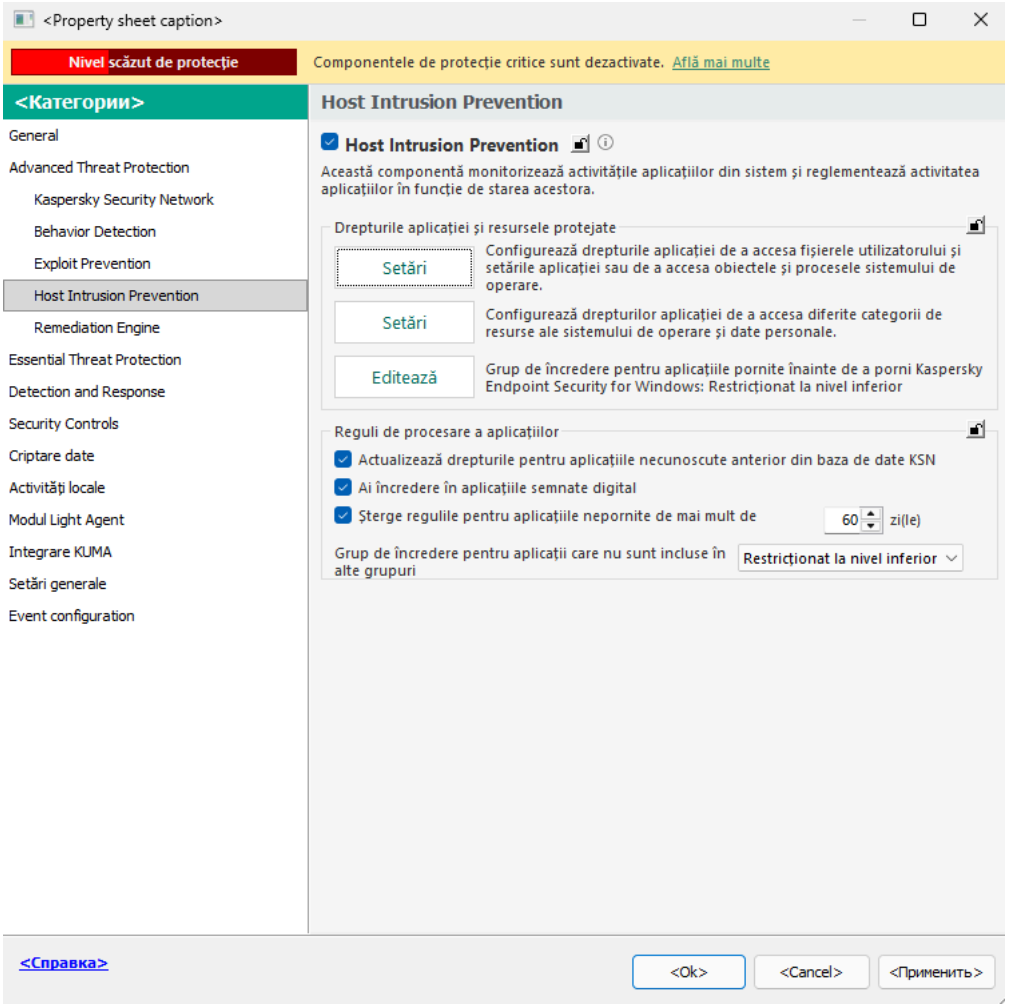
Kaspersky Endpoint Security plasează întotdeauna aplicațiile semnate cu certificate Microsoft sau Kaspersky în grupul *De încredere*.

Cum se selectează un grup de încredere pentru aplicații semnate digital în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.

2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

3. În fereastra politicii, selectați **Advanced Threat Protection → Host Intrusion Prevention**.



Setări Intrusion Prevention

4. În blocul **Application processing rules**, utilizează caseta de selectare **Trust digitally signed applications** pentru a activa sau dezactiva atribuirea automată în grupul de încredere Trusted pentru aplicațiile care conțin semnătura digitală a producătorilor de încredere.

   Trusted vendors sunt acei producători de software incluși de Kaspersky în grupul de încredere. De asemenea, puteți adăuga manual certificatul producătorului în depozitul de certificate de sistem de încredere.

   Dacă această casetă de selectare nu este bifată, componenta Host Intrusion Prevention nu consideră aplicațiile semnate digital ca fiind de încredere și folosește alți parametri pentru a determina grupul lor de încredere.

5. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se selectează un grup de încredere pentru aplicații semnate digital în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management → Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **Host Threat Protection → Host Intrusion Prevention**.

5. În blocul **Application processing rules**, utilizează caseta de selectare **Trust digitally signed applications** pentru a activa sau dezactiva atribuirea automată în grupul de încredere Trusted pentru aplicațiile care conțin semnătura digitală a producătorilor de încredere.

Trusted vendors sunt acei producători de software incluși de Kaspersky în grupul de încredere. De asemenea, puteți adăuga manual certificatul producătorului în depozitul de certificate de sistem de încredere.

Dacă această casetă de selectare nu este bifată, componenta Host Intrusion Prevention nu consideră aplicațiile semnate digital ca fiind de încredere și folosește alți parametri pentru a determina grupul lor de încredere.

6. Salvați-vă modificările.

Cum se selectează un grup de încredere pentru aplicații semnate digital în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Advanced Threat Protection → Host Intrusion Prevention**.
3. În blocul **Application processing rules**, utilizează caseta de selectare **Trust digitally signed applications** pentru a activa sau dezactiva atribuirea automată în grupul de încredere Trusted pentru aplicațiile care conțin semnătura digitală a producătorilor de încredere.

   Trusted vendors sunt acei producători de software incluși de Kaspersky în grupul de încredere. De asemenea, puteți adăuga manual certificatul producătorului în depozitul de certificate de sistem de încredere.

   Dacă această casetă de selectare nu este bifată, componenta Host Intrusion Prevention nu consideră aplicațiile semnate digital ca fiind de încredere și folosește alți parametri pentru a determina grupul lor de încredere.

4. Salvați-vă modificările.

Gestionarea drepturilor pentru aplicație

În mod implicit, activitate aplicației este controlată pe baza drepturilor aplicației definite pentru respectivul grup de încredere pe care Kaspersky Endpoint Security l-a alocat aplicației când aceasta a pornit prima dată. Dacă este necesar, poți edita drepturile pentru aplicații pentru un întreg grup de încredere, pentru o aplicație individuală sau pentru un grup de aplicații dintr-un grup de încredere.

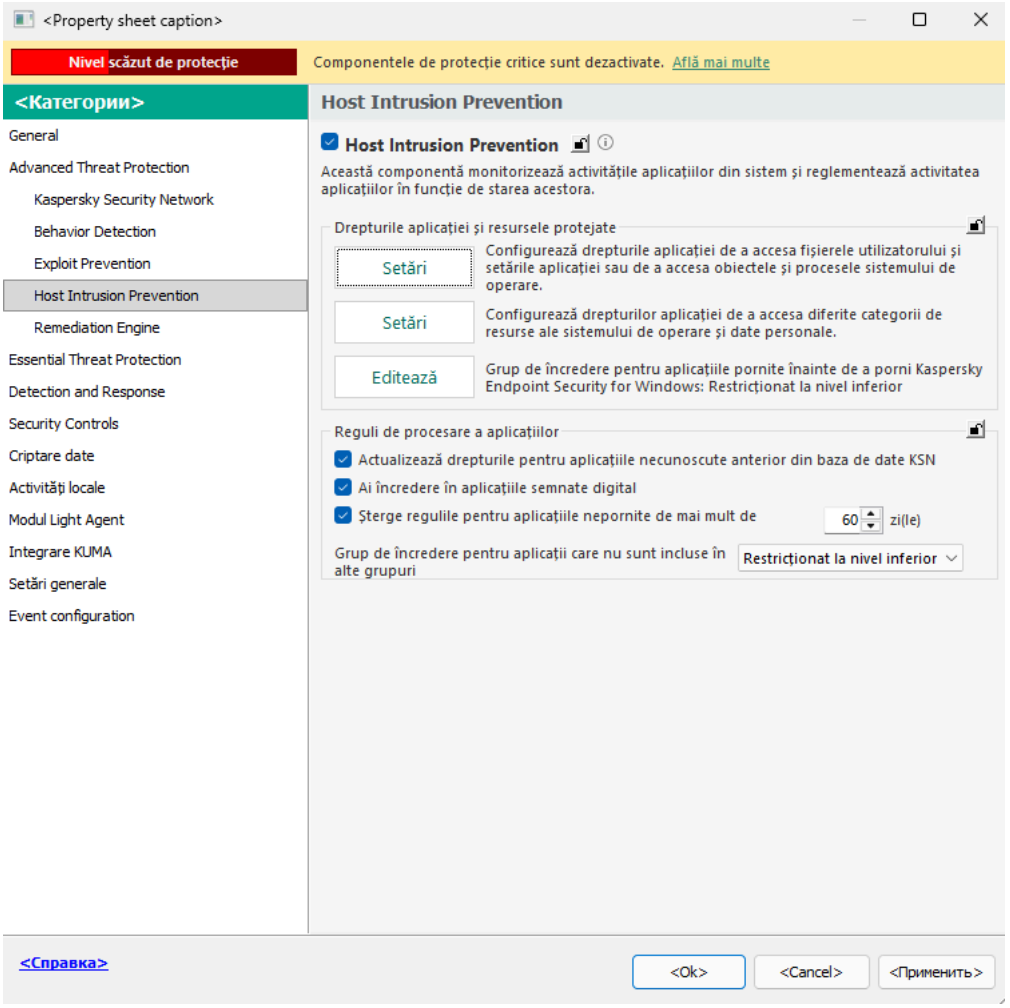
Drepturile pentru aplicații definite manual au o prioritate mai mare decât drepturile pentru aplicații definite pentru un grup de încredere. Cu alte cuvinte, dacă drepturile pentru aplicații definite manual diferă de drepturile pentru aplicații pentru un grup de încredere, componenta Host Intrusion Prevention controlează activitatea aplicației conform drepturilor pentru aplicații definite manual.

Regulile pe care le creați pentru aplicații sunt moștenite de aplicațiile secundare. De exemplu, dacă refuzați toate activitățile de rețea pentru cmd.exe, aceste activități vor fi refuzate, de asemenea, și pentru aplicația notepad.exe dacă este pornită cu cmd.exe. Atunci când o aplicație nu este o aplicație secundară a unei aplicații de la care se execută, regulile nu sunt moștenite.

Cum se modifică drepturile pentru aplicații în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

3. În fereastra politicii, selectați **Advanced Threat Protection → Host Intrusion Prevention**.



Setări Intrusion Prevention

4. În blocul **Drepturile aplicației și resursele protejate**, fă clic pe butonul **Setări**.

   Tastfel se deschide fereastra de configurare a drepturilor aplicațiilor și lista resurselor protejate.

5. Accesați fila **Drepturi aplicație**.

6. Fă clic pe **Adaugă**.

7. În fereastra care se deschide, introduceți criteriul de căutare pentru aplicația ale cărei drepturi de aplicație doriți să le modificați.

   Puteți introduce numele aplicației sau numele producătorului. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști.

8. Fă clic pe **Împrospătează**.

   Kaspersky Endpoint Security va căuta aplicația în lista consolidată de aplicații instalate pe computerele gestionate. Kaspersky Endpoint Security va afișa o listă cu aplicațiile care satisfac criteriul dvs. de căutare.

9. Selectați aplicația necesară.

10. În lista verticală **Adaugă aplicații selectate la grupul de încredere**, selectați **Grupuri implicite** și faceți clic pe **OK**.

    Aplicația va fi adăugată la grupul implicit.

11. Selectați aplicația relevantă și apoi selectați **Drepturi aplicație** din meniul contextual al aplicației.

    Aceasta deschide proprietățile aplicației.

12. Efectuează una dintre următoarele acțiuni:

    - Dacă doriți să editați drepturile grupului de încredere care reglementează operațiile cu registry-ul sistemului de operare, fișierele utilizatorului și setările aplicațiilor, selectați **Fișiere și registry de sistem**.
    - Dacă doriți să editați drepturile grupului de încredere care reglementează accesul la procesele și obiectele sistemului de operare, selectați **Drepturi**.

    Activitatea în rețea a aplicațiilor este controlată de componenta Firewall folosind *regulile de rețea*.

13. Pentru resursa relevantă, în coloana acțiunii corespunzătoare, faceți clic dreapta pentru a se deschide meniul contextual și selectați opțiunea necesară: **Moștenește**, **Permite** (✓) sau **Blochează** (⊘).

14. Dacă doriți să monitorizați utilizarea resurselor computerului, selectați **Înregistrează evenimentele în jurnal** (✓ / ⊘).

    Kaspersky Endpoint Security va înregistra informațiile despre funcționarea componentei Host Intrusion Prevention. Rapoartele conțin informații despre operațiile efectuate de aplicație cu resursele computerului (permise sau interzise). Rapoartele conțin, de asemenea, informații despre aplicațiile care utilizează fiecare resursă.

15. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se modifică drepturile pentru aplicații în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Host Threat Protection** → **Host Intrusion Prevention**.
5. În blocul **Application rights and protected resources**, faceți clic pe linkul **Application rights and protected resources**.

   Tastfel se deschide fereastra de configurare a drepturilor aplicațiilor și lista resurselor protejate.
6. Accesați fila **Application rights**.

   Veți vedea o listă cu grupurile de încredere în partea stângă a ferestrei, iar proprietățile acestora în partea dreaptă.
7. Fă clic pe **Add**.

   Aceasta pornește Expertul pentru adăugarea unei aplicații la un grup de încredere.
8. Selectați grupul de încredere relevant pentru aplicație.
9. Selectați **Application**. Mergeți la pasul următor.

   Dacă doriți să modificați grupul de încredere pentru mai multe aplicații, selectați **Group** și definiți un nume pentru grupul de aplicații.

10. În lista de aplicații deschisă, selectați aplicațiile ale căror drepturi de aplicație doriți să le modificați.

    Utilizați un filtru. Puteți introduce numele aplicației sau numele producătorului. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști.

11. Ieșiți din Expert.

    Aplicația va fi adăugată în grupul de încredere.

12. În partea stângă a ferestrei, selectați aplicația relevantă.

13. În partea dreaptă a ferestrei, în lista verticală, efectuați una dintre următoarele acțiuni:

    - Dacă doriți să editați drepturile grupului de încredere care reglementează operațiile cu registry-ul sistemului de operare, fișierele utilizatorului și setările aplicațiilor, selectați **Files and system registry**.
    - Dacă doriți să editați drepturile grupului de încredere care reglementează accesul la procesele și obiectele sistemului de operare, selectați **Rights**.

    Activitatea în rețea a aplicațiilor este controlată de componenta Firewall folosind *regulile de rețea*.

14. Pentru resursa relevantă, în coloana acțiunii corespunzătoare, selectați opțiunea necesară: **Inherit**, **Allow** (), **Block** ().

15. Dacă doriți să monitorizați utilizarea resurselor computerului, selectați **Log events** (/).

    Kaspersky Endpoint Security va înregistra informațiile despre funcționarea componentei Host Intrusion Prevention. Rapoartele conțin informații despre operațiile efectuate de aplicație cu resursele computerului (permise sau interzise). Rapoartele conțin, de asemenea, informații despre aplicațiile care utilizează fiecare resursă.

16. Salvați-vă modificările.

Cum se modifică drepturile pentru aplicații în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul .

2. În fereastra cu setările aplicației, selectați **Advanced Threat Protection → Host Intrusion Prevention**.

3. Fă clic pe **Gestionează aplicațiile**.

    Acest lucru va deschide lista aplicațiilor instalate.

4. Selectați aplicația necesară.

5. În meniul contextual al aplicației, selectați **Detalii și reguli**.

    Aceasta deschide proprietățile aplicației.

6. Efectuează una dintre următoarele acțiuni:

    - Dacă doriți să editați drepturile grupului de încredere care reglementează operațiile cu registry-ul sistemului de operare, fișierele utilizatorului și setările aplicațiilor, selectați **Fișiere și registry de sistem**.
    - Dacă doriți să editați drepturile grupului de încredere care reglementează accesul la procesele și obiectele sistemului de operare, selectați **Drepturi**.

7. Pentru resursa relevantă, în coloana acțiunii corespunzătoare, faceți clic dreapta pentru a se deschide meniul contextual și selectați opțiunea necesară: **Moștenește**, **Permite** (✓) sau **Refuză** (!).

8. Dacă doriți să monitorizați utilizarea resurselor computerului, selectați **Înregistrează evenimentele în jurnal** (📊).

   Kaspersky Endpoint Security va înregistra informațiile despre funcționarea componentei Host Intrusion Prevention. Rapoartele conțin informații despre operațiile efectuate de aplicație cu resursele computerului (permise sau interzise). Rapoartele conțin, de asemenea, informații despre aplicațiile care utilizează fiecare resursă.

9. Selectați fila **Excluderi** și configurați setările avansate ale aplicației (consultați tabelul de mai jos).

10. Salvați-vă modificările.

Setări avansate ale aplicației

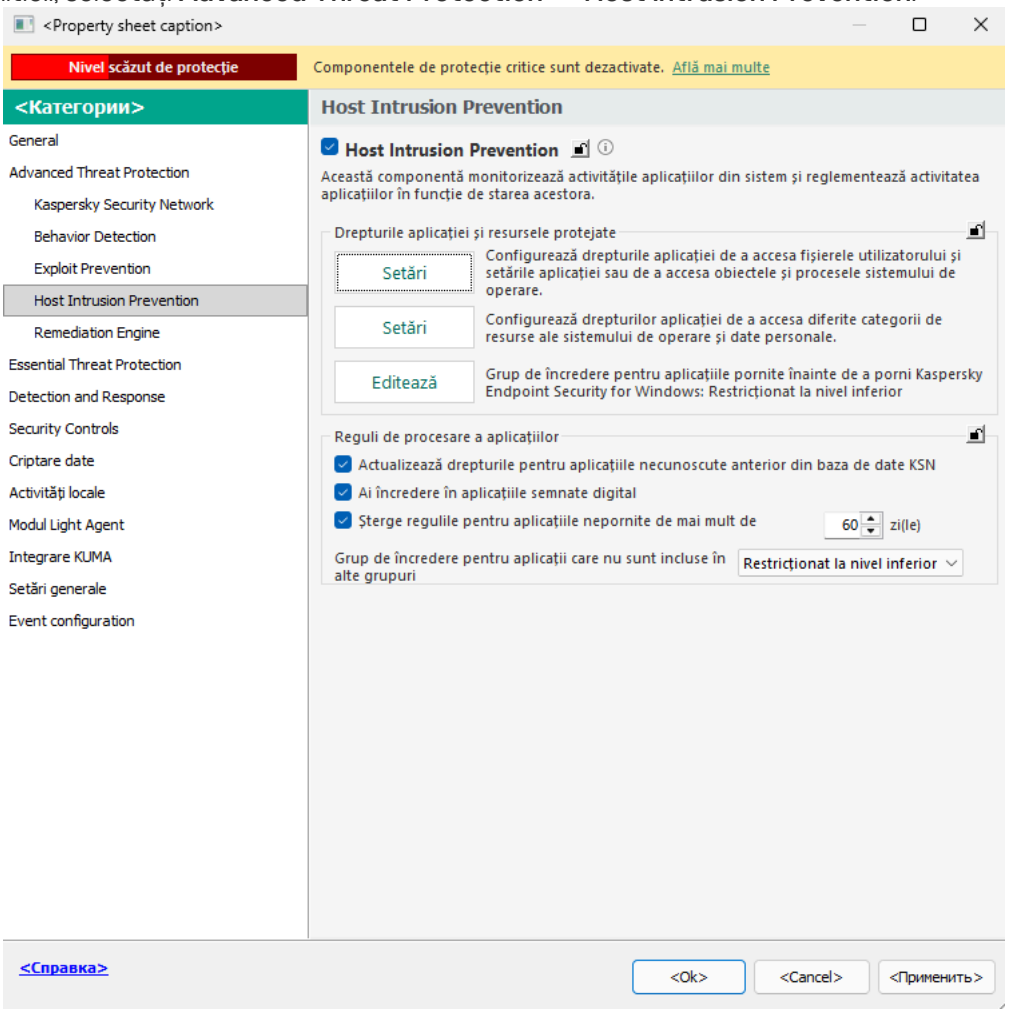
Parametru	Descriere
Nu scana fișierele deschise de această aplicație	Toate fișierele deschise de aplicația de încredere sunt excluse de la scanări de Kaspersky Endpoint Security. De exemplu, dacă utilizați aplicații pentru copierea de rezervă a fișierelor, această caracteristică ajută la reducerea consumului de resurse de către Kaspersky Endpoint Security.
Nu monitoriza activitatea aplicației	Kaspersky Endpoint Security nu va monitoriza activitatea fișierelor și a rețelei aplicației în sistemul de operare. Poți configura monitorizarea activității aplicației pentru diferite componente ale Kaspersky Endpoint Security: • **Nu monitoriza pentru componentele de protecție și control**. Activitatea aplicației este monitorizată de următoarele componente: Behavior Detection, Exploit Prevention, Host Intrusion Prevention, Remediation Engine și Firewall. • **Nu monitoriza pentru Managed Detection and Response și Endpoint Detection and Response**. Activitatea aplicației este monitorizată de MDR Agent încorporat și EDR (KATA) Agent încorporat. • **Nu intercepta intrarea interactivă în consolă pentru Endpoint Detection and Response**. Kaspersky Endpoint Security nu trimite date de telemetrie despre gestionarea aplicației pe consolă. Datele de telemetrie sunt folosite de Kaspersky Anti Targeted Attack Platform (EDR).
Nu moșteni restricții de la procesul principal (aplicația principală)	Restricțiile configurate pentru procesul părinte nu vor fi aplicate de Kaspersky Endpoint Security unui proces copil. Procesul părinte este inițiat de o aplicație pentru care sunt configurate drepturile aplicației (Host Intrusion Prevention) și regulile de rețea ale aplicației (Firewall).
Nu monitoriza activitatea aplicației subordonate	Kaspersky Endpoint Security nu va monitoriza activitatea fișierelor sau activitatea de rețea a aplicațiilor care sunt pornite de această aplicație. Poți aplica excluderea]n mod recursiv. Astfel ca aplicația să nu monitorizeze activitatea întregului lanț de aplicații secundare.
Permite interacțiunea cu interfața Kaspersky Endpoint Security	Autoprotecția Kaspersky Endpoint Security blochează toate încercările de a gestiona serviciile aplicațiilor de pe un computer la distanță. Dacă această casetă de selectare este bifată, aplicația cu acces la distanță are permisiunea de a gestiona setările Kaspersky Endpoint Security prin interfața Kaspersky Endpoint Security.
Nu scana traficul criptat / Nu scana tot traficul	Traficul de rețea inițiat de aplicație va fi exclus din scanări de Kaspersky Endpoint Security. Puteți exclude de la scanări fie traficul, fie doar traficul criptat. De asemenea, puteți exclude adresele IP și numerele de port individuale din scanări. Kaspersky Endpoint Security versiunea 14.0 sau o versiune anterioară nu acceptă excluderea traficului de rețea dacă este specificat un hash pentru o aplicație de încredere în loc de o cale.

Protejarea resurselor sistemului de operare și a datelor personale

Componenta Host Intrusion Prevention gestionează drepturile aplicațiilor de a efectua acțiuni asupra unor diverse categorii de resurse de sistem și de date de identitate. Specialiștii de la Kaspersky au elaborat categorii prestabilite de resurse protejate. De exemplu, categoria *Sistem de operare* are o subcategorie *Setări pornire* care listează toate cheile de registry asociate cu executarea automată a aplicațiilor. Categoriile de resurse protejate și resursele protejate din aceste categorii nu pot fi editate sau șterse.

Cum se adăugă o resursă protejată în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Advanced Threat Protection → Host Intrusion Prevention**.



Setări Intrusion Prevention

4. În blocul **Drepturile aplicației și resursele protejate**, fă clic pe butonul **Setări**.

   Tastfel se deschide fereastra de configurare a drepturilor aplicațiilor și lista resurselor protejate.

5. Accesați fila **Resurse protejate**.

   Veți vedea o listă cu resursele protejate în partea stângă a ferestrei și drepturile corespunzătoare pentru accesarea acelor resurse, în funcție de grupul de încredere specific.

6. Selectați categoria de resurse protejate la care doriți să adăugați o nouă resursă protejată.

   Dacă doriți să adăugați o subcategorie, faceți clic pe **Adaugă → Categorie**.

7. Faceți clic pe butonul **Adaugă**. În lista verticală, selectați tipul de resursă pe care dorești s-o adaugi: **Fișier sau director** sau **Cheie de registry**.

8. În fereastra care se deschide, selectați un fișier, director sau o cheie de registry.

   Puteți vedea drepturile aplicațiilor pentru a accesa resursele adăugate. Pentru aceasta, selectați o resursă adăugată în partea stângă a ferestrei și Kaspersky Endpoint Security va afișa drepturile de acces pentru fiecare grup de încredere. De asemenea, puteți dezactiva controlul activității aplicațiilor cu resursele, utilizând caseta de selectare de lângă o resursă.

9. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se adaugă o resursă protejată în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **Host Threat Protection** → **Host Intrusion Prevention**.

5. În blocul **Application rights and protected resources**, faceți clic pe linkul **Application rights and protected resources**.

   Tastfel se deschide fereastra de configurare a drepturilor aplicațiilor și lista resurselor protejate.

6. Accesați fila **Protected resources**.

   Veți vedea o listă cu resursele protejate în partea stângă a ferestrei și drepturile corespunzătoare pentru accesarea acelor resurse, în funcție de grupul de încredere specific.

7. Fă clic pe **Add**.

   Funcția Expert pentru resursă nouă pornește.

8. Fă clic pe blocul **Group name**, selectează categoria de resurse protejate la care dorești să adaugi o nouă resursă protejată.

   Dacă doriți să adăugați o subcategorie, selectați opțiunea **Category of protected resources**.

9. Selectați tipul resursei pe care doriți să o adăugați: **File or folder** sau **Registry key**.

10. Selectați un fișier, un dosar sau o cheie de registry.

11. Ieșiți din Expert.

    Puteți vedea drepturile aplicațiilor pentru a accesa resursele adăugate. Pentru aceasta, selectați o resursă adăugată în partea stângă a ferestrei și Kaspersky Endpoint Security va afișa drepturile de acces pentru fiecare grup de încredere. De asemenea, puteți bifa caseta din coloana **Status** pentru a dezactiva controlul activității aplicației cu resursele.

12. Salvați-vă modificările.

Cum se adaugă o resursă protejată în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Advanced Threat Protection** → **Host Intrusion Prevention**.

3. Fă clic pe **Gestionează resursele**.

   Se deschide lista resurselor protejate.

4. Selectați categoria de resurse protejate la care doriți să adăugați o nouă resursă protejată.

   Dacă doriți să adăugați o subcategorie, faceți clic pe **Adaugă** → **Categorie**.

5. Faceți clic pe butonul **Adaugă**. În lista verticală, selectați tipul de resursă pe care dorești s-o adaugi: **Fișier sau director** sau **Cheie de registry**.

6. În fereastra care se deschide, selectați un fișier, director sau o cheie de registry.

   Puteți vedea drepturile aplicațiilor pentru a accesa resursele adăugate. Pentru aceasta, selectați o resursă adăugată în partea stângă a ferestrei și Kaspersky Endpoint Security va afișa o listă de aplicații și drepturile de acces pentru fiecare aplicație. De asemenea, puteți dezactiva controlul activității aplicației cu resursele, utilizând butonul **Activare control** din coloana **Stare**.

7. Salvați-vă modificările.

Kaspersky Endpoint Security va controla accesul la resursele adăugate ale sistemului de operare și la datele personale. Kaspersky Endpoint Security controlează accesul unei aplicații la resurse pe baza grupului de încredere alocat aplicației. De asemenea, puteți schimba manual grupul de încredere al unei aplicații.

Ștergerea informațiilor despre aplicațiile neutilizate

Kaspersky Endpoint Security folosește drepturile aplicației pentru a controla activitățile aplicațiilor. Drepturile aplicației sunt determinate de grupul lor de încredere. Kaspersky Endpoint Security pune o aplicație într-un grup de încredere atunci când aplicația este pornită prima dată. Puteți schimba manual grupul de încredere al unei aplicații. De asemenea, puteți configura manual drepturile unei aplicații individuale. Kaspersky Endpoint Security stochează următoarele informații despre o aplicație: grup de încredere al aplicației și drepturi ale aplicației.

Kaspersky Endpoint Security șterge automat informațiile despre aplicațiile neutilizate pentru a economisi resursele computerului. Kaspersky Endpoint Security șterge informațiile despre aplicație în conformitate cu următoarele reguli:

- Dacă grupul de încredere și drepturile unei aplicații au fost determinate automat, Kaspersky Endpoint Security șterge informațiile despre această aplicație după 30 de zile. Nu este posibilă modificarea termenului de stocare a informațiilor despre aplicație sau oprirea ștergerii automate.

- Dacă introduceți manual o aplicație într-un grup de încredere sau i-ați configurat drepturile de acces, Kaspersky Endpoint Security șterge informațiile despre această aplicație după 60 de zile (termen de stocare implicit). Puteți modifica termenul de stocare pentru informațiile despre aplicație sau puteți dezactiva ștergerea automată (consultați instrucțiunile de mai jos).

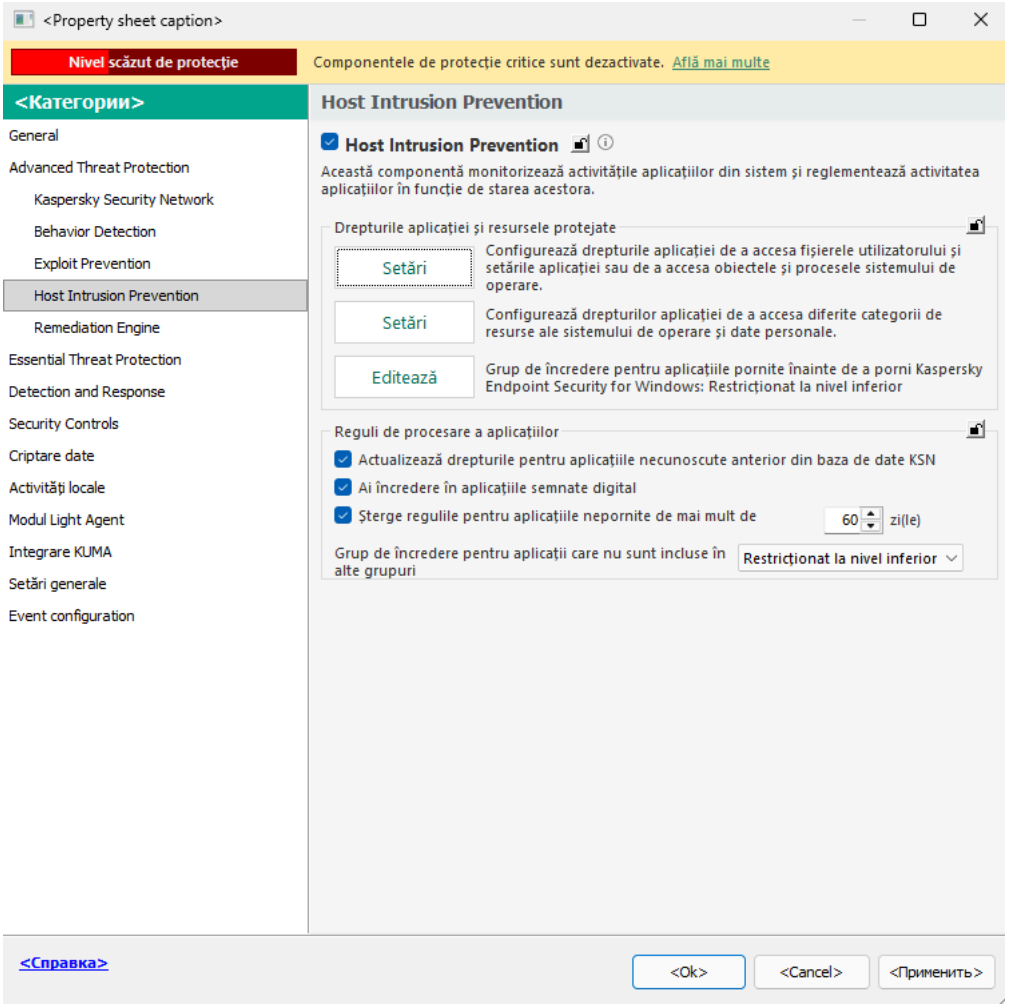
Când porniți o aplicație ale cărei informații au fost șterse, Kaspersky Endpoint Security analizează aplicația ca și cum ar porni pentru prima dată.

Cum se configurează ștergere automată a informațiilor despre aplicațiile neutilizate în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.

2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

3. În fereastra politicii, selectați **Advanced Threat Protection → Host Intrusion Prevention**.



Setări Intrusion Prevention

4. În blocul **Reguli de procesare a aplicațiilor**, efectuează una dintre următoarele acțiuni:

- Dacă doriți să configurați ștergerea automată, bifați caseta de selectare **Șterge regulile pentru aplicațiile nepornite de mai mult de N zi(le)** și specificați numărul de zile.

  Informațiile despre aplicațiile pe care le-ați introdus manual într-un grup de încredere sau ale căror drepturi de acces le-ați configurat manual vor fi șterse de Kaspersky Endpoint Security după numărul de zile stabilit. Informațiile despre aplicațiile al căror grup de încredere și drepturi de aplicare au fost stabilite automat vor fi, de asemenea, șterse de Kaspersky Endpoint Security după 30 de zile.

- Dacă doriți să dezactivați ștergerea automată, debifați caseta de selectare **Șterge regulile pentru aplicațiile nepornite de mai mult de N zi(le)**.

  Informațiile despre aplicațiile pe care le-ați introdus manual într-un grup de încredere sau ale căror drepturi de acces le-ați configurat manual vor fi stocate de Kaspersky Endpoint Security pe termen nelimitat, fără termene limită de stocare. Kaspersky Endpoint Security va șterge doar informațiile despre aplicațiile al căror grup de încredere și drepturi de aplicație au fost determinate automat după 30 de zile.

5. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se configurează ștergerea automată a informațiilor despre aplicațiile neutilizate în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management → Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **Host Threat Protection** → **Host Intrusion Prevention**.

5. În blocul **Application processing rules**, efectuează una dintre următoarele acțiuni:

   - Dacă dorești să configurezi ștergerea automată, bifează caseta de selectare **Delete rules for applications that have not been started for longer than (days, 1 to 90)** și specifică numărul de zile.

     Informațiile despre aplicațiile pe care le-ați introdus manual într-un grup de încredere sau ale căror drepturi de acces le-ați configurat manual vor fi șterse de Kaspersky Endpoint Security după numărul de zile stabilit. Informațiile despre aplicațiile al căror grup de încredere și drepturi de aplicare au fost stabilite automat vor fi, de asemenea, șterse de Kaspersky Endpoint Security după 30 de zile.

   - Dacă dorești să dezactivezi ștergerea automată, debifează caseta de selectare **Delete rules for applications that have not been started for longer than (days, 1 to 90)**.

     Informațiile despre aplicațiile pe care le-ați introdus manual într-un grup de încredere sau ale căror drepturi de acces le-ați configurat manual vor fi stocate de Kaspersky Endpoint Security pe termen nelimitat, fără termene limită de stocare. Kaspersky Endpoint Security va șterge doar informațiile despre aplicațiile al căror grup de încredere și drepturi de aplicație au fost determinate automat după 30 de zile.

6. Salvați-vă modificările.

Cum se configurează ștergerea automată a informațiilor despre aplicațiile neutilizate în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Advanced Threat Protection** → **Host Intrusion Prevention**.

3. În blocul **Reguli de procesare a aplicațiilor**, efectuează una dintre următoarele acțiuni:

   - Dacă doriți să configurați ștergerea automată, bifați caseta de selectare **Șterge regulile pentru aplicațiile nepornite de mai mult de N zile (între 1 și 90)** și specificați numărul de zile.

     Informațiile despre aplicațiile pe care le-ați introdus manual într-un grup de încredere sau ale căror drepturi de acces le-ați configurat manual vor fi șterse de Kaspersky Endpoint Security după numărul de zile stabilit. Informațiile despre aplicațiile al căror grup de încredere și drepturi de aplicare au fost stabilite automat vor fi, de asemenea, șterse de Kaspersky Endpoint Security după 30 de zile.

   - Dacă doriți să dezactivați ștergerea automată, debifați caseta de selectare **Șterge regulile pentru aplicațiile nepornite de mai mult de N zile (între 1 și 90)**.

     Informațiile despre aplicațiile pe care le-ați introdus manual într-un grup de încredere sau ale căror drepturi de acces le-ați configurat manual vor fi stocate de Kaspersky Endpoint Security pe termen nelimitat, fără termene limită de stocare. Kaspersky Endpoint Security va șterge doar informațiile despre aplicațiile al căror grup de încredere și drepturi de aplicație au fost determinate automat după 30 de zile.

4. Salvați-vă modificările.

Monitorizarea Host Intrusion Prevention

Puteți primi rapoarte privind funcționarea componentei Host Intrusion Prevention. Rapoartele conțin informații despre operațiile efectuate de aplicație cu resursele computerului (permise sau interzise). Rapoartele conțin, de asemenea, informații despre aplicațiile care utilizează fiecare resursă.

Pentru a monitoriza operațiile componentei Host Intrusion Prevention trebuie să activați scrierea în raport. De exemplu, puteți activa redirecționarea rapoartelor pentru aplicații individuale în setările componentei Host Intrusion Prevention.

Când configurați monitorizarea componentei Host Intrusion Prevention, țineți cont de posibila încărcare a rețelei atunci când redirecționați evenimentele către Kaspersky Security Center. De asemenea, puteți activa salvarea rapoartelor numai în jurnalul local al Kaspersky Endpoint Security.

Protejarea accesului la componentele audio și video

Funcționalitatea de protecție a semnalului audio și cea de protecție a accesului la camera web nu sunt acceptate pe computerele bazate pe arhitectura Arm.

Infractorii cibernetici pot utiliza programe speciale pentru a încerca să obțină acces la dispozitive care înregistrează audio și video (cum ar fi microfoane sau camere web). Kaspersky Endpoint Security controlează când aplicațiile primesc o fluxuri audio sau video și protejează datele împotriva interceptării neautorizate.

În mod implicit, Kaspersky Endpoint Security permite primirea de fluxuri audio și video numai pentru aplicațiile din grupul *De încredere*. Aplicațiile din grupurile *Restricționat la nivel inferior*, *Restricționat la nivel superior* și *Nu este de încredere* grupurile nu au voie să primească flux audio și flux video de la dispozitive. Puteți permite manual aplicațiilor să primească fluxuri audio și video.

Funcții speciale ale protecției fluxului audio

Protecția redării fluxului audio are următoarele caracteristici speciale:

- Componenta Host Intrusion Prevention trebuie să fie activată pentru ca această funcționalitate să funcționeze.
- Dacă aplicația a început să primească fluxul audio înainte de pornirea componentei Host Intrusion Prevention, Kaspersky Endpoint Security permite aplicației să primească fluxul audio și nu afișează notificări.
- Dacă ai mutat aplicația în grupul *Nu este de încredere* sau *Restricționat la nivel superior* după ce aplicația a început să primească fluxul audio, Kaspersky Endpoint Security permite aplicației să primească fluxul audio și nu afișează notificări.
- După modificarea setărilor de acces al aplicației la dispozitivele de înregistrare a sunetului (de exemplu, dacă s-a blocat primirea fluxului audio de către aplicație), această aplicație trebuie repornită pentru a nu mai primi fluxul audio.
- Controlul accesului la fluxul audio de la dispozitivele de înregistrare a sunetului nu depinde de setările de acces la camera Web ale unei aplicații.
- Kaspersky Endpoint Security protejează accesul doar la microfoanele încorporate și la microfoanele externe. Nu sunt acceptate alte dispozitive de redare în flux.

- Kaspersky Endpoint Security nu poate garanta protecția unui flux audio de la dispozitive precum camere DSLR, camere video portabile și camere de acțiune.
- Atunci când executați aplicații de înregistrare sau redare audio și video pentru prima dată după instalarea Kaspersky Endpoint Security este posibil ca redarea sau înregistrarea audio și video să fie întreruptă. Acest lucru este necesar pentru a activa funcționalitatea care controlează accesul aplicațiilor la dispozitivele de înregistrare a sunetului. Serviciul de sistem care controlează componentele hardware audio va fi repornit atunci când Kaspersky Endpoint Security este executat pentru prima dată.

Caracteristici speciale ale protecției accesului la camera web al aplicației

Funcția de protecție a accesului la camera Web prezintă următoarele considerații și limitări:

- Aplicația controlează numai imaginile video și imaginile statice provenite din procesarea datelor de la camera Web.
- Aplicația controlează fluxul audio dacă acesta face parte din fluxul video primit de la camera Web.
- Aplicația controlează numai camerele Web conectate prin USB sau IEEE1394 și care sunt afișate ca Dispozitive de imagini în Manager dispozitive Windows.
- Kaspersky Endpoint Security acceptă următoarele camere Web:
  - 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 nu poate garanta asistență pentru camerele Web care nu sunt specificate în această listă.

BadUSB Attack Prevention

Unii viruși modifică firmware-ul dispozitivelor USB pentru a păcăli sistemul de operare să detecteze dispozitivul USB ca tastatură. Ca urmare, virusul poate executa comenzi în contul dvs. de utilizator pentru a descărca programe malware, de exemplu.

Componenta BadUSB Attack Prevention împiedică dispozitivele USB infectate care emulează o tastatură să se conecteze la computer.

Atunci când un dispozitiv USB este conectat la un computer și este identificat drept tastatură de sistemul de operare, aplicația solicită utilizatorului să introducă un cod numeric generat de aplicație de la tastatură sau folosind Tastatura de pe ecran, dacă este disponibilă (consultă figura de mai jos). Această procedură este cunoscută sub numele de Autorizare tastatură.

Dacă a fost introdus corect codul, aplicația salvează parametrii de identificare – VID/PID pentru tastatură și numărul portului la care a fost conectată – în lista de tastaturi autorizate. Autorizarea tastaturii nu trebuie repetată atunci când tastatura este reconectată sau după repornirea sistemului de operare.

Atunci când tastatura autorizată este conectată la un alt port USB al computerului, aplicația afișează din nou o solicitare de autorizare a acestei tastaturi.

Dacă a fost introdus incorect codul numeric, aplicația generează un cod nou. Puteți configura numărul de încercări pentru introducerea codului numeric. În cazul în care codul numeric este introdus incorect de mai multe ori sau fereastra de autorizare a tastaturii este închisă (a se vedea figura de mai jos), aplicația blochează intrarea de pe această tastatură. Atunci când intervalul de blocare al dispozitivului USB trece sau după ce sistemul de operare este repornit, aplicația solicită utilizatorului să efectueze din nou autorizarea tastaturii.

Aplicația permite utilizarea unei tastaturi autorizate și blochează o tastatură care nu a fost autorizată.

Componenta BadUSB Attack Protection nu este instalată implicit. Dacă aveți nevoie de componenta BadUSB Attack Prevention, puteți adăuga componenta în proprietățile pachetului de instalare înainte de a instala aplicația sau de a modifica componentele disponibile ale aplicației după instalarea aplicației.



Autorizare tastatură

Activarea și dezactivarea componentei BadUSB Attack Prevention

Dispozitivele USB identificate de sistemul de operare drept tastaturi și conectate la computer înainte de instalarea componentei BadUSB Attack Prevention sunt considerate a fi autorizate după instalarea componentei.

Cum se activează sau dezactivează componenta BadUSB Attack Prevention în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Essential Threat Protection → BadUSB Attack Prevention**.
4. Utilizează caseta de selectare **BadUSB Attack Prevention** pentru a activa sau a dezactiva componenta.
5. În blocul **Autorizarea dispozitivului USB la conectare**, modificați setările de securitate pentru introducerea codului de autorizare:
   - **Numărul maxim de încercări de autorizare a dispozitivului USB**. Blocarea automată a dispozitivului USB în cazul în care codul de autorizare este introdus incorect de numărul specificat de ori. Valorile valide sunt de la 1 la 10. De exemplu, dacă permiți cinci încercări de introducere a codul de autorizare, aplicația blochează dispozitivul USB după a cincea încercare eșuată. Kaspersky Endpoint Security afișează durata blocării dispozitivului USB. După expirarea acestui timp, vei avea din nou 5 încercări de introducere a codului de autorizare.
   - **Expiră când este atins numărul maxim de încercări (minute)**. Durata blocării dispozitivului USB după numărul specificat de încercări nereușite de introducere a codului de autorizare. Valorile valide sunt de la 1 la 180 (minute).
6. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

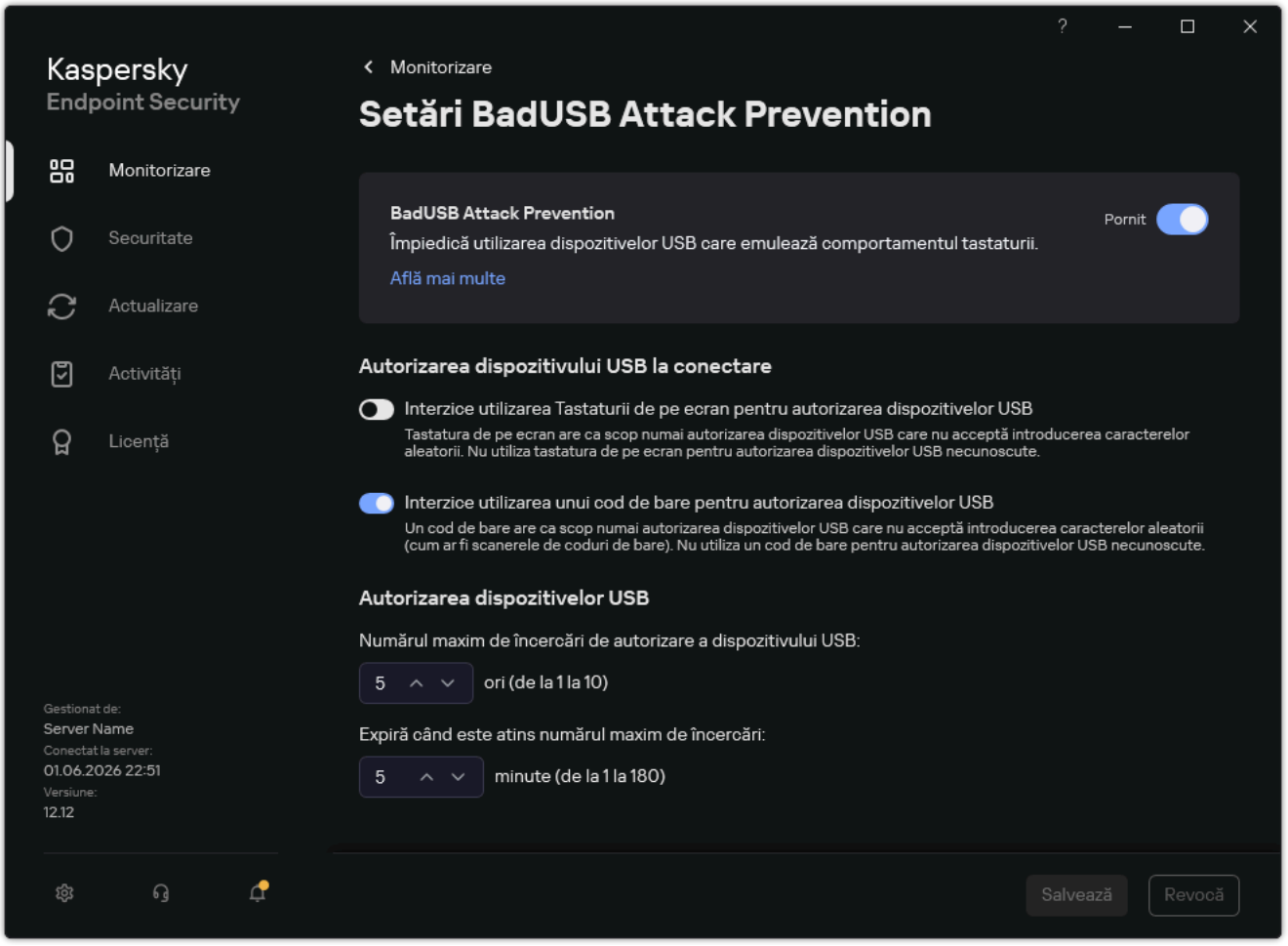
Cum se activează sau dezactivează componenta BadUSB Attack Prevention în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management → Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.
   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Host Threat Protection → BadUSB Attack Prevention**.
5. Utilizați comutatorul **BadUSB Attack Prevention ENABLED** pentru a activa sau a dezactiva componenta.
6. În blocul **Authorization of USB devices**, modificați setările de securitate pentru introducerea codului de autorizare:
   - **Maximum number of USB device authorization attempts**. Blocarea automată a dispozitivului USB în cazul în care codul de autorizare este introdus incorect de numărul specificat de ori. Valorile valide sunt de la 1 la 10. De exemplu, dacă permiți cinci încercări de introducere a codul de autorizare, aplicația blochează dispozitivul USB după a cincea încercare eșuată. Kaspersky Endpoint Security afișează durata blocării dispozitivului USB. După expirarea acestui timp, vei avea din nou 5 încercări de introducere a codului de autorizare.
   - **Timeout when reaching the maximum number of attempts (min)**. Durata blocării dispozitivului USB după numărul specificat de încercări nereușite de introducere a codului de autorizare. Valorile valide sunt de la 1 la 180 (minute).
7. Salvați-vă modificările.

Cum se activează sau dezactivează componenta BadUSB Attack Prevention în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Essential Threat Protection → BadUSB Attack Prevention**.



Setările componentei BadUSB Attack Prevention

3. Utilizați comutatorul **BadUSB Attack Prevention** pentru a activa sau a dezactiva componenta.

4. În blocul **Autorizarea dispozitivului USB la conectare**, modificați setările de securitate pentru introducerea codului de autorizare:

   - **Numărul maxim de încercări de autorizare a dispozitivului USB**. Blocarea automată a dispozitivului USB în cazul în care codul de autorizare este introdus incorect de numărul specificat de ori. Valorile valide sunt de la 1 la 10. De exemplu, dacă permiți cinci încercări de introducere a codul de autorizare, aplicația blochează dispozitivul USB după a cincea încercare eșuată. Kaspersky Endpoint Security afișează durata blocării dispozitivului USB. După expirarea acestui timp, vei avea din nou 5 încercări de introducere a codului de autorizare.

   - **Expiră când este atins numărul maxim de încercări**. Durata blocării dispozitivului USB după numărul specificat de încercări nereușite de introducere a codului de autorizare. Valorile valide sunt de la 1 la 180 (minute).

5. Salvați-vă modificările.

Prin urmare, dacă BadUSB Attack Prevention este activat, Kaspersky Endpoint Security necesită autorizarea unui dispozitiv USB conectat identificat ca tastatură de sistemul de operare. Utilizatorul nu poate folosi o tastatură neautorizată până când aceasta nu este autorizată.

Utilizarea tastaturii vizuale pentru autorizarea dispozitivelor USB

Tastatura virtuală trebuie folosită numai pentru autorizarea dispozitivelor USB care nu acceptă introducerea caracterelor aleatorii (cum ar fi scanerele de coduri de bare). Nu se recomandă folosirea tastaturii virtuale pentru autorizarea dispozitivelor USB necunoscute.

Cum să permiți sau să interzici utilizarea tastaturii pe ecran pentru autorizare în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Essential Threat Protection → BadUSB Attack Prevention**.
4. Utilizați caseta de selectare **Interzice utilizarea Tastaturii de pe ecran pentru autorizarea dispozitivelor USB** pentru a bloca sau a permite utilizarea tastaturii vizuale pentru autorizare.
5. Salvați-vă modificările.

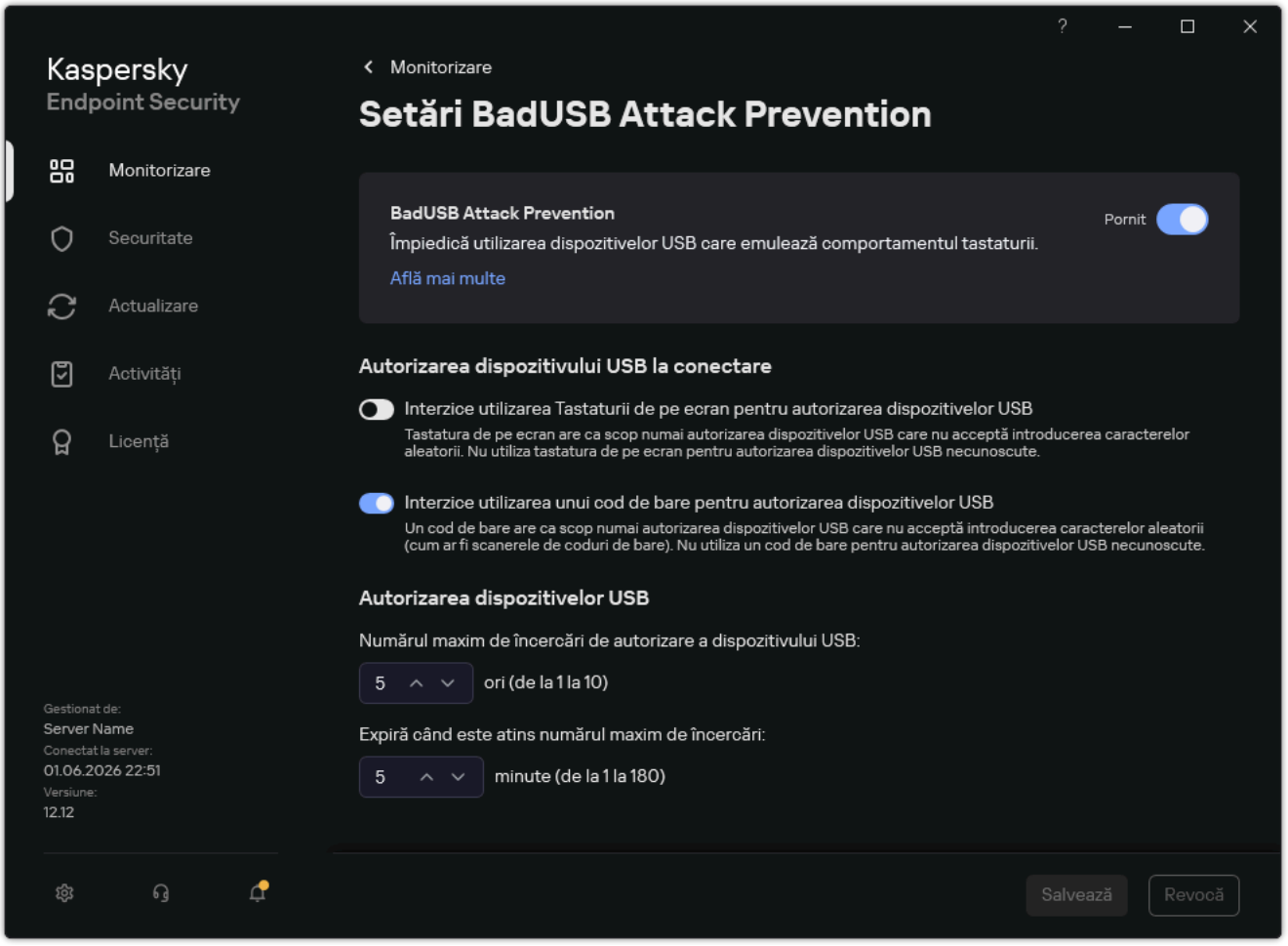
Cum să permiți sau să interzici utilizarea tastaturii pe ecran pentru autorizare în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management → Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Host Threat Protection → BadUSB Attack Prevention**.
5. Utilizați comutatorul **Prohibit use of On-Screen Keyboard for authorization of USB devices** pentru a bloca sau a permite utilizarea tastaturii vizuale pentru autorizare.
6. Salvați-vă modificările.

Cum să permiți sau să interzici utilizarea tastaturii pe ecran pentru autorizare în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **BadUSB Attack Prevention**.



Setările componentei BadUSB Attack Prevention

3. Utilizați comutatorul **Interzice utilizarea Tastaturii de pe ecran pentru autorizarea dispozitivelor USB** pentru a bloca sau a permite utilizarea tastaturii vizuale pentru autorizare.

4. Salvați-vă modificările.



Autorizarea dispozitivelor USB

Autorizarea scanerului de coduri de bare

Când conectezi un scaner de coduri de bare la computer, componenta BadUSB Attack Prevention identifică acest dispozitiv ca dispozitiv de intrare și îți solicită să efectuezi autorizarea. Pentru a autoriza scanerul de coduri de bare, trebuie să scanezi un cod de bare afișat pe ecran. Aplicația generează un cod de bare în formatul Code39, care este acceptat de majoritatea scanerelor de coduri de bare și de coduri QR.

Kaspersky Endpoint Security acceptă și o altă metodă de autorizare a scanerului de coduri de bare. Dacă utilizezi dispozitive cu ecran tactil, poți utiliza o tastatură de pe ecran pentru a introduce un cod. Pentru aceasta, trebuie să permiți tastatura de pe ecran. Această metodă este convenabilă, de exemplu, în cazul scanerelor de coduri de bare staționare, încorporate în casele de marcat. Alte metode de autorizare a scanerului de coduri de bare sunt interzise.

În mod implicit, aplicația nu folosește un cod de bare pentru autorizarea dispozitivelor USB.

Cum se activează autorizarea dispozitivelor USB folosind un cod de bare în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.

2. În arborele consolei, selectați **Policies**.

3. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

4. În fereastra politicii, selectați **Essential Threat Protection → BadUSB Attack Prevention**.

5. Utilizează caseta de selectare **Interzice utilizarea unui cod de bare pentru autorizarea dispozitivelor USB** pentru a bloca sau a permite utilizarea codurilor de bare pentru autorizare.

6. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se activează autorizarea dispozitivelor USB folosind un cod de bare în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați fila **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **Host Threat Protection** → **BadUSB Attack Prevention**.

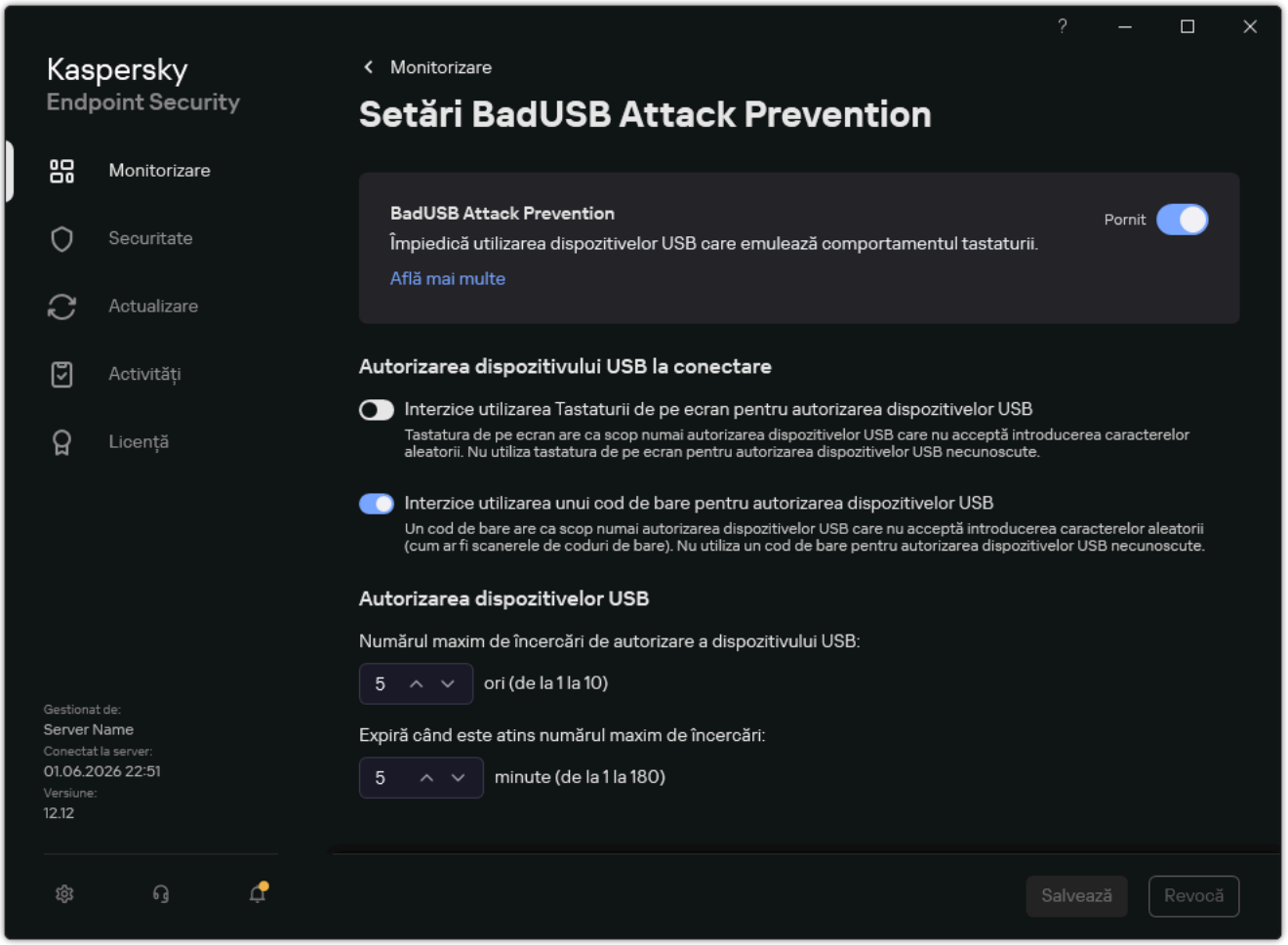
5. Utilizează comutatorul **Prohibit use of a barcode for authorization of USB devices** pentru a bloca sau a permite utilizarea codurilor de bare pentru autorizare.

6. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se activează autorizarea dispozitivelor USB folosond un cod în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

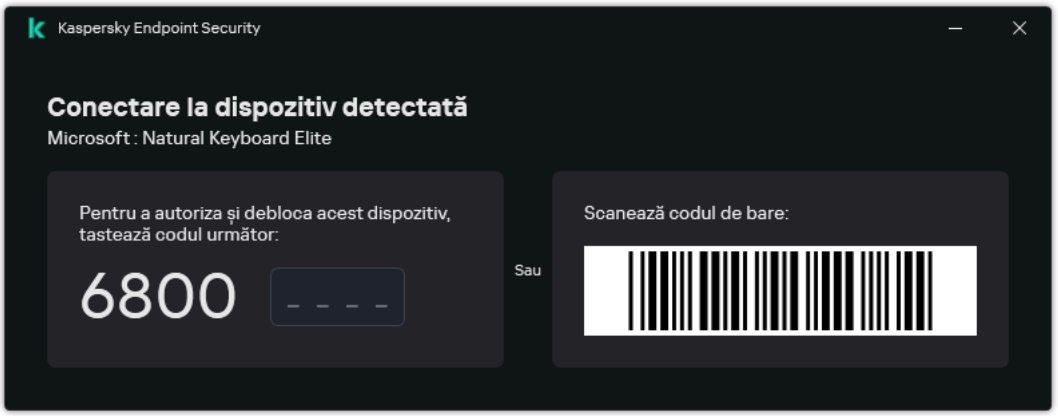
2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **BadUSB Attack Prevention**.



Setările componentei BadUSB Attack Prevention

3. Utilizează comutatorul **Interzice utilizarea unui cod de bare pentru autorizarea dispozitivelor USB** pentru a bloca sau a permite utilizarea codurilor de bare pentru autorizare.

4. Salvați-vă modificările.

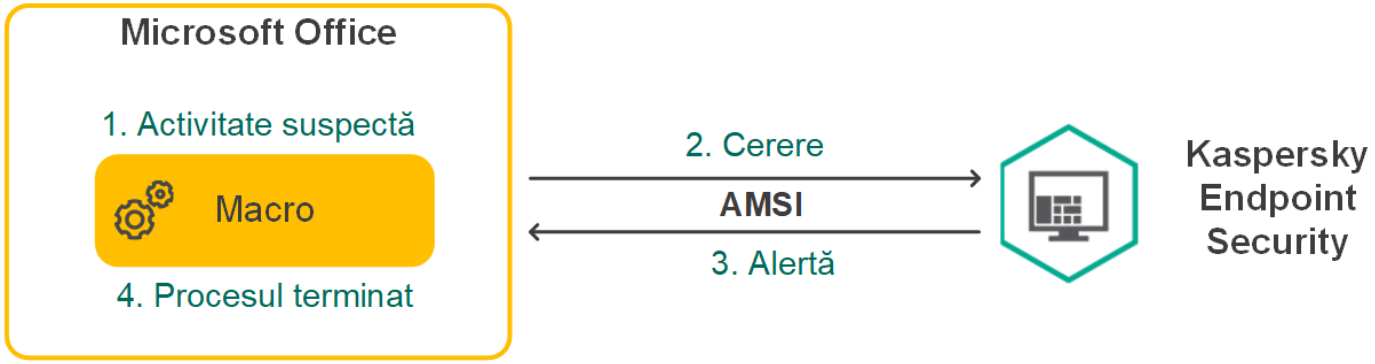


Autorizarea scanerului de coduri de bare

Protecție AMSI

Componenta Protecție AMSI are rolul de a susține interfața Antimalware Scan Interface de la Microsoft. *Antimalware Scan Interface (AMSI)* permite aplicațiilor terțe cu suport AMSI să trimită obiecte (de exemplu, scripturi PowerShell) către Kaspersky Endpoint Security pentru scanare suplimentară și primește apoi rezultatele scanării pentru aceste obiecte. Aplicațiile terțe pot include, de exemplu, aplicații Microsoft Office (vezi figura de mai jos). Pentru detalii despre AMSI, consultați documentația Microsoft.

Componenta Protecție AMSI poate doar să detecteze o amenințare și să notifice o aplicație terță despre aceasta. O aplicație terță, după primirea unei notificări despre o amenințare, nu permite efectuarea de acțiuni rău intenționate (de exemplu, aceasta încheie acțiunea).



Exemplu funcționare AMSI

Componenta Protecție AMSI poate refuza o solicitare de la o aplicație terță, de exemplu dacă această aplicație depășește numărul maxim de solicitări într-un interval specificat. Kaspersky Endpoint Security trimite informații despre o solicitare respinsă de la o aplicație terță către Serverul de administrare. Componenta AMSI Protection nu respinge solicitările de la acele aplicații terțe pentru care integrarea continuă cu componenta AMSI Protection este activată.

Componenta Protecție AMSI este disponibilă pentru următoarele sisteme de operare pentru stații de lucru și servere:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multi-session;
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise.
- Windows Server 2016 Essentials / Standard / Datacenter (inclusiv modul Server Core);
- Windows Server 2019 Essentials / Standard / Datacenter (inclusiv modul Server Core);
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (inclusiv modul Server Core);
- Windows Server 2025 Standard / Datacenter.

Activarea și dezactivarea componentei Protecție AMSI

În mod implicit, componenta Protecție AMSI este activată și funcționează în modul recomandat de Kaspersky (consultă tabelul de mai jos).

Cum se activează sau dezactivează componenta Protecție AMSI în Consola de administrare (MMC)

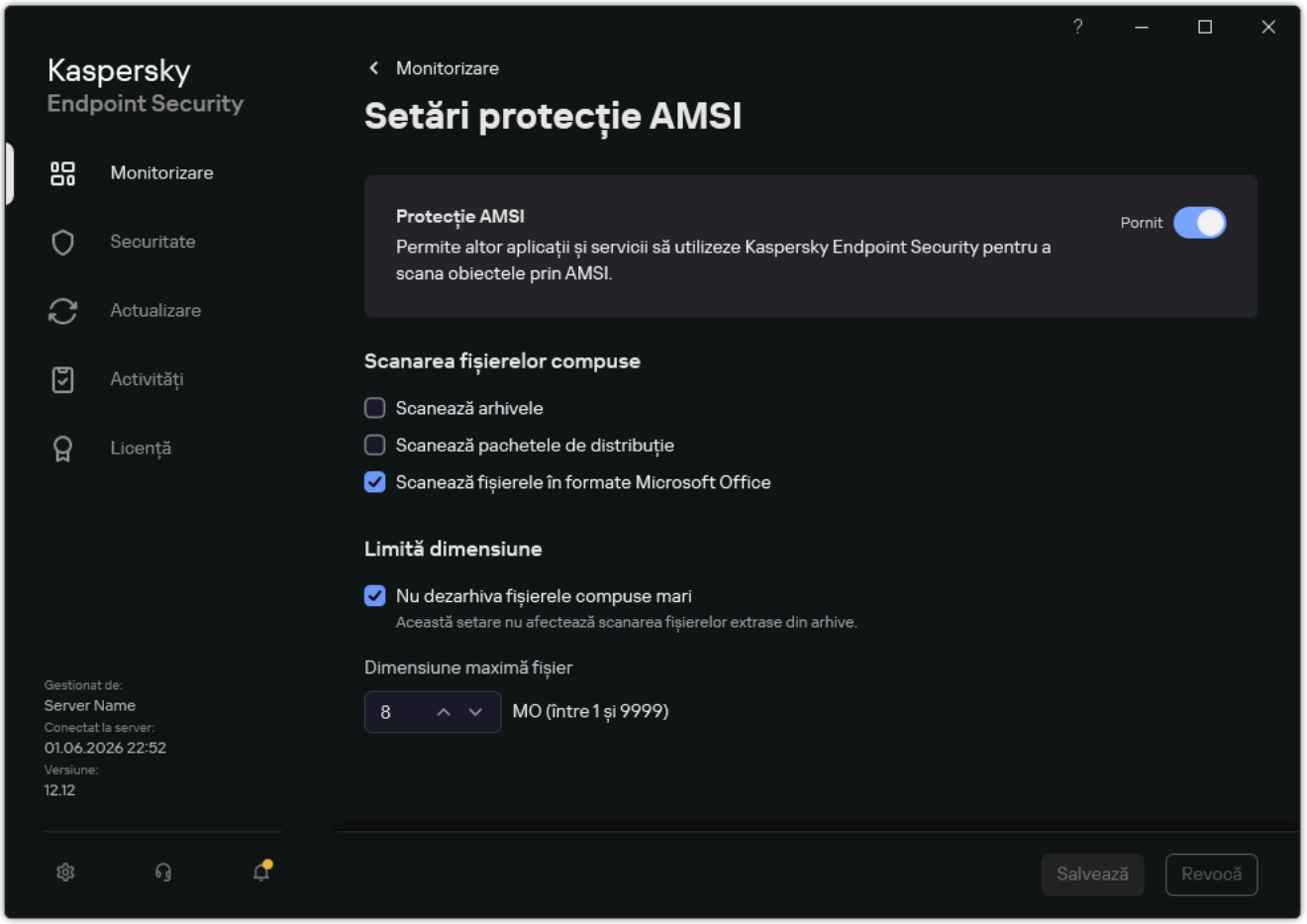
1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Essential Threat Protection** → **Scaner AMSI**.
4. Utilizează caseta de selectare **Scaner AMSI** pentru a activa sau a dezactiva componenta.
5. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se activează sau dezactivează componenta Protecție AMSI în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.
   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Host Threat Protection** → **AMSI Protection**.
5. Utilizați comutatorul **AMSI Protection ENABLED** pentru a activa sau a dezactiva componenta.
6. Salvați-vă modificările. Pentru a aplica politica pe computere, închide lacătele .

Cum se activează sau dezactivează componenta Protecție AMSI în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **Protecție AMSI**.



Setări protecție AMSI

3. Utilizați comutatorul **Protecție AMSI** pentru a activa sau a dezactiva componenta.
4. Salvați-vă modificările.

Setările componentei Protecție AMSI recomandate de experții Kaspersky

Parametru	Valoare	Descriere
Scanează arhivele	**Oprit**	Scanarea arhivelor ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE și a altor arhive. Aplicația scanează arhivele nu doar după extensie, dar și după format. La verificarea arhivelor, aplicația efectuează o dezarhivare recursivă. Acest lucru permite detectarea amenințărilor din arhivele cu mai multe niveluri (o arhivă într-o arhivă).
Scanează pachetele de distribuție	**Oprit**	Scanarea pachetelor de distribuție ale aplicațiilor terțe.
Scanează fișierele în formate Microsoft Office	**Pornit**	Scanează fișierele Microsoft Office (DOC, DOCX, XLS, PPT și alte extensii Microsoft). Fișierele în format Office includ și obiecte OLE. Aplicația scanează fișierele în format office mai mici de 1 MO, indiferent dacă această casetă de selectare este bifată sau nu.
Nu dezarhiva fișierele compuse mari	**Dimensiune maximă fișier**: 8 MO	Dacă această casetă de selectare este bifată, aplicația nu scanează fișierele compuse a căror dimensiune depășește valoarea specificată. În cazul în care această casetă de selectare este nebifată, aplicația scanează fișierele compuse indiferent de dimensiuni. Aplicația scanează fișierele mari extrase din arhive, indiferent dacă această casetă de selectare este bifată sau nu.

Optimizarea scanării fișierelor de către componenta Protecție AMSI

Poți optimiza scanarea fișierelor, reducând durata scanării și sporind viteza de funcționare a aplicației Kaspersky Endpoint Security. Poți selecta fișierele compuse care necesită scanare: arhive, pachete de distribuție sau fișiere în formate office. De asemenea, poți limita dimensiunea fișierelor compuse care urmează să fie scanate. Componenta Protecție AMSI nu va dezarhiva fișierele compuse mai mari decât dimensiunea specificată.

O tehnică obișnuită pentru ascunderea virușilor și a altor programe malware o reprezintă încorporarea acestora în fișiere compuse, precum arhivele. Pentru a detecta virușii și celelalte programe malware ascunse în acest mod, fișierul compus trebuie dezarhivat, fapt care poate încetini scanarea. Poți limita tipurile de fișiere compuse de scanat, accelerând astfel scanarea.

Cum se optimizează scanarea fișierelor de către componenta Protecție AMSI în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Essential Threat Protection** → **Scaner AMSI**.
4. În blocul **Scanare fișiere compuse**, specifică tipurile de fișiere compuse pe care dorești să le scanezi: arhive, pachete de distribuție sau fișiere în formate Office.
5. În blocul **Limită dimensiune**, efectuează una dintre următoarele acțiuni:
   - Pentru a bloca componenta Protecție AMSI să dezarhiveze fișiere compuse de dimensiuni mari, bifează caseta de selectare **Nu dezarhiva fișierele compuse mari** și specifică valoarea necesară. Componenta Protecție AMSI nu va dezarhiva fișierele compuse mai mari decât dimensiunea specificată.
   - Pentru a permite componentei Protecție AMSI să dezarhiveze fișierele compuse de dimensiuni mari, debifați caseta de selectare **Nu dezarhiva fișierele compuse mari**.

   Componenta Protecție AMSI scanează fișierele mari extrase din arhive, indiferent dacă este bifată sau nu caseta de selectare **Nu dezarhiva fișierele compuse mari**.
6. Salvați-vă modificările. Pentru a aplica politica pe computere, închide lacătele .

Cum se optimizează scanarea fișierelor de către componenta Protecție AMSI în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Host Threat Protection** → **AMSI Protection**.

5. În blocul **Scan of compound files**, specifică tipurile de fișiere compuse pe care dorești să le scanezi: arhive, pachete de distribuție sau fișiere în formate Office.

6. În blocul **Scan optimization**, efectuează una dintre următoarele acțiuni:

   - Pentru a bloca componenta Protecție AMSI să dezarhiveze fișiere compuse de dimensiuni mari, bifează caseta de selectare **Size limits enabled** și specifică valoarea necesară. Componenta Protecție AMSI nu va dezarhiva fișierele compuse mai mari decât dimensiunea specificată.

   - Pentru a permite componentei Protecție AMSI să dezarhiveze fișierele compuse de dimensiuni mari, debifați caseta de selectare **Size limits enabled**.

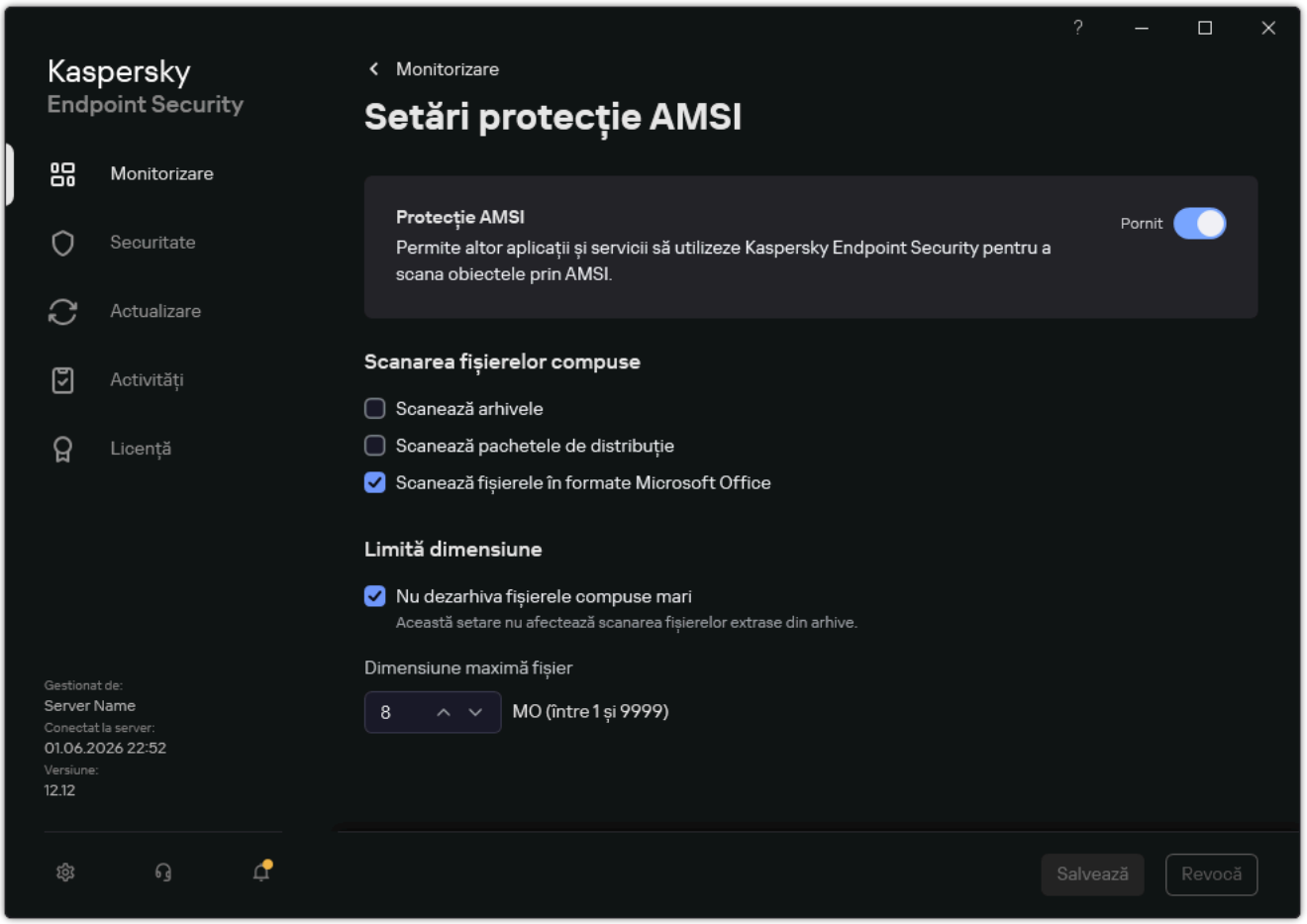
   Componenta Protecție AMSI scanează fișierele mari extrase din arhive, indiferent dacă este bifată sau nu caseta de selectare **Size limits enabled**.

7. Salvați-vă modificările. Pentru a aplica politica pe computere, închide lacătele.

Cum se optimizează scanarea fișierelor de către componenta Protecție AMSI în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul.

2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **Protecție AMSI**.



Setări protecție AMSI

3. În blocul **Scanarea fișierelor compuse**, specifică tipurile de fișiere compuse pe care dorești să le scanezi: arhive, pachete de distribuție sau fișiere în formate Office.

4. În blocul **Limită dimensiune**, efectuează una dintre următoarele acțiuni:

   - Pentru a bloca componenta Protecție AMSI să dezarhiveze fișiere compuse de dimensiuni mari, bifează caseta de selectare **Nu dezarhiva fișierele compuse mari** și specifică valoarea necesară. Componenta Protecție AMSI nu va dezarhiva fișierele compuse mai mari decât dimensiunea specificată.

   - Pentru a permite componentei Protecție AMSI să dezarhiveze fișierele compuse de dimensiuni mari, debifați caseta de selectare **Nu dezarhiva fișierele compuse mari**.

   Componenta Protecție AMSI scanează fișierele mari extrase din arhive, indiferent dacă este bifată sau nu caseta de selectare **Nu dezarhiva fișierele compuse mari**.

5. Salvați-vă modificările.

Web Threat Protection

Componenta Web Threat Protection previne descărcarea de pe Internet a fișierelor rău intenționate și, de asemenea, blochează site-urile web rău intenționate și de phishing. Componenta oferă protecție computerului cu ajutorul bazelor de date antivirus, a serviciului cloud Kaspersky Security Network și a analizei euristice.

Kaspersky Endpoint Security scanează traficul HTTP, HTTPS și FTP. Kaspersky Endpoint Security scanează adresele URL și adresele IP.

Pentru a utiliza componenta Web Threat Protection, trebuie să finalizezi configurarea inițială a aplicației:

- Pentru monitorizarea traficului HTTPS, activează scanarea conexiunilor criptate (activată în mod implicit).
- Selectează porturile pe care Kaspersky Endpoint Security trebuie să monitorizeze (implicit, aplicația monitorizează toate porturile).
- Selectează aplicațiile al căror trafic dorești să îl monitorizeze Kaspersky Endpoint Security. Majoritatea browserelor sunt deja prezente în lista de aplicații recomandate de Kaspersky. Dacă browserul tău lipsește din listă, adaugă-l manual.
- Îți recomandăm să injectezi un script de interacțiune a paginii web în traficul web (în mod implicit, injectarea de script este dezactivată). Acest script permite înregistrarea evenimentelor Web Threat Protection pentru jurnalul de evenimente al aplicației, jurnalul de evenimente al sistemului de operare și rapoarte.

Când un utilizator încearcă să deschidă un site web periculos sau de tip phishing, Kaspersky Endpoint Security va bloca accesul și va afișa un avertisment.

Activarea și dezactivarea Web Threat Protection

În mod implicit, componenta Web Threat Protection este activată și se execută cu setările recomandate de experții Kaspersky. Pentru Web Threat Protection, aplicația poate aplica diferite grupuri de setări. Aceste grupuri de setări care sunt stocate în aplicație sunt denumite *niveluri de securitate*: **Ridicat**, **Recomandat**, **Redus**. Setările pentru nivelul de securitate **Recomandat** al traficului web sunt considerate a fi setările optime recomandate de către experții de la Kaspersky (consultați tabelul de mai jos). Poți selecta unul dintre nivelurile preinstalate de securitate a traficului Web primit sau transmis prin protocoalele HTTP și FTP sau poți configura un nivel particularizat de securitate a traficului Web. Dacă modifici setările pentru nivelul de securitate a traficului Web, poți reveni oricând la setările recomandate pentru nivelul de securitate a traficului Web.

Poți selecta sau configura nivelul de securitate numai în Consola de administrare (MMC) sau în interfața locală a aplicației. Nu poți selecta sau configura nivelul de securitate în Web Console sau Cloud Console.

Cum se activează sau dezactivează componenta Web Threat Protection în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Essential Threat Protection** → **Web Threat Protection**.
4. Utilizează caseta de selectare **Web Threat Protection** pentru a activa sau a dezactiva componenta.
5. Dacă ați activat componenta, efectuați una dintre următoarele acțiuni în blocul **Nivel de securitate**:
   - Dacă doriți să aplicați unul dintre nivelurile de securitate presetate, selectați-l folosind glisorul:
     - **Ridicat**. Nivelul de securitate la care componenta Web Threat Protection efectuează o scanare maximă a traficului web pe care un computer îl primește prin protocoalele HTTP și FTP. Web Threat Protection scanează detaliat toate obiectele de trafic Web, utilizând setul complet de baze de date ale aplicației, și efectuează cea mai riguroasă analiză euristică posibil.
     - **Recomandat**. Nivelul de securitate care asigură raportul optim între performanțele aplicației și securitatea traficului Web. Componenta Web Threat Protection efectuează analiza euristică la nivelul Scanare medie. Acest nivel de securitate a traficului Web este recomandat de specialiștii Kaspersky. Valorile setărilor pentru nivelul de securitate recomandat sunt furnizate în tabelul de mai jos.
     - **Redus**. Setările acestui nivel de securitate a traficului web asigură viteza maximă de scanare a traficului web. Componenta Web Threat Protection efectuează analiza euristică la nivelul Scanare ușoară.
   - Dacă doriți să configurați un nivel de securitate personalizat, faceți clic pe butonul **Setări** și definiți propriile setări pentru componentă.

     Puteți restabili valorile nivelurilor de securitate prestabilite făcând clic pe butonul **În mod implicit**.

6. În blocul **Acțiune la detectarea amenințării**, selectați acțiunea pe care aplicația Kaspersky Endpoint Security să o efectueze asupra obiectelor de trafic web rău intenționate:

   - **Blochează**. Dacă această opțiune este selectată și un obiect infectat este detectat în traficul web, componenta Web Threat Protection blochează accesul la obiectul respectiv și afișează un mesaj în browser.

   - **Informează**. Dacă această opțiune este selectată și un obiect infectat este detectat în traficul web, Kaspersky Endpoint Security permite descărcarea acestui obiect pe computer, dar adaugă informații despre obiectul infectat în lista de amenințări active.

7. Salvați-vă modificările.

Cum se activează sau dezactivează componenta Web Threat Protection în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **Communication & Web Protection** → **Web Threat Protection**.

5. Utilizați comutatorul **Web Threat Protection ENABLED** pentru a activa sau a dezactiva componenta.

6. În blocul **Action on threat detection**, selectați acțiunea pe care aplicația Kaspersky Endpoint Security să o efectueze asupra obiectelor de trafic web rău intenționate:

   - **Block**. Dacă această opțiune este selectată și un obiect infectat este detectat în traficul web, componenta Web Threat Protection blochează accesul la obiectul respectiv și afișează un mesaj în browser.

   - **Allow, inform, or prompt for action (depends on OS)**. Dacă această opțiune este selectată și un obiect infectat este detectat în traficul web, Kaspersky Endpoint Security permite descărcarea acestui obiect pe computer, dar adaugă informații despre obiectul infectat în lista de amenințări active.

7. Daca este necesar, întocmește o listă de adrese web de încredere.

8. Salvați-vă modificările.

Cum se activează sau dezactivează componenta Web Threat Protection

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **Web Threat Protection**.

3. Utilizați comutatorul **Web Threat Protection** pentru a activa sau a dezactiva componenta.

4. Dacă ați activat componenta, efectuați una dintre următoarele acțiuni în blocul **Nivel de securitate**:

   - Dacă doriți să aplicați unul dintre nivelurile de securitate presetate, selectați-l folosind glisorul:

     - **Ridicat**. Nivelul de securitate la care componenta Web Threat Protection efectuează o scanare maximă a traficului web pe care un computer îl primește prin protocoalele HTTP și FTP. Web Threat Protection scanează detaliat toate obiectele de trafic Web, utilizând setul complet de baze de date ale aplicației, și efectuează cea mai riguroasă analiză euristică posibil.

     - **Recomandat**. Nivelul de securitate care asigură raportul optim între performanțele aplicației și securitatea traficului Web. Componenta Web Threat Protection efectuează analiza euristică la nivelul Scanare medie. Acest nivel de securitate a traficului Web este recomandat de specialiștii Kaspersky. Valorile setărilor pentru nivelul de securitate recomandat sunt furnizate în tabelul de mai jos.

     - **Redus**. Setările acestui nivel de securitate a traficului web asigură viteza maximă de scanare a traficului web. Componenta Web Threat Protection efectuează analiza euristică la nivelul Scanare ușoară.

   - Dacă dorești să configurezi un nivel de securitate personalizat, fă clic pe butonul **Setări avansate** și definește propriile setări pentru componentă.

     Puteți restabili valorile nivelurilor de securitate prestabilite făcând clic pe butonul **Restaurare nivel recomandat de securitate**.

5. În blocul **Acțiune la detectarea amenințării**, selectați acțiunea pe care aplicația Kaspersky Endpoint Security să o efectueze asupra obiectelor de trafic web rău intenționate:

   - **Blochează**. Dacă această opțiune este selectată și un obiect infectat este detectat în traficul web, componenta Web Threat Protection blochează accesul la obiectul respectiv și afișează un mesaj în browser.

   - **Informează**. Dacă această opțiune este selectată și un obiect infectat este detectat în traficul web, Kaspersky Endpoint Security permite descărcarea acestui obiect pe computer, dar adaugă informații despre obiectul infectat în lista de amenințări active.

6. Salvați-vă modificările.

Setări Web Threat Protection recomandate de experții Kaspersky (nivel de securitate recomandat)

Parametru	Valoare	Descriere
Verifică adresa web în baza de date cu adrese web rău intenționate	**Pornit**	Scanarea linkurilor pentru a determina dacă sunt incluse în baza de date cu adrese URL rău intenționate vă permite să urmăriți site-urile web care au fost adăugate în lista respinse. Baza de date de adrese Web rău intenționate este întreținută de Kaspersky, fiind inclusă în pachetul de instalare a aplicației și actualizată prin actualizări ale bazei de date Kaspersky Endpoint Security.
Verifică adresa web în baza de date cu adrese web de phishing	**Pornit**	Baza de date de adrese Web de phishing include adresele Web ale site-urilor Web despre care se cunoaște în prezent că sunt utilizate pentru a lansa atacuri de phisihing. Kaspersky completează această bază de date cu linkuri de phishing cu adrese obținute de la organizația internațională cunoscută ca Anti-Phishing Working Group. Baza de date de adrese de phishing este inclusă în pachetul de instalare a aplicației și completată cu actualizări ale bazei de date Kaspersky Endpoint Security.
Utilizează analiza euristică (Web Threat Protection)	**Scanare medie**	Tehnologia a fost dezvoltată pentru detectarea amenințărilor care nu se pot detecta utilizând versiunea curentă a bazelor de date ale aplicației Kaspersky. Aceasta detectează fișiere care este posibil să fie infectate cu un virus necunoscut sau cu o variație nouă a unui virus cunoscut. Atunci când traficul web este scanat pentru viruși și alte aplicații care prezintă o amenințare, analizorul euristic execută instrucțiunile din fișierele executabile. Numărul de instrucțiuni executate de analizorul euristic depinde de nivelul specificat pentru analizorul euristic. Nivelul analizei euristice asigură un echilibru între gradul de detaliere a căutării de amenințări noi, gradul de solicitare a resurselor sistemului de operare și durata analizei euristice.
Utilizează analiza euristică (Anti-Phishing)	**Pornit**	Tehnologia a fost dezvoltată pentru detectarea amenințărilor care nu se pot detecta utilizând versiunea curentă a bazelor de date ale aplicației Kaspersky. Aceasta detectează fișiere care este posibil să fie infectate cu un virus necunoscut sau cu o variație nouă a unui virus cunoscut.
Acțiune la detectarea amenințării	**Blochează**	Dacă această opțiune este selectată și un obiect infectat este detectat în traficul web, componenta Web Threat Protection blochează accesul la obiectul respectiv și afișează un mesaj în browser.

Configurarea metodelor de detectare a adreselor web rău intenționate

Web Threat Protection detectează adresele web rău intenționate folosind baze de date antivirus Serviciu cloud Kaspersky Security Network, și analiza euristică.

Poți selecta metode de detectare a adreselor web rău intenționate numai în Consola de administrare (MMC) sau în interfața locală a aplicației. Nu poți selecta metode de detectare a adreselor web rău intenționate în Web Console sau Cloud Console. Opțiunea implicită este verificarea adreselor web în baza de date cu adrese rău intenționate cu analiza euristică (scanare medie).

Scanarea folosind baza de date cu adrese rău intenționate

Scanarea linkurilor pentru a determina dacă sunt incluse în baza de date cu adrese URL rău intenționate vă permite să urmăriți site-urile web care au fost adăugate în lista respinse. Baza de date de adrese Web rău intenționate este întreținută de Kaspersky, fiind inclusă în pachetul de instalare a aplicației și actualizată prin actualizări ale bazei de date Kaspersky Endpoint Security.

Kaspersky Endpoint Security scanează toate linkurile pentru a determina dacă acestea sunt listate în baze de date de adrese URL dăunătoare. Setările de scanare a conexiunii securizate a aplicației nu afectează funcționalitatea de scanare a linkurilor. Cu alte cuvinte, dacă scanarea conexiunilor criptate este dezactivată, Kaspersky Endpoint Security verifică linkurile în bazele de date cu adrese web rău intenționate, chiar dacă traficul de rețea este transmis printr-o conexiune criptată.

Cum se activează sau se dezactivează verificarea adreselor web în baza de date cu adrese web rău intenționate folosind Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Essential Threat Protection** → **Web Threat Protection**.
4. În blocul **Nivel de securitate**, fă clic pe butonul **Setări**.
5. În fereastra care se deschide, în blocul **Metode de scanare**, bifați sau debifați caseta de selectare **Verifică adresa web în baza de date cu adrese web rău intenționate** pentru a activa sau dezactiva verificarea adreselor în baza de date cu adrese web rău intenționate.
6. Salvați-vă modificările.

Cum se activează sau se dezactivează verificarea adreselor în baza de date cu adrese rău intenționate din interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **Web Threat Protection**.
3. Fă clic pe **Setări avansate**.
4. În blocul **Metode de scanare**, bifați sau debifați caseta de selectare **Verifică adresa web în baza de date cu adrese web rău intenționate** pentru a activa sau dezactiva verificarea adreselor în baza de date cu adrese web rău intenționate.
5. Salvați-vă modificările.

Analiză euristică

În timpul analizei euristice, Kaspersky Endpoint Security analizează activitatea aplicațiilor în sistemul de operare. Analiza euristică poate detecta amenințări pentru care în prezent nu există nicio înregistrare în bazele de date Kaspersky Endpoint Security.

Atunci când traficul web este scanat pentru viruși și alte aplicații care prezintă o amenințare, analizorul euristic execută instrucțiunile din fișierele executabile. Numărul de instrucțiuni executate de analizorul euristic depinde de nivelul specificat pentru analizorul euristic. Nivelul analizei euristice asigură un echilibru între gradul de detaliere a căutării de amenințări noi, gradul de solicitare a resurselor sistemului de operare și durata analizei euristice.

Cum se activează sau dezactivează utilizarea analizei euristice în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Essential Threat Protection** → **Web Threat Protection**.
4. În blocul **Nivel de securitate**, fă clic pe butonul **Setări**.
5. În fereastra care se deschide, în blocul **Metode de scanare**, bifează caseta de selectare **Utilizează analiza euristică** dacă dorești ca aplicația să utilizeze analiza euristică atunci când scanează traficul web pentru viruși și alte programe malware.
6. Utilizați glisorul pentru a seta nivelul analizei euristice: **scanare ușoară**, **scanare medie** sau **scanare profundă**.

   Atunci când traficul web este scanat pentru viruși și alte aplicații care prezintă o amenințare, analizorul euristic execută instrucțiunile din fișierele executabile. Numărul de instrucțiuni executate de analizorul euristic depinde de nivelul specificat pentru analizorul euristic. Nivelul analizei euristice asigură un echilibru între gradul de detaliere a căutării de amenințări noi, gradul de solicitare a resurselor sistemului de operare și durata analizei euristice.
7. Salvați-vă modificările.

Cum se activează sau dezactivează utilizarea analizei euristice în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul .
2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **Web Threat Protection**.
3. Fă clic pe **Setări avansate**.
4. În blocul **Metode de scanare**, bifați caseta de selectare **Utilizează analiza euristică** dacă doriți ca aplicația să utilizeze analiza euristică atunci când scanează traficul web pentru viruși și alte programe malware.

   Atunci când traficul web este scanat pentru viruși și alte aplicații care prezintă o amenințare, analizorul euristic execută instrucțiunile din fișierele executabile. Numărul de instrucțiuni executate de analizorul euristic depinde de nivelul specificat pentru analizorul euristic. Nivelul analizei euristice asigură un echilibru între gradul de detaliere a căutării de amenințări noi, gradul de solicitare a resurselor sistemului de operare și durata analizei euristice.
5. Salvați-vă modificările.

Anti-Phishing

Web Threat Protection verifică linkurile pentru a vedea dacă aparțin adreselor web de phishing. Acest lucru ajută la prevenire *atacurilor de tip phishing*. Un atac de tip phishing poate fi deghizat, de exemplu, într-un mesaj de e-mail presupus a veni de la bancă în care este inclus un link către site-ul Web oficial al băncii respective. Dacă faci clic pe link, vei fi direcționat către o copie fidelă a site-ului Web al băncii, browserul afișând inclusiv adresa Web reală a băncii, chiar dacă tu ai accesat un site falsificat. Începând din acest moment, toate acțiunile pe care le faci pe site sunt urmărite și pot fi utilizate pentru a ți se sustrage bani.

Deoarece linkurile către site-uri web de phishing pot fi primite și din alte surse decât mesajele de e-mail, precum programele de mesagerie instantanee, componenta Web Threat Protection monitorizează la nivelul traficului web încercările de accesare a unui site web de phishing și blochează accesul la astfel de site-uri web. Listele de adrese URL de phishing sunt incluse în kitul de distribuire Kaspersky Endpoint Security.

Poți configura componenta Anti-Phishing numai în Consola de administrare (MMC) sau în interfața locală a aplicației. Nu poți configura componenta Anti-Phishing în Web Console sau Cloud Console. În mod implicit, componenta Anti-Phishing cu analiză euristică este activată.

Cum se activează sau dezactivează componenta Anti-Phishing în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Essential Threat Protection** → **Web Threat Protection**.
4. În blocul **Nivel de securitate**, fă clic pe butonul **Setări**.

5. În fereastra care se deschide, în blocul **Setări anti-phishing**, bifați sau debifați caseta de selectare **Verifică adresa web în baza de date cu adrese web de phishing** pentru a activa sau dezactiva componenta Anti-phishing.

   Baza de date de adrese Web de phishing include adresele Web ale site-urilor Web despre care se cunoaște în prezent că sunt utilizate pentru a lansa atacuri de phisihing. Kaspersky completează această bază de date cu linkuri de phishing cu adrese obținute de la organizația internațională cunoscută ca Anti-Phishing Working Group. Baza de date de adrese de phishing este inclusă în pachetul de instalare a aplicației și completată cu actualizări ale bazei de date Kaspersky Endpoint Security.

6. Bifați caseta de selectare **Utilizează analiza euristică** dacă doriți ca aplicația să utilizeze analiza euristică atunci când scanează pagini web pentru linkuri de phishing.

   În timpul analizei euristice, Kaspersky Endpoint Security analizează activitatea aplicațiilor în sistemul de operare. Analiza euristică poate detecta amenințări pentru care în prezent nu există nicio înregistrare în bazele de date Kaspersky Endpoint Security.

   Pentru a scana link-uri, pe lângă baza de date antivirus și analiza euristică, poți utiliza bazele de date Kaspersky Security Network privind reputația.

7. Salvați-vă modificările.

Cum se activează sau dezactivează componenta Anti-Phishing în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Essential Threat Protection → Web Threat Protection**.

3. Fă clic pe **Setări avansate**.

4. Dacă doriți ca componenta Web Threat Protection să verifice linkurile în bazele de date ale adreselor URL de phishing, bifați caseta de selectare **Verifică adresa web în baza de date cu adrese web de phishing** blocul **Anti-Phishing**. Baza de date de adrese Web de phishing include adresele Web ale site-urilor Web despre care se cunoaște în prezent că sunt utilizate pentru a lansa atacuri de phisihing. Kaspersky completează această bază de date cu linkuri de phishing cu adrese obținute de la organizația internațională cunoscută ca Anti-Phishing Working Group. Baza de date de adrese de phishing este inclusă în pachetul de instalare a aplicației și completată cu actualizări ale bazei de date Kaspersky Endpoint Security.

5. Bifați caseta de selectare **Utilizează analiza euristică** dacă doriți ca aplicația să utilizeze analiza euristică atunci când scanează pagini web pentru linkuri de phishing.

   În timpul analizei euristice, Kaspersky Endpoint Security analizează activitatea aplicațiilor în sistemul de operare. Analiza euristică poate detecta amenințări pentru care în prezent nu există nicio înregistrare în bazele de date Kaspersky Endpoint Security.

   Pentru a scana link-uri, pe lângă baza de date antivirus și analiza euristică, poți utiliza bazele de date Kaspersky Security Network privind reputația.

6. Salvați-vă modificările.

Crearea listei de adrese web de încredere

Pe lângă site-urile web rău intenționate și de phishing, Web Threat Protection poate bloca alte site-uri web. De exemplu, Web Threat Protection blochează traficul HTTP care nu îndeplinește standardele RFC. Poți crea o listă de adrese URL în al căror conținut ai încredere. Componenta Web Threat Protection nu analizează existența virușilor și a altor amenințări în informațiile provenite de la adrese URL de încredere. Această opțiune poate fi utilă, de exemplu, atunci când componenta Web Threat Protection interferează cu descărcarea unui fișier de pe un site web cunoscut.

O adresă URL poate fi adresa unei anumite pagini web sau adresa unui site web.

Modificarea listei de adrese web de încredere dintr-o politică poate fi blocată de proprietățile politicii principale. Pentru a modifica lista, trebuie să permiteți modificarea setărilor zonei de încredere în Web Console („lacătul" trebuie să fie deblocat).

Zonele de încredere sunt grupate diferit în Consola de administrare (MMC) și în Web Console. De asemenea, modul în care se împiedică modificarea parametrilor zonei de încredere este diferit („lacăte" diferite). Vă recomandăm să utilizați exclusiv Web Console pentru gestionarea aplicației. În cazul în care configurați zona de încredere pe console diferite, este posibil ca plug-inul de gestionare să reseteze „lacătul" la starea implicită.

Cum se adăugă o adresă web de încredere în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Essential Threat Protection** → **Web Threat Protection**.
4. În blocul **Nivel de securitate**, fă clic pe butonul **Setări**.
5. În fereastra care se deschide, selectează fila **Adrese web de încredere**.
6. Bifați caseta de selectare **Nu se scanează traficul web de la adresele web de încredere**.

   Dacă este selectată această opțiune, componenta Web Threat Protection nu scanează conținutul paginilor sau al site-urilor web ale căror adrese sunt incluse în lista de adrese web de încredere. Puteți adăuga la o listă de adrese URL de încredere atât adresa, cât și masca de adresă a unei pagini/unui site Web.
7. Creează o listă de adrese URL/pagini Web în al căror conținut ai încredere.

   Kaspersky Endpoint Security acceptă caracterele `*` și `?` la introducerea unei măști.

   De asemenea, poți importa o listă de adrese web de încredere dintr-un fișier XML.
8. Salvați-vă modificările.

Cum se adaugă o adresă web de încredere în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Communication & Web Protection** → **Web Threat Protection**.
5. Fă clic pe **Trusted web addresses**.
6. Creează o listă de adrese URL/pagini Web în al căror conținut ai încredere.

   Kaspersky Endpoint Security acceptă caracterele `*` și `?` la introducerea unei măști.

   De asemenea, poți importa o listă de adrese web de încredere dintr-un fișier JSON.
7. Salvați-vă modificările.

Cum se adaugă o adresă web de încredere în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **Web Threat Protection**.
3. Fă clic pe **Setări avansate**.
4. Bifați caseta de selectare **Nu scana traficul web de la adrese URL de încredere**.

   Dacă este selectată această opțiune, componenta Web Threat Protection nu scanează conținutul paginilor sau al site-urilor web ale căror adrese sunt incluse în lista de adrese web de încredere. Puteți adăuga la o listă de adrese URL de încredere atât adresa, cât și masca de adresă a unei pagini/unui site Web.
5. Creează o listă de adrese URL/pagini Web în al căror conținut ai încredere.

   Kaspersky Endpoint Security acceptă caracterele `*` și `?` la introducerea unei măști.

   De asemenea, poți importa o listă de adrese web de încredere dintr-un fișier XML.
6. Salvați-vă modificările.

Ca rezultat, Web Threat Protection nu scanează traficul adreselor web de încredere. Utilizatorul poate deschide întotdeauna un site web de încredere și poate descărca un fișier de pe acel site web. Dacă nu ați putut obține acces la site-ul web, verificați setările componentelor Scanare conexiuni criptate, Control Web și Monitorizare porturi de rețea. Dacă Kaspersky Endpoint Security detectează un fișier descărcat de pe un site web de încredere ca fiind rău intenționat, poți adăuga acest fișier la excluderi.

Poți, de asemenea, să creezi o listă generală de excluderi pentru conexiunile criptate. În acest caz, Kaspersky Endpoint Security nu scanează traficul HTTPS al adreselor web de încredere atunci când componentele Web Threat Protection, Mail Threat Protection și Control Web își fac treaba.

Exportul și importul listei de adrese URL de încredere

Puteți exporta lista de adrese URL de încredere într-un fișier XML. Apoi puteți modifica fișierul pentru a adăuga, de exemplu, un număr mare de adrese URL de același tip. De asemenea, puteți utiliza funcția de export/import pentru a face o copie de rezervă a listei de adrese URL de încredere sau pentru a migra lista pe un alt server.

Cum se exportă și se importă o listă de adrese URL de încredere în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Essential Threat Protection → Web Threat Protection**.
4. În blocul **Nivel de securitate**, fă clic pe butonul **Setări**.
5. În fereastra care se deschide, selectează fila **Adrese web de încredere**.
6. Pentru a exporta lista de adrese URL de încredere:
   a. Selectați adresele URL de încredere pe care doriți să le exportați. Pentru a selecta mai multe porturi, utilizați tastele **CTRL** sau **SHIFT**.

      Dacă nu ați selectat nicio adresă URL de încredere, Kaspersky Endpoint Security va exporta toate adresele URL.

   b. Faceți clic pe linkul **Exportă**.
   c. În fereastra care se deschide, specificați numele fișierului XML în care doriți să exporți lista de adrese URL de încredere și selectați directorul în care doriți să salvați acest fișier.
   d. Salvați fișierul.

      Kaspersky Endpoint Security exportă întreaga listă de adrese URL de încredere în fișierul XML.
7. Pentru a importa lista de adrese de încredere:
   a. Faceți clic pe linkul **Importă**.

      În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de adrese de încredere.

   b. Deschideți fișierul.

      În cazul în care computerul are deja o listă de adrese de încredere, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul XML.
8. Salvați-vă modificările.

Cum se exportă și se importă o listă de adrese URL de încredere în Consola Web și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management → Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **Communication & Web Protection** → **Web Threat Protection**.

5. Pentru a exporta lista excluderilor din blocul **Rules list**:

   a. Selectați adresele URL de încredere pe care doriți să le exportați.

   b. Fă clic pe butonul → **Export**.

   Kaspersky Endpoint Security exportă lista de adrese web de încredere într-un fișier JSON în directorul de descărcări implicit.

6. Pentru a importa lista de excluderi în blocul **Rules list**:

   a. Fă clic pe butonul → **Import**.

   În fereastra care se deschide, selectați fișierul JSON din care doriți să importați lista de adrese de încredere.

   b. Deschideți fișierul.

   În cazul în care computerul are deja o listă de adrese de încredere, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul JSON.

7. Salvați-vă modificările.

Mail Threat Protection

Componenta Mail Threat Protection scanează atașările mesajelor de e-mail primite și trimise în vederea detectării virușilor și a altor amenințări. Componenta oferă protecție computerului cu ajutorul bazelor de date antivirus, a serviciului cloud Kaspersky Security Network și a analizei euristice.

Mail Threat Protection poate scana atât mesajele primite, cât și cele trimise. Aplicația acceptă POP3, SMTP, IMAP și NNTP în următorii clienți de e-mail:

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail
- MyOffice Mail
- R7-Office Organizer

Pentru a scana traficul în clienții de e-mail Mozilla Thunderbird, MyOffice Mail și R7-Office Organizer, trebuie să adaugi un certificat Kaspersky la magazinul de certificate și să selectezi propriul magazin de certificate.

Mail Threat Protection nu acceptă alte protocoale și clienți de e-mail.

Este posibil ca Mail Threat Protection să nu poată obține întotdeauna acces *la nivel de protocol* la mesaje (de exemplu, atunci când utilizați soluția Microsoft Exchange). Din acest motiv, Mail Threat Protection include o extensie pentru Microsoft Office Outlook. Extensia permite scanarea mesajelor la *nivelul clientului de mail*. Extensia Mail Threat Protection acceptă versiunile pe 32 de biți și pe 64 de biți ale Outlook 2010, 2013, 2016, 2019, 2021, 2024 și 365. Pe computerele bazate pe arhitectura Arm, extensia Mail Threat Protection acceptă versiunile pe 32 de biți și 64 de biți ale Outlook 2016, Outlook 2021, Outlook 2024 și Outlook 365 pentru Arm64.

Componenta Mail Threat Protection nu scanează mesajele dacă clientul de e-mail este deschis într-un browser.

Când un fișier rău intenționat este detectat într-un atașament, Kaspersky Endpoint Security adaugă informații despre acțiunea efectuată la subiectul mesajului, de exemplu, *[Mesajul a fost procesat]<subiect mesaj>*.

Activarea și dezactivarea Mail Threat Protection

În mod implicit, componenta Mail Threat Protection este activată și se execută cu setările recomandate de experții Kaspersky. Pentru Mail Threat Protection, aplicația poate aplica diferite grupuri de setări. Aceste grupuri de setări care sunt stocate în aplicație sunt denumite *niveluri de securitate*: **Ridicat**, **Recomandat**, **Redus**. Setările pentru nivelul de securitate a e-mailurilor **Recomandat** sunt considerate a fi setările optime recomandate de către experții de la Kaspersky (consultați tabelul de mai jos). Poți selecta unul dintre nivelurile preinstalate de securitate a e-mailului sau poți configura un nivel particularizat de securitate a e-mailului. Dacă ai modificat setările pentru nivelul de securitate a e-mailului, poți reveni oricând la setările recomandate pentru nivelul de securitate a e-mailului.

Dacă lucrezi cu clientul de e-mail Mozilla Thunderbird, componenta Mail Threat Protection nu scanează de viruși și alte amenințări mesajele transmise prin protocolul IMAP dacă sunt utilizate filtre pentru mutarea mesajelor din directorul Inbox.

Cum se activează sau dezactivează componenta Mail Threat Protection în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Essential Threat Protection** → **Mail Threat Protection**.
4. Utilizează caseta de selectare **Mail Threat Protection** pentru a activa sau a dezactiva componenta.

5. Dacă ați activat componenta, efectuați una dintre următoarele acțiuni în blocul **Nivel de securitate**:

   - Dacă doriți să aplicați unul dintre nivelurile de securitate presetate, selectați-l folosind glisorul:

     - **Ridicat**. Atunci când este selectat acest nivel de securitate pentru e-mail, componenta Mail Threat Protection scanează mesajele de e-mail cât mai complet. Componenta Mail Threat Protection scanează mesajele primite și trimise și efectuează o analiză euristică profundă. Nivelul Ridicat de securitate a e-mailurilor este recomandat pentru mediile cu risc ridicat. Un exemplu de astfel de mediu este o conexiune la un serviciu de e-mail gratuit de la o rețea de domiciliu neapărată de o protecție pentru e-mail centralizată.

     - **Recomandat**. Nivelul de securitate pentru e-mail care asigură echilibrul optim între performanțele aplicației și securitatea pentru e-mail. Componenta Mail Threat Protection scanează mesajele de e-mail primite și trimise și efectuează o analiză euristică de nivel mediu. Acest nivel de securitate pentru e-mail este recomandat de specialiștii de la Kaspersky. Valorile setărilor pentru nivelul de securitate recomandat sunt furnizate în tabelul de mai jos.

     - **Redus**. Atunci când este selectat acest nivel de securitate pentru e-mail, componenta Mail Threat Protection scanează numai mesajele de e-mail primite, efectuează o analiză euristică rapidă și nu scanează arhivele atașate la mesaje de e-mail. La acest nivel de securitate pentru e-mail, componenta Mail Threat Protection scanează mesajele de e-mail la viteză maximă și utilizează un minim de resurse ale sistemului de operare. Nivelul Redus de securitate pentru e-mail este recomandat pentru lucrul în medii bine protejate. Un exemplu de astfel de mediu poate fi o rețea LAN de întreprindere care deține securitate centralizată pentru e-mail.

   - Dacă doriți să configurați un nivel de securitate personalizat, faceți clic pe butonul **Setări** și definiți propriile setări pentru componentă.

     Puteți restabili valorile nivelurilor de securitate prestabilite făcând clic pe butonul **În mod implicit**.

6. În blocul **Acțiune la detectarea amenințării**, selectează acțiunea pe care aplicația Kaspersky Endpoint Security trebuie să o efectueze asupra obiectelor rău intenționate:

   - **Dezinfectează; șterge dacă dezinfectarea nu reușește**. Când un obiect infectat este detectat într-un mesaj de intrare sau de ieșire, aplicația încearcă să dezinfecteze obiectul detectat. Utilizatorul va putea accesa mesajul cu o atașare sigură. Dacă obiectul nu poate fi dezinfectat, aplicația șterge obiectul infectat. Aplicația adaugă informații despre acțiunea efectuată la subiectul mesajului: *[Mesajul a fost procesat] <subiect mesaj>*.

   - **Dezinfectează; blochează dacă dezinfectarea nu reușește**. Când un obiect infectat este detectat într-un mesaj de intrare, aplicația încearcă să dezinfecteze obiectul detectat. Utilizatorul va putea accesa mesajul cu o atașare sigură. Dacă obiectul nu poate fi dezinfectat, aplicația adaugă un avertisment subiectului mesajului. Utilizatorul va putea accesa mesajul cu atașarea originală. Când un obiect infectat este detectat într-un mesaj de ieșire, aplicația încearcă să dezinfecteze obiectul detectat. Dacă obiectul nu poate fi dezinfectat, aplicația blochează transmiterea mesajului, iar clientul de e-mail afișează o eroare.

   - **Blochează**. Dacă un obiect infectat este detectat într-un mesaj de intrare, aplicația adaugă un avertisment la subiectul mesajului. Utilizatorul va putea accesa mesajul cu atașarea originală. Dacă un obiect infectat este detectat într-un mesaj de ieșire, aplicația blochează transmiterea mesajului, iar clientul de e-mail afișează o eroare.

7. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se activează sau dezactivează componenta Mail Threat Protection în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Communication & Web Protection** → **Mail Threat Protection**.
5. Utilizați comutatorul **Mail Threat Protection ENABLED** pentru a activa sau a dezactiva componenta.
6. În blocul **Action on threat detection**, selectează acțiunea pe care aplicația Kaspersky Endpoint Security trebuie să o efectueze asupra obiectelor rău intenționate:

   - **Disinfect, delete if disinfection fails**. Când un obiect infectat este detectat într-un mesaj de intrare sau de ieșire, aplicația încearcă să dezinfecteze obiectul detectat. Utilizatorul va putea accesa mesajul cu o atașare sigură. Dacă obiectul nu poate fi dezinfectat, aplicația șterge obiectul infectat. Aplicația adaugă informații despre acțiunea efectuată la subiectul mesajului: *[Mesajul a fost procesat] <subiect mesaj>*.
   - **Disinfect, block if disinfection fails**. Când un obiect infectat este detectat într-un mesaj de intrare, aplicația încearcă să dezinfecteze obiectul detectat. Utilizatorul va putea accesa mesajul cu o atașare sigură. Dacă obiectul nu poate fi dezinfectat, aplicația adaugă un avertisment subiectului mesajului. Utilizatorul va putea accesa mesajul cu atașarea originală. Când un obiect infectat este detectat într-un mesaj de ieșire, aplicația încearcă să dezinfecteze obiectul detectat. Dacă obiectul nu poate fi dezinfectat, aplicația blochează transmiterea mesajului, iar clientul de e-mail afișează o eroare.
   - **Block**. Dacă un obiect infectat este detectat într-un mesaj de intrare, aplicația adaugă un avertisment la subiectul mesajului. Utilizatorul va putea accesa mesajul cu atașarea originală. Dacă un obiect infectat este detectat într-un mesaj de ieșire, aplicația blochează transmiterea mesajului, iar clientul de e-mail afișează o eroare.
7. Dacă este necesar, editează setările avansate ale componentei Mail Threat Protection.
8. Salvați-vă modificările.

Cum se activează sau dezactivează componenta Mail Threat Protection în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **Mail Threat Protection**.
3. Utilizați comutatorul **Mail Threat Protection** pentru a activa sau a dezactiva componenta.

4. Dacă ați activat componenta, efectuați una dintre următoarele acțiuni în blocul **Nivel de securitate**:

   - Dacă doriți să aplicați unul dintre nivelurile de securitate presetate, selectați-l folosind glisorul:

     - **Ridicat**. Atunci când este selectat acest nivel de securitate pentru e-mail, componenta Mail Threat Protection scanează mesajele de e-mail cât mai complet. Componenta Mail Threat Protection scanează mesajele primite și trimise și efectuează o analiză euristică profundă. Nivelul Ridicat de securitate a e-mailurilor este recomandat pentru mediile cu risc ridicat. Un exemplu de astfel de mediu este o conexiune la un serviciu de e-mail gratuit de la o rețea de domiciliu neapărată de o protecție pentru e-mail centralizată.

     - **Recomandat**. Nivelul de securitate pentru e-mail care asigură echilibrul optim între performanțele aplicației și securitatea pentru e-mail. Componenta Mail Threat Protection scanează mesajele de e-mail primite și trimise și efectuează o analiză euristică de nivel mediu. Acest nivel de securitate pentru e-mail este recomandat de specialiștii de la Kaspersky. Valorile setărilor pentru nivelul de securitate recomandat sunt furnizate în tabelul de mai jos.

     - **Redus**. Atunci când este selectat acest nivel de securitate pentru e-mail, componenta Mail Threat Protection scanează numai mesajele de e-mail primite, efectuează o analiză euristică rapidă și nu scanează arhivele atașate la mesaje de e-mail. La acest nivel de securitate pentru e-mail, componenta Mail Threat Protection scanează mesajele de e-mail la viteză maximă și utilizează un minim de resurse ale sistemului de operare. Nivelul Redus de securitate pentru e-mail este recomandat pentru lucrul în medii bine protejate. Un exemplu de astfel de mediu poate fi o rețea LAN de întreprindere care deține securitate centralizată pentru e-mail.

   - Dacă dorești să configurezi un nivel de securitate personalizat, fă clic pe butonul **Setări avansate** și definește propriile setări pentru componentă.

     Puteți restabili valorile nivelurilor de securitate prestabilite făcând clic pe butonul **Restaurare nivel recomandat de securitate**.

5. În blocul **Acțiune la detectarea amenințării**, selectează acțiunea pe care aplicația Kaspersky Endpoint Security trebuie să o efectueze asupra obiectelor rău intenționate:

   - **Dezinfectează; șterge dacă dezinfectarea nu reușește**. Când un obiect infectat este detectat într-un mesaj de intrare sau de ieșire, aplicația încearcă să dezinfecteze obiectul detectat. Utilizatorul va putea accesa mesajul cu o atașare sigură. Dacă obiectul nu poate fi dezinfectat, aplicația șterge obiectul infectat. Aplicația adaugă informații despre acțiunea efectuată la subiectul mesajului: *[Mesajul a fost procesat] <subiect mesaj>*.

   - **Dezinfectează; blochează dacă dezinfectarea nu reușește**. Când un obiect infectat este detectat într-un mesaj de intrare, aplicația încearcă să dezinfecteze obiectul detectat. Utilizatorul va putea accesa mesajul cu o atașare sigură. Dacă obiectul nu poate fi dezinfectat, aplicația adaugă un avertisment subiectului mesajului. Utilizatorul va putea accesa mesajul cu atașarea originală. Când un obiect infectat este detectat într-un mesaj de ieșire, aplicația încearcă să dezinfecteze obiectul detectat. Dacă obiectul nu poate fi dezinfectat, aplicația blochează transmiterea mesajului, iar clientul de e-mail afișează o eroare.

   - **Blochează**. Dacă un obiect infectat este detectat într-un mesaj de intrare, aplicația adaugă un avertisment la subiectul mesajului. Utilizatorul va putea accesa mesajul cu atașarea originală. Dacă un obiect infectat este detectat într-un mesaj de ieșire, aplicația blochează transmiterea mesajului, iar clientul de e-mail afișează o eroare.

6. Salvați-vă modificările.

Setări Mail Threat Protection recomandate de experții Kaspersky (nivel de securitate recomandat)

Parametru	Valoare	Descriere
Domeniu de protecție	**Mesajele primite și trimise**	*Domeniul de protecție* include obiecte pe care componenta le verifică atunci când este executată: mesaje primite și trimise sau numai mesaje primite. Pentru a vă proteja calculatoarele, trebuie să scanați doar mesajele primite. Puteți activa scanarea mesajelor trimise pentru a preveni trimiterea fișierelor infectate în arhive. De asemenea, puteți activa scanarea mesajelor trimise dacă doriți să împiedicați trimiterea fișierelor în anumite formate, cum ar fi fișierele audio și video, de exemplu.
Conectează extensia Microsoft Outlook	**Pornit**	Dacă această casetă de selectare este bifată, scanarea mesajelor de e-mail transmise prin protocoalele POP3, SMTP, NNTP, IMAP este activată în extensia integrată în Microsoft Outlook. Dacă mesajele de e-mail sunt scanate folosind extensia pentru Microsoft Outlook, se recomandă folosirea modului Cached Exchange Mode. Pentru informații mai detaliate despre modul Cached Exchange și recomandări privind utilizarea sa, consultați Baza de cunoștințe Microsoft.
Scanează arhivele atașate	**Pornit**	Scanarea arhivelor ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE și a altor arhive. Aplicația scanează arhivele nu doar după extensie, dar și după format. La verificarea arhivelor, aplicația efectuează o dezarhivare recursivă. Acest lucru permite detectarea amenințărilor din arhivele cu mai multe niveluri (o arhivă într-o arhivă).
Scanează fișierele atașate în formate Microsoft Office	**Pornit**	Scanează fișierele Microsoft Office (DOC, DOCX, XLS, PPT și alte extensii Microsoft). Fișierele în format Office includ și obiecte OLE. Aplicația scanează fișierele în format office mai mici de 1 MO, indiferent dacă această casetă de selectare este bifată sau nu.
Filtrare atașări	**Redenumește atașările de tipurile selectate**	Dacă această opțiune este selectată, componenta Mail Threat Protection va înlocui ultimul caracter din extensie găsit în fișierele atașate din tipurile specificate cu caracterul de subliniere (de exemplu, attachment.doc_). Astfel, pentru a deschide fișierul, utilizatorul trebuie să redenumească fișierul.
Analiză euristică	**Scanare medie**	Tehnologia a fost dezvoltată pentru detectarea amenințărilor care nu se pot detecta utilizând versiunea curentă a bazelor de date ale aplicației Kaspersky. Aceasta detectează fișiere care este posibil să fie infectate cu un virus necunoscut sau cu o variație nouă a unui virus cunoscut. Când scanează fișierele pentru codul rău intenționat, analizatorul euristic execută instrucțiunile din fișierele executabile. Numărul de instrucțiuni executate de analizorul euristic depinde de nivelul specificat pentru analizorul euristic. Nivelul analizei euristice asigură un echilibru între gradul de detaliere a căutării de amenințări noi, gradul de solicitare a resurselor sistemului de operare și durata analizei euristice.
Acțiune la detectarea amenințării	**Dezinfectează; șterge dacă dezinfectarea nu reușește**	Când un obiect infectat este detectat într-un mesaj de intrare sau de ieșire, aplicația încearcă să dezinfecteze obiectul detectat. Utilizatorul va putea accesa mesajul cu o atașare sigură. Dacă obiectul nu poate fi dezinfectat, aplicația șterge obiectul infectat. Aplicația adaugă informații despre acțiunea efectuată la subiectul mesajului: *[Mesajul a fost procesat] <subiect mesaj>*.

Schimbarea acțiunii de efectuat asupra mesajelor de e-mail infectate

În mod implicit, componenta Mail Threat Protection încearcă automat să dezinfecteze toate mesajele de e-mail infectate detectate. Dacă dezinfectarea nu reușește, componenta Mail Threat Protection șterge aceste mesaje de e-mail.

Pentru a schimba acțiunea de efectuat asupra mesajelor de e-mail infectate:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Essential Threat Protection → Mail Threat Protection**.

3. În blocul **Acțiune la detectarea amenințării**, selectați acțiunea pe care aplicația Kaspersky Endpoint Security să o efectueze atunci când este detectat un mesaj infectat:

   - **Dezinfectează; șterge dacă dezinfectarea nu reușește**. Când un obiect infectat este detectat într-un mesaj de intrare sau de ieșire, aplicația încearcă să dezinfecteze obiectul detectat. Utilizatorul va putea accesa mesajul cu o atașare sigură. Dacă obiectul nu poate fi dezinfectat, aplicația șterge obiectul infectat. Aplicația adaugă informații despre acțiunea efectuată la subiectul mesajului: *[Mesajul a fost procesat] <subiect mesaj>*.

   - **Dezinfectează; blochează dacă dezinfectarea nu reușește**. Când un obiect infectat este detectat într-un mesaj de intrare, aplicația încearcă să dezinfecteze obiectul detectat. Utilizatorul va putea accesa mesajul cu o atașare sigură. Dacă obiectul nu poate fi dezinfectat, aplicația adaugă un avertisment subiectului mesajului. Utilizatorul va putea accesa mesajul cu atașarea originală. Când un obiect infectat este detectat într-un mesaj de ieșire, aplicația încearcă să dezinfecteze obiectul detectat. Dacă obiectul nu poate fi dezinfectat, aplicația blochează transmiterea mesajului, iar clientul de e-mail afișează o eroare.

   - **Blochează**. Dacă un obiect infectat este detectat într-un mesaj de intrare, aplicația adaugă un avertisment la subiectul mesajului. Utilizatorul va putea accesa mesajul cu atașarea originală. Dacă un obiect infectat este detectat într-un mesaj de ieșire, aplicația blochează transmiterea mesajului, iar clientul de e-mail afișează o eroare.

4. Salvați-vă modificările.

Specificarea domeniului de protecție al componentei Mail Threat Protection

Domeniul de protecție se referă la obiectele care sunt scanate de către componentă atunci când este activă. Proprietățile domeniilor de protecție diferă de la o componentă la alta. Proprietățile domeniului de protecție al componentei Mail Threat Protection includ setările de integrare a componentei Mail Threat Protection în clienții de e-mail și tipurile de mesaje de e-mail și de protocoale de e-mail al căror trafic este scanat de componenta Mail Threat Protection. În mod implicit, aplicația Kaspersky Endpoint Security scanează atât mesajele de e-mail primite, cât și pe cele trimise, precum și traficul efectuat prin protocoalele POP3, SMTP, NNTP și IMAP și este integrată în clientul de e-mail Microsoft Office Outlook.

Pentru a specifica domeniul de protecție al componentei Mail Threat Protection:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **Mail Threat Protection**.

3. Fă clic pe **Setări avansate**.

4. În blocul **Domeniu de protecție**, selectați mesajele de scanat:

   - **Mesajele primite și trimise**.

   - **Numai mesajele primite**.

   Pentru a vă proteja calculatoarele, trebuie să scanați doar mesajele primite. Puteți activa scanarea mesajelor trimise pentru a preveni trimiterea fișierelor infectate în arhive. De asemenea, puteți activa scanarea mesajelor trimise dacă doriți să împiedicați trimiterea fișierelor în anumite formate, cum ar fi fișierele audio și video, de exemplu.

Dacă alegi să scanezi numai mesajele primite, se recomandă să efectuezi o scanare pentru toate mesajele trimise, deoarece există posibilitatea ca pe computerul tău să existe viermi de e-mail care se răspândesc prin e-mail. Acest lucru contribuie la evitarea problemelor rezultate din trimiterea nemonitorizată de mesaje e-mail infectate de pe computerul tău.

5. În blocul **Conectivitate**, efectuează următoarele acțiuni:

   - Dacă doriți ca componenta Mail Threat Protection să scaneze mesajele transmise prin protocoalele POP3, SMTP, NNTP și IMAP înainte de a ajunge pe computerul utilizatorului, bifați caseta de selectare **Scanează traficul POP3, SMTP, NNTP și IMAP**.

     Dacă nu doriți ca componenta Mail Threat Protection să scaneze mesajele transmise prin protocoalele POP3, SMTP, NNTP și IMAP înainte de a ajunge pe computerul utilizatorului, debifați caseta de selectare **Scanează traficul POP3, SMTP, NNTP și IMAP**. În acest caz, mesajele sunt scanate de către extensia Mail Threat Protection încorporată în clientul de e-mail Microsoft Office Outlook după ce sunt primite pe computerul utilizatorului, dacă este bifată caseta de selectare **Conectează extensia Microsoft Outlook**.

     Dacă utilizați un alt client de e-mail decât Microsoft Office Outlook, componenta Mail Threat Protection nu scanează mesajele transmise prin protocoalele POP3, SMTP, NNTP și IMAP în cazul în care caseta de selectare **Scanează traficul POP3, SMTP, NNTP și IMAP** este debifată.

   - Dacă doriți să permiteți accesul la setările componentei Mail Threat Protection din Microsoft Office Outlook și să permiteți ca mesajele transmise prin protocoalele POP3, SMTP, NNTP, IMAP și MAPI să fie scanate după ce ajung pe computer folosind extensia încorporată în Microsoft Office Outlook, bifați caseta de selectare **Conectează extensia Microsoft Outlook**.

     Dacă doriți să blocați accesul la setările componentei Mail Threat Protection din Microsoft Office Outlook și să dezactivați scanarea mesajelor transmise prin protocoalele POP3, SMTP, NNTP, IMAP și MAPI după ce ajung pe computer folosind extensia încorporată în Microsoft Office Outlook, debifați caseta de selectare **Conectează extensia Microsoft Outlook**.

     Extensia Mail Threat Protection este încorporată în clientul de e-mail Microsoft Office Outlook în cursul instalării aplicației Kaspersky Endpoint Security.

6. Salvați-vă modificările.

Scanarea fișierelor compuse atașate la mesaje de e-mail

Poți activa sau dezactiva scanarea atașărilor la mesaje de e-mail, poți limita dimensiunea maximă a atașărilor la mesaje de scanat și poți limita durata maximă de scanare a unei atașări la un mesaj.

Pentru a configura scanarea fișierelor compuse care sunt atașate la mesajele de e-mail:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **Mail Threat Protection**.

3. Fă clic pe **Setări avansate**.

4. În blocul **Scanarea fișierelor compuse**, configurați setările de scanare:

   - **Scanează fișierele atașate în formate Microsoft Office**. Scanează fișierele Microsoft Office (DOC, DOCX, XLS, PPT și alte extensii Microsoft). Fișierele în format Office includ și obiecte OLE. Aplicația scanează fișierele în format office mai mici de 1 MO, indiferent dacă această casetă de selectare este bifată sau nu.

   - **Scanează arhivele atașate**. Scanarea arhivelor ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE și a altor arhive. Aplicația scanează arhivele nu doar după extensie, dar și după format. La verificarea arhivelor, aplicația efectuează o dezarhivare recursivă. Acest lucru permite detectarea amenințărilor din arhivele cu mai multe niveluri (o arhivă într-o arhivă).

     Dacă în timpul scanării, aplicația detectează o parolă pentru o arhivă în textul mesajului, această parolă va fi folosită pentru a scana conținutul arhivei în căutarea unor aplicații rău intenționate. În acest caz, parola nu este salvată. O arhivă este dezarhivată în timpul scanării. Dacă apare o eroare a aplicației în timpul procesului de dezarhivare, puteți șterge manual fișierele dezarhivate care sunt salvate pe următoarea cale: %systemroot%\temp. Fișierele au prefixul PR.

   - **Nu scana arhivele mai mari de N MO (între 1 și 9999)**. Dacă această casetă de selectare este bifată, componenta Mail Threat Protection exclude de la scanare arhivele atașate la mesaje de e-mail, dacă dimensiunea acestora depășește valoarea specificată. Dacă această casetă este debifată, componenta Mail Threat Protection scanează arhivele atașate la mesaje de e-mail indiferent de dimensiunea lor.

   - **Limitează timpul pentru verificarea arhivelor la N sec (între 1 și 9999)**. Atunci când caseta de selectare este bifată, intervalul de timp alocat pentru scanarea arhivelor atașate la mesaje de e-mail este limitat la perioada specificată.

5. Salvați-vă modificările.

Filtrarea atașărilor mesajelor de e-mail

Filtrarea atașărilor nu se aplică mesajelor de e-mail expediate.

Aplicațiile rău intenționate pot fi distribuite sub forma unor atașări în mesaje de e-mail. Poți configura filtrarea pe baza tipului de atașări la mesaje, astfel încât fișierele de tipul specificat să fie redenumite sau șterse în mod automat. Redenumind o atașare de un anumit tip, Kaspersky Endpoint Security îți poate proteja computerul împotriva executării automate a unei aplicații rău intenționate.

Pentru a configura filtrarea atașărilor:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **Mail Threat Protection**.

3. Fă clic pe **Setări avansate**.

4. În blocul **Filtrare atașări**, efectuează una dintre următoarele acțiuni:

   - **Dezactivează filtrarea**. Dacă este selectată această opțiune, componenta Mail Threat Protection nu filtrează fișierele atașate la mesaje de e-mail.

   - **Redenumește atașările de tipurile selectate**. Dacă această opțiune este selectată, componenta Mail Threat Protection va înlocui ultimul caracter din extensie găsit în fișierele atașate din tipurile specificate cu caracterul de subliniere (de exemplu, attachment.doc_). Astfel, pentru a deschide fișierul, utilizatorul trebuie să redenumească fișierul.

   - **Șterge atașările de tipurile selectate**. Dacă este selectată această opțiune, componenta Mail Threat Protection șterge fișierele atașate de tipurile specificate din mesajele de e-mail.

5. Dacă ai selectat opțiunea **Redenumește atașările de tipurile selectate** sau opțiunea **Șterge atașările de tipurile selectate** în cursul etapei anterioare, bifați casetele de selectare de lângă tipurile de fișiere relevante.

6. Salvați-vă modificările.

Exportul și importul extensiilor pentru filtrarea atașamentelor

Puteți exporta lista de extensii pentru filtrarea atașamentelor într-un fișier XML. Puteți utiliza funcția de export/import pentru a face o copie de rezervă a listei de extensii sau pentru a migra lista pe un alt server.

Cum se exportă și se importă o listă de extensii pentru filtrarea atașamentelor în Consola de administrare (MMC)

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **Communication & Web Protection** → **Mail Threat Protection**.

5. Pentru a exporta lista extensiilor din blocul **Attachment filter**:

   a. Selectați extensiile pe care doriți să le exportați.

   b. Faceți clic pe linkul **Export**.

   c. În fereastra care se deschide, specificați numele fișierului XML în care doriți să exporți lista de extensii și selectați directorul în care doriți să salvați acest fișier.

   d. Salvați fișierul.

   Kaspersky Endpoint Security exportă întreaga listă de extensii în fișierul XML.

6. Pentru a importa lista de extensii în blocul **Attachment filter**:

   a. Faceți clic pe linkul **Import**.

   b. În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de extensii.

c. Deschideți fișierul.

În cazul în care computerul are deja o listă de extensii, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul XML.

7. Salvați-vă modificările.

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Essential Threat Protection** → **Mail Threat Protection**.
4. În blocul **Nivel de securitate**, fă clic pe butonul **Setări**.
5. Se deschide o fereastră; în acea fereastră, selectați fila **Filtrare atașare**.
6. Pentru a exporta lista de extensii:
   a. Selectați extensiile pe care doriți să le exportați. Pentru a selecta mai multe porturi, utilizați tastele **CTRL** sau **SHIFT**.
   b. Faceți clic pe linkul **Exportă**.
   c. În fereastra care se deschide, specificați numele fișierului XML în care doriți să exporți lista de extensii și selectați directorul în care doriți să salvați acest fișier.
   d. Salvați fișierul.

      Kaspersky Endpoint Security exportă întreaga listă de extensii în fișierul XML.
7. Pentru a importa lista de extensii:
   a. Faceți clic pe linkul **Importă**.
   b. În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de extensii.
   c. Deschideți fișierul.

      În cazul în care computerul are deja o listă de extensii, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul XML.
8. Salvați-vă modificările.

Scanarea e-mailurilor în Microsoft Office Outlook

În cursul instalării Kaspersky Endpoint Security, extensia Mail Threat Protection este încorporată în Microsoft Office Outlook (denumit în continuare Outlook). Extensia permite scanarea mesajelor la nivelul unui client de e-mail și nu la nivelul protocolului. Pe lângă mesaje, extensia vă permite să scanați obiectele primite prin interfața MAPI din depozitele Microsoft Exchange (de exemplu, obiecte din Calendar). Această scanare are loc în clientul de e-mail.

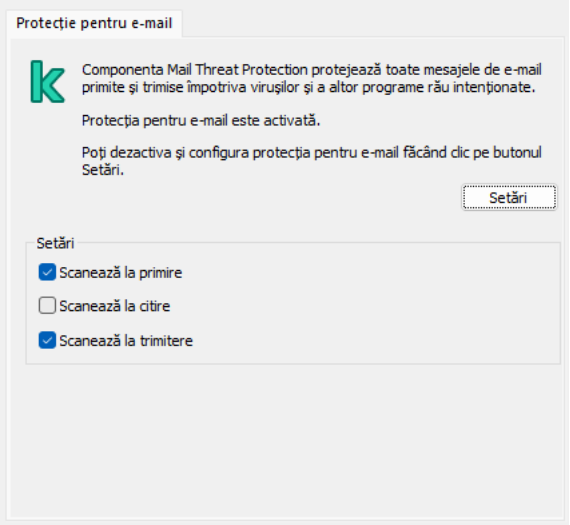
Puteți deschide setărilor componentei Mail Threat Protection din Outlook și puteți specifica momentului în care mesajele de e-mail trebuie scanate de viruși și alte amenințări.

Extensia Mail Threat Protection acceptă versiunile pe 32 de biți și pe 64 de biți ale Outlook 2010, 2013, 2016, 2019, 2021, 2024 și 365.

Pe computerele bazate pe arhitectura Arm, extensia Mail Threat Protection acceptă versiunile pe 32 de biți și 64 de biți ale Outlook 2016, Outlook 2021, Outlook 2024 și Outlook 365 pentru Arm64.

În Outlook, mesajele primite sunt întâi scanate de componenta Mail Threat Protection (dacă este bifată caseta de selectare Scanare trafic POP3, SMTP, NNTP și IMAP în interfața Kaspersky Endpoint Security) și apoi de extensia Mail Threat Protection pentru Outlook. Dacă componenta Mail Threat Protection detectează un obiect periculos într-un mesaj de e-mail, te notifică despre acest eveniment.

Setările componentei Mail Threat Protection pot fi configurate direct în Outlook dacă extensia Microsoft Outlook este conectată în interfața Kaspersky Endpoint Security (consultați figura de mai jos).



Setările componentei Mail Threat Protection în Outlook

Mesajele trimise sunt scanate mai întâi de extensia Mail Threat Protection pentru Outlook și apoi de componenta Mail Threat Protection.

Dacă mesajele de e-mail sunt scanate folosind extensia Mail Threat Protection pentru Outlook, se recomandă folosirea modului Exchange în cache. Pentru informații mai detaliate despre modul Cached Exchange și recomandări privind utilizarea sa, consultați Baza de cunoștințe Microsoft.

Pentru a configura modul de funcționare al extensiei Mail Threat Protection pentru Outlook:

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Essential Threat Protection** → **Mail Threat Protection**.
4. În blocul **Nivel de securitate**, fă clic pe butonul **Setări**.
5. În fereastra care se deschide, în blocull **Conectivitate**, fă clic pe butonul **Setări**.

6. În fereastra **Protecție pentru e-mail**, efectuați una dintre următoarele acțiuni:

   - Bifați caseta de selectare **Scanează la primire** dacă dorești ca extensia Mail Threat Protection pentru Outlook să scaneze mesajele primite atunci când acestea ajung în mailbox.
   - Bifați caseta de selectare **Scanează la citire** dacă dorești ca extensia Mail Threat Protection pentru Outlook să scaneze mesajele primite atunci când utilizatorul le deschide.
   - Bifați caseta de selectare **Scanează la trimitere** dacă dorești ca extensia Mail Threat Protection pentru Outlook să scaneze mesajele trimise atunci când acestea sunt expediate.

7. Salvați-vă modificările.

Scanarea e-mailurilor în Thunderbird, MyOffice, R7-Office

Componenta Mail Threat Protection scanează atașările mesajelor de e-mail primite și trimise în vederea detectării virușilor și a altor amenințări. Pentru clienții de e-mail Mozilla Thunderbird, MyOffice Mail și R7-Office Organizer, aplicația obține acces la mesaje doar la *nivel de protocol* (POP3, SMTP, IMAP, NNTP).

Pentru a scana traficul în clienții de e-mail Mozilla Thunderbird, MyOffice Mail și R7-Office Organizer, trebuie să adaugi un certificat Kaspersky la magazinul de certificate și să selectezi propriul magazin de certificate.

Componenta Mail Threat Protection nu scanează mesajele dacă clientul de e-mail este deschis într-un browser.

Mail Threat Protection în timp real

Mail Threat Protection poate scana atât mesajele primite, cât și cele trimise. În mod implicit, componenta Mail Threat Protection încearcă automat să dezinfecteze toate mesajele de e-mail infectate detectate. Dacă dezinfectarea nu reușește, componenta Mail Threat Protection șterge aceste mesaje de e-mail. Când un fișier rău intenționat este detectat într-un atașament, Kaspersky Endpoint Security adaugă informații despre acțiunea efectuată la subiectul mesajului, de exemplu, *[Mesajul a fost procesat]<subiect mesaj>*.

Dacă lucrezi cu clientul de e-mail Mozilla Thunderbird, componenta Mail Threat Protection nu scanează de viruși și alte amenințări mesajele transmise prin protocolul IMAP dacă sunt utilizate filtre pentru mutarea mesajelor din directorul Inbox.

Scanare malware în bazele de date de e-mail

Activitatea *Scanare malware* permite scanarea fișierelor în format de e-mail. Dacă se detectează un obiect rău intenționat în fișierele acestor clienți de e-mail, Kaspersky Endpoint Security doar adaugă informații despre obiectele detectate la lista de amenințări active. Aplicația nu dezinfectează și nu șterge fișierele infectate din bazele de date de e-mail, indiferent de setările activității.

Eliminarea amenințărilor active

Mail Threat Protection previne infectarea computerului la nivel de protocol, dar dacă computerul a fost infectat înainte de instalarea componentei Kaspersky Endpoint Security, aplicația poate doar să detecteze amenințarea în bazele de date de e-mail. Mail Threat Protection nu include componente care permit în mod specific dezasamblarea unui mesaj în părți (antet, corp, atașamente), ca în cazul Microsoft Office Outlook. Prin urmare, aplicația nu poate șterge sau dezinfecta obiectele detectate. Kaspersky Endpoint Security doar adaugă informații despre obiectele detectate la lista amenințărilor active.

Pentru a elimina amenințările active:

1. Găsește și șterge manual mesajul în care a fost obiectul în interfața clientului de e-mail.

   Aplicația afișează informații despre obiectele detectate în lista amenințărilor active.

   Exemplu de card pentru obiect detectat:

   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. Efectuează operațiunea de compactare a bazei de date.

   Când un mesaj este șters din interfața cu utilizatorul, clientul de e-mail doar adaugă un marcaj de ștergere. Clientul de e-mail șterge cu adevarat mesajul doar după o compactare a bazei de date. Pentru detalii despre compactarea bazei de date, consultă secțiunea de ajutor a clientului de e-mail (de exemplu, Mozilla Thunderbird).

3. Execută activitatea *Scanare malware* din nou și asigură-te că amenințarea nu mai există.

Network Threat Protection

Componenta *Network Threat Protection* (numită și Intrusion Detection System, IDS) monitorizează traficul de rețea de intrare pentru activitatea caracteristică atacurilor de rețea. Când aplicația detectează o încercare de atac asupra rețelei pe computerul unui utilizator, aceasta blochează conexiunea la rețea cu respectivul computer atacator. Descrierile tipurilor de atacuri de rețea cunoscute în prezent și ale modurilor de combatere a acestora sunt furnizate în bazele de date ale aplicației. Lista de atacuri de rețea pe care le detectează componenta Network Threat Protection este actualizată în cursul actualizărilor bazelor de date și modulelor aplicației.

Activarea și dezactivarea componentei Network Threat Protection

În mod implicit, componenta Network Threat Protection este și se execută în modul optim. Kaspersky Endpoint Security monitorizează traficul de rețea de intrare pentru activitatea caracteristică atacurilor de rețea și blochează atacurile.

Cum se activează sau dezactivează componenta Network Threat Protection în Consola de administrare (MMC)

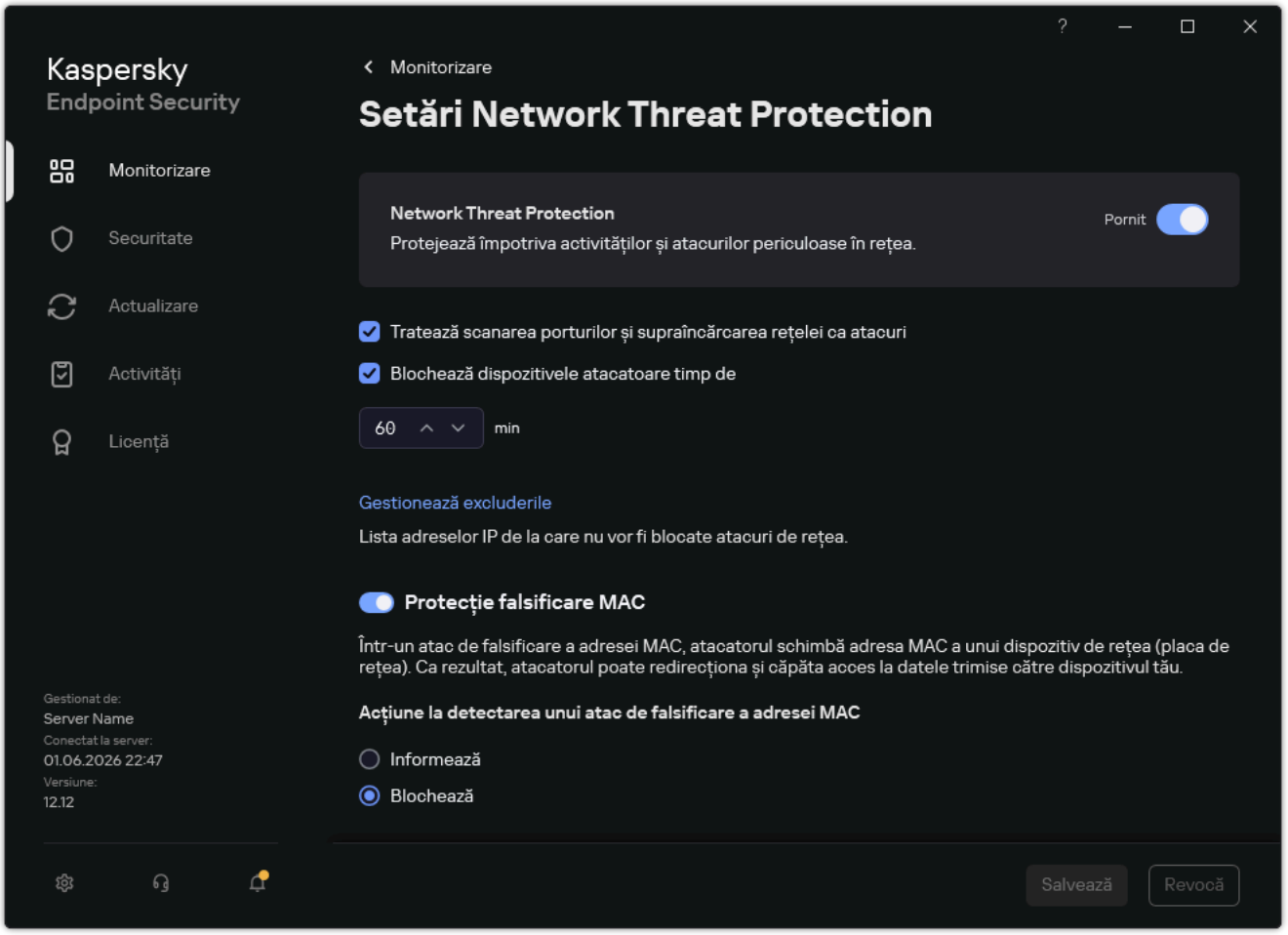
1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Essential Threat Protection → Network Threat Protection**.
4. Utilizează caseta de selectare **Network Threat Protection** pentru a activa sau a dezactiva componenta.
5. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se activează sau dezactivează componenta Network Threat Protection în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management → Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.
   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Communication & Web Protection → Network Threat Protection**.
5. Utilizați comutatorul **Network Threat Protection ENABLED** pentru a activa sau a dezactiva componenta.
6. Salvați-vă modificările.

Cum se activează sau dezactivează componenta Network Threat Protection în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Essential Threat Protection → Network Threat Protection**.



Setări Network Threat Protection

3. Utilizați comutatorul **Network Threat Protection** pentru a activa sau a dezactiva componenta.
4. Salvați-vă modificările.

Blocarea unui computer atacator

În cazul în care componenta Network Threat Protection este activată, Kaspersky Endpoint Security blochează automat amenințările din rețea. În plus, aplicația poate bloca computerul atacator și poate restricționa trimiterea pachetelor de rețea pentru o anumită perioadă de timp. În mod implicit, Kaspersky Endpoint Security blochează computerul timp de o oră.

Cum se blochează un computer atacator în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Essential Threat Protection → Network Threat Protection**.

4. În **Setări Network Threat Protection**, bifează caseta de selectare **Blochează dispozitivele atacatoare timp de N min**.

   Dacă această opțiune este activată, componenta Network Threat Protection adaugă computerul atacator la lista de computere blocate. Aceasta înseamnă că componenta Network Threat Protection blochează conectarea rețelei cu un computer agresor după prima încercare de atac asupra rețelei, pentru perioada de timp specificată. Acest lucru protejează automat computerul utilizatorului împotriva posibilelor viitoare atacuri de rețea inițiate de la aceeași adresă. Durata minimă pe care un computer atacator trebuie să o petreacă în lista blocului este de un minut. Durata maximă este de 999 de minute.

5. Setați o durată de blocare diferită pentru un computer atacator în câmpul din partea dreaptă a casetei de selectare **Blochează dispozitivele atacatoare timp de N min**.

6. Salvați-vă modificările.

Cum se blochează un computer atacator în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management → Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **Communication & Web Protection → Network Threat Protection**.

5. În blocul **Action on threat detection**, bifați caseta de selectare **Block attack and attacking device for (min)**.

   Dacă această opțiune este activată, componenta Network Threat Protection adaugă computerul atacator la lista de computere blocate. Aceasta înseamnă că componenta Network Threat Protection blochează conectarea rețelei cu un computer agresor după prima încercare de atac asupra rețelei, pentru perioada de timp specificată. Acest lucru protejează automat computerul utilizatorului împotriva posibilelor viitoare atacuri de rețea inițiate de la aceeași adresă. Durata minimă pe care un computer atacator trebuie să o petreacă în lista blocului este de un minut. Durata maximă este de 999 de minute.

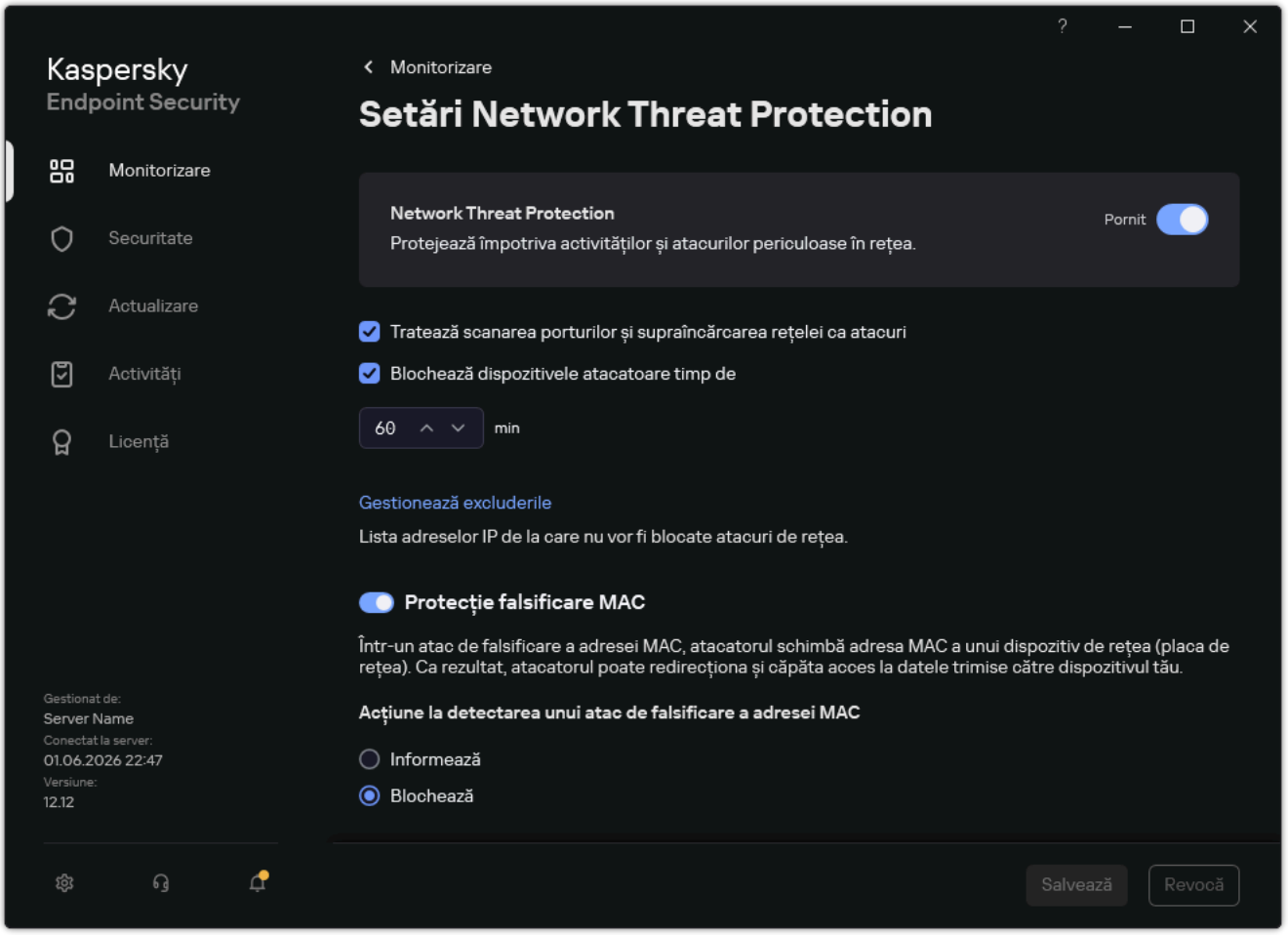
6. Schimbă durata de blocare a computerului atacator.

7. Salvați-vă modificările.

Cum se blochează un computer atacator în interfața cu utilizatorul a aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Essential Threat Protection → Network Threat Protection**.



Setări Network Threat Protection

3. Activează comutatorul **Blochează dispozitivele atacatoare timp de N min**.

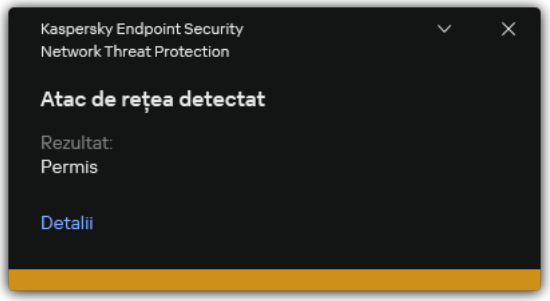
   Dacă această opțiune este activată, componenta Network Threat Protection adaugă computerul atacator la lista de computere blocate. Aceasta înseamnă că componenta Network Threat Protection blochează conectarea rețelei cu un computer agresor după prima încercare de atac asupra rețelei, pentru perioada de timp specificată. Acest lucru protejează automat computerul utilizatorului împotriva posibilelor viitoare atacuri de rețea inițiate de la aceeași adresă. Durata minimă pe care un computer atacator trebuie să o petreacă în lista blocului este de un minut. Durata maximă este de 999 de minute.

4. Setați o durată de blocare diferită pentru un computer atacator în câmpul de sub comutatorul **Blochează dispozitivele atacatoare timp de N min**.

5. Salvați-vă modificările.

Prin urmare, atunci când Kaspersky Endpoint Security detectează o încercare de atac asupra rețelei lansat împotriva computerului utilizatorului, aceasta va bloca toate conexiunile cu computerul atacator. Kaspersky Endpoint Security creează evenimentul *Network attack detected*. Evenimentul conține informații despre computerul atacator: Adresele IP și MAC.

Poți vizualiza adresa MAC a computerului atacator numai în interfața de utilizator a aplicației sau în consola Kaspersky Security Center versiunea 15.1 sau o versiune ulterioară.



Notificare despre detectarea atacurilor de rețea

Kaspersky Endpoint Security deblochează computerul când expiră timpul specificat. Consola Kaspersky Security Center nu oferă alte instrumente pentru monitorizarea computerelor blocate cu excepția evenimentelor *Network attack detected* din raport. Puteți vizualiza doar o listă de computere blocate în interfața aplicației. Această funcționalitate este oferită de instrumentul *Monitorizare rețea*. De asemenea, puteți utiliza instrumentul Monitorizare rețea pentru a debloca un computer.

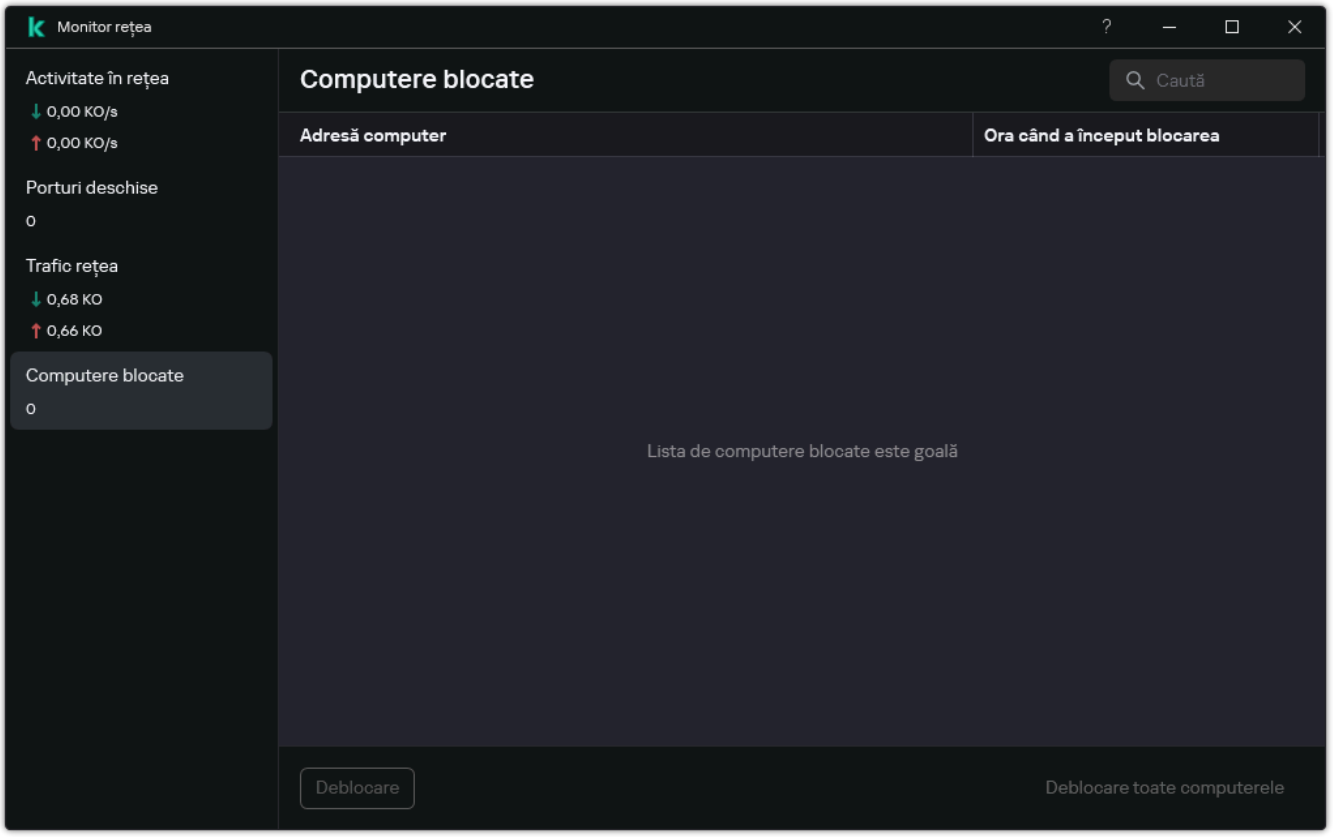
Pentru a debloca un computer:

1. În fereastra principală a aplicației, în secțiunea **Monitorizare**, faceți clic pe dala **Monitor rețea**.
2. Accesați fila **Computere blocate**.

   Aceasta deschide o listă de computere blocate (vezi figura de mai jos).

   Kaspersky Endpoint Security golește lista cu obiecte blocate atunci când aplicația este repornită și când setările componentei Network Threat Protection sunt modificate.

3. Selectați computerul pe care doriți să-l deblocați și faceți clic pe **Deblocare**.



Lista computerelor blocate

Configurarea adreselor de excluderi de la blocare

Kaspersky Endpoint Security poate recunoaște un atac de rețea și poate bloca o conexiune de rețea nesecurizată care transmite un număr mare de pachete (de exemplu, de la camerele de supraveghere). Pentru a lucra cu dispozitive de încredere, puteți adăuga adresele IP ale acestor dispozitive la lista de excluderi. De asemenea, puteți selecta protocolul și portul care sunt utilizate pentru comunicare și puteți permite activități de rețea specifice.

Capacitatea de a selecta protocoale și porturi pentru excluderi a fost adăugată în Kaspersky Endpoint Security 12.2. Asigurați-vă că aplicația și plug-in-ul de gestionare sunt actualizate la versiunea 12.2 sau o versiune ulterioară. Dacă utilizați o versiune anterioară a aplicației sau a plug-in-ului de gestionare, Kaspersky Endpoint Security poate permite activități de rețea numai după adresa IP.

Modificarea listei de excluderi blocate poate fi blocată de proprietățile politicii principale. Pentru a modifica lista, trebuie să permiteți modificarea setărilor zonei de încredere în Web Console („lacătul" trebuie să fie deblocat).

Zonele de încredere sunt grupate diferit în Consola de administrare (MMC) și în Web Console. De asemenea, modul în care se împiedică modificarea parametrilor zonei de încredere este diferit („lacăte" diferite). Vă recomandăm să utilizați exclusiv Web Console pentru gestionarea aplicației. În cazul în care configurați zona de încredere pe console diferite, este posibil ca plug-inul de gestionare să reseteze „lacătul" la starea implicită.

Cum se configurează adresele excluderilor de la blocare în Consola de administrare (MMC)

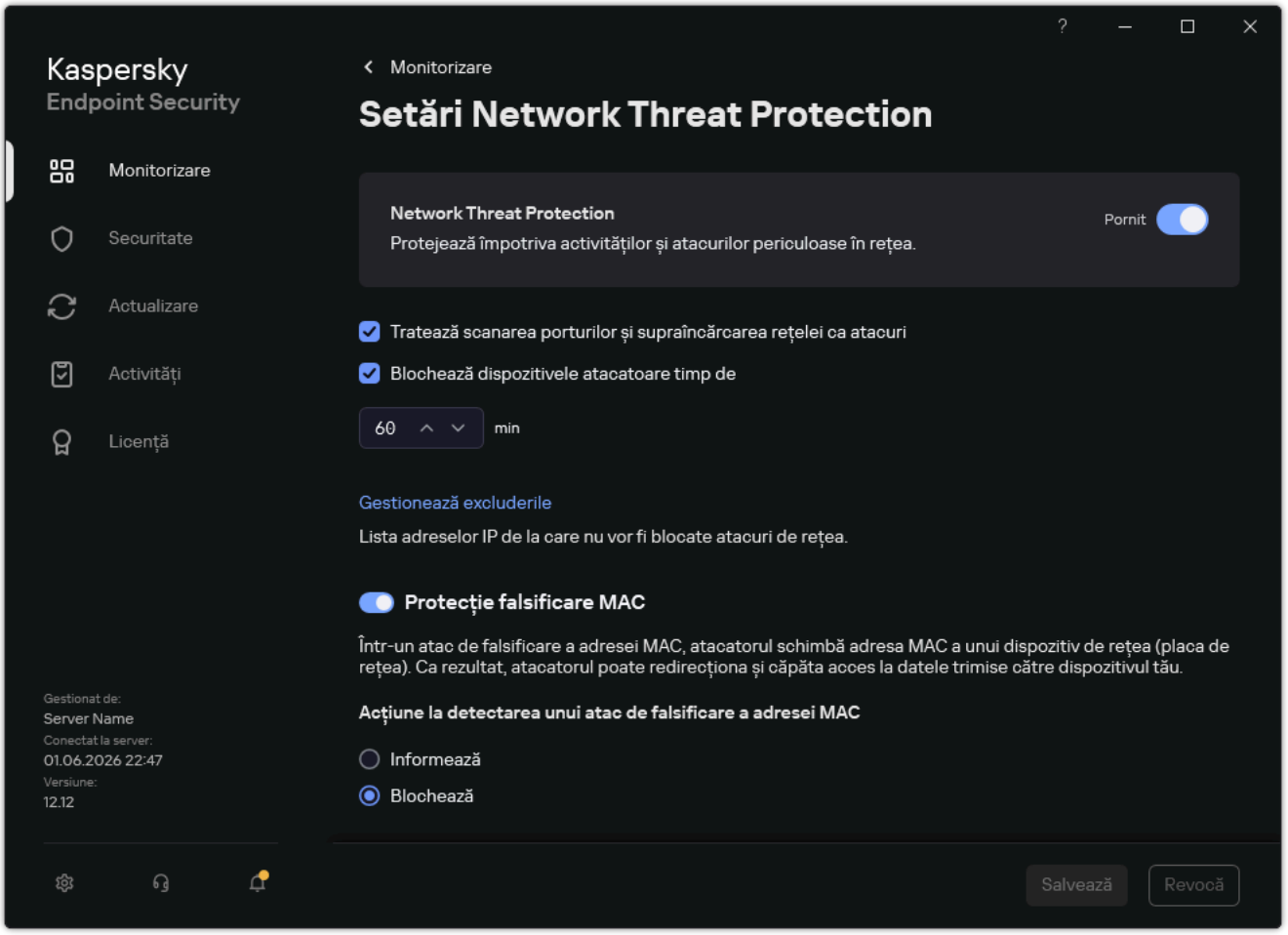
1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Essential Threat Protection** → **Network Threat Protection**.
4. În blocul **Setări Network Threat Protection**, fă clic pe butonul **Excluderi**.
5. În fereastra care se deschide, faceți clic pe butonul **Adaugă**.
6. Introdu adresa IP a computerului de la care nu trebuie blocate atacurile de rețea.
   Dacă este necesar, selectați protocolul și porturile prin care sunt transmise datele.
7. Salvați-vă modificările.

Cum se configurează adresele excluderilor de la blocare în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.
   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Communication & Web Protection** → **Network Threat Protection**.
5. În partea superioară a ferestrei, fă clic pe linkul **Trusted IP addresses**.
6. În fereastra care se deschide, faceți clic pe butonul **Add**.
7. Introdu adresa IP a computerului de la care nu trebuie blocate atacurile de rețea.
   Dacă este necesar, specifică subrețeaua.
8. Salvați-vă modificările.

Cum se configurează adresele excluderilor de la blocare în interfața cu utilizatorul a aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Essential Threat Protection → Network Threat Protection**.



Setări Network Threat Protection

3. Faceți clic pe linkul **Gestionează excluderile**.
4. În fereastra care se deschide, faceți clic pe butonul **Adaugă**.
5. Introdu adresa IP a computerului de la care nu trebuie blocate atacurile de rețea.

   Dacă este necesar, selectați protocolul și porturile prin care sunt transmise datele.
6. Salvați-vă modificările.

Exportul și importul listei de excluderi de la blocare

Poți exporta lista de excluderi într-un fișier XML. Apoi puteți modifica fișierul pentru a adăuga, de exemplu, un număr mare de adrese de același tip. De asemenea, puteți utiliza funcția de export/import pentru a face o copie de rezervă a listei de excluderi sau pentru a migra lista pe un alt server.

Cum se exportă și se importă o listă de excluderi în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

3. În fereastra politicii, selectați **Essential Threat Protection** → **Network Threat Protection**.

4. În blocul **Setări Network Threat Protection**, fă clic pe butonul **Excluderi**.

5. Pentru a exporta lista de reguli:

   a. Selectați excluderile pe care doriți să le exportați. Pentru a selecta mai multe porturi, utilizați tastele **CTRL** sau **SHIFT**.

   Dacă nu ați selectat nicio excludere, Kaspersky Endpoint Security va exporta toate excluderile.

   b. Fă clic pe butonul → **Exportă**.

   c. În fereastra care se deschide, specificați numele fișierului XML în care doriți să exporți lista de excluderi și selectați directorul în care doriți să salvați acest fișier.

   d. Salvați fișierul.

   Kaspersky Endpoint Security exportă întreaga listă de excluderi în fișierul XML.

6. Pentru a importa lista de excluderi:

   a. Fă clic pe butonul → **Importă**.

   b. În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de excluderi.

   c. Deschideți fișierul.

   În cazul în care computerul are deja o listă de excluderi, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul XML.

7. Salvați-vă modificările.

Cum se exportă și se importă o listă de excluderi în Consola Web și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **Communication & Web Protection** → **Network Threat Protection**.

5. În partea superioară a ferestrei, fă clic pe linkul **Trusted IP addresses**.

   Se deschide lista cu excluderi.

6. Pentru a exporta lista de reguli:

   a. Selectați excluderile pe care doriți să le exportați.

   b. Fă clic pe butonul → **Export**.

   Kaspersky Endpoint Security exportă lista de excluderi într-un fișier JSON în directorul pentru descărcări implicit.

7. Pentru a importa lista de excluderi:

   a. Fă clic pe butonul → **Import**.

      În fereastra care se deschide, selectați fișierul JSON din care doriți să importați lista de excluderi.

   b. Deschideți fișierul.

      În cazul în care computerul are deja o listă de excluderi, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul JSON.

8. Salvați-vă modificările.

Configurarea componentei Network Threat Protection în funcție de tip

Kaspersky Endpoint Security lvă permite să gestionați protecția împotriva următoarelor tipuri de atacuri de rețea:

- *Supraîncărcare rețea* este un atac asupra resurselor rețelei unei organizații (cum ar fi serverele web). Acest atac constă în trimiterea unui număr mare de soliciăr pentru a supraîncărca lățimea de bandă a resurselor rețelei. Când se întâmplă acest lucru, utilizatorii nu mai pot accesa resursele rețelei organizației.

- Un atac de tip *Scanare port* constă în scanarea porturilor UDP, TCP și a serviciilor de rețea de pe computer. Acest atac permite atacatorului să identifice gradul de vulnerabilitate al computerului înainte să efectueze tipuri mai periculoase de atacuri de rețea. De asemenea, atacul de tip Scanare port permite atacatorului să identifice sistemul de operare de pe computer și să selecteze atacurile de rețea corespunzătoare pentru acest sistem de operare.

- Un *atac de falsificare a adresei MAC* constă în schimbarea adresei MAC a unui dispozitiv de rețea (placă de rețea). Drept urmare, un atacator poate redirecționa datele trimise către un dispozitiv către un alt dispozitiv și poate avea acces la aceste date. Kaspersky Endpoint Security vă permite să blocați atacurile de falsificare a adresei MAC și să primiți notificări despre atacuri.

Puteți dezactiva detectarea acestor tipuri de atacuri în cazul în care unele dintre aplicațiile permise efectuează operații tipice pentru aceste tipuri de atacuri. Acest lucru va ajuta la evita alarmelor false.

În mod implicit, Kaspersky Endpoint Security nu monitorizează atacurile de tip Supraîncărcare rețea, Scanare port și Falsificare adresă MAC.

Nu îți recomandăm să activezi protecția împotriva falsificării MAC pe mașinile virtuale din infrastructura Microsoft Hyper-V. Datorită specificului platformei Microsoft Hyper-V, Kaspersky Industrial CyberSecurity for Nodes poate bloca hypervisorul din cauza rezultatelor fals pozitive.

Cum se configurează componenta Network Threat Protection în funcție de tip în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.

2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

3. În fereastra politicii, selectați **Essential Threat Protection** → **Network Threat Protection**.

4. Utilizați caseta de selectare **Tratează scanarea porturilor și supraîncărcarea rețelei ca atacuri** pentru a activa sau dezactiva detectarea acestor atacuri.

   Dacă această funcționalitate este activată, Kaspersky Endpoint Security monitorizează traficul de rețea pentru scanarea porturilor și inundarea rețelei. Dacă este detectat un astfel de comportament, aplicația notifică utilizatorul și trimite evenimentul corespunzător către Kaspersky Security Center. Aplicația furnizează informații despre computerul care face solicitările. Aceste informații sunt necesare pentru un răspuns în timp util. Cu toate acestea, Kaspersky Endpoint Security nu blochează computerul care face solicitările, deoarece un astfel de trafic poate fi un eveniment normal în rețeaua companiei.

5. În blocul **Modul Protecție împotriva falsificării adresei MAC**, selectați una dintre următoarele opțiuni:

   - **Nu se urmăresc încercările de falsificare a adresei MAC**.
   - **Informează**.
   - **Blochează**.

6. Salvați-vă modificările.

Cum se configurează componenta Network Threat Protection în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.
4. Accesați **Communication & Web Protection** → **Network Threat Protection**.
5. Utilizați caseta de selectare **Treat port scanning and network flooding as attacks** pentru a activa sau dezactiva detectarea acestor atacuri.

   Dacă această funcționalitate este activată, Kaspersky Endpoint Security monitorizează traficul de rețea pentru scanarea porturilor și inundarea rețelei. Dacă este detectat un astfel de comportament, aplicația notifică utilizatorul și trimite evenimentul corespunzător către Kaspersky Security Center. Aplicația furnizează informații despre computerul care face solicitările. Aceste informații sunt necesare pentru un răspuns în timp util. Cu toate acestea, Kaspersky Endpoint Security nu blochează computerul care face solicitările, deoarece un astfel de trafic poate fi un eveniment normal în rețeaua companiei.

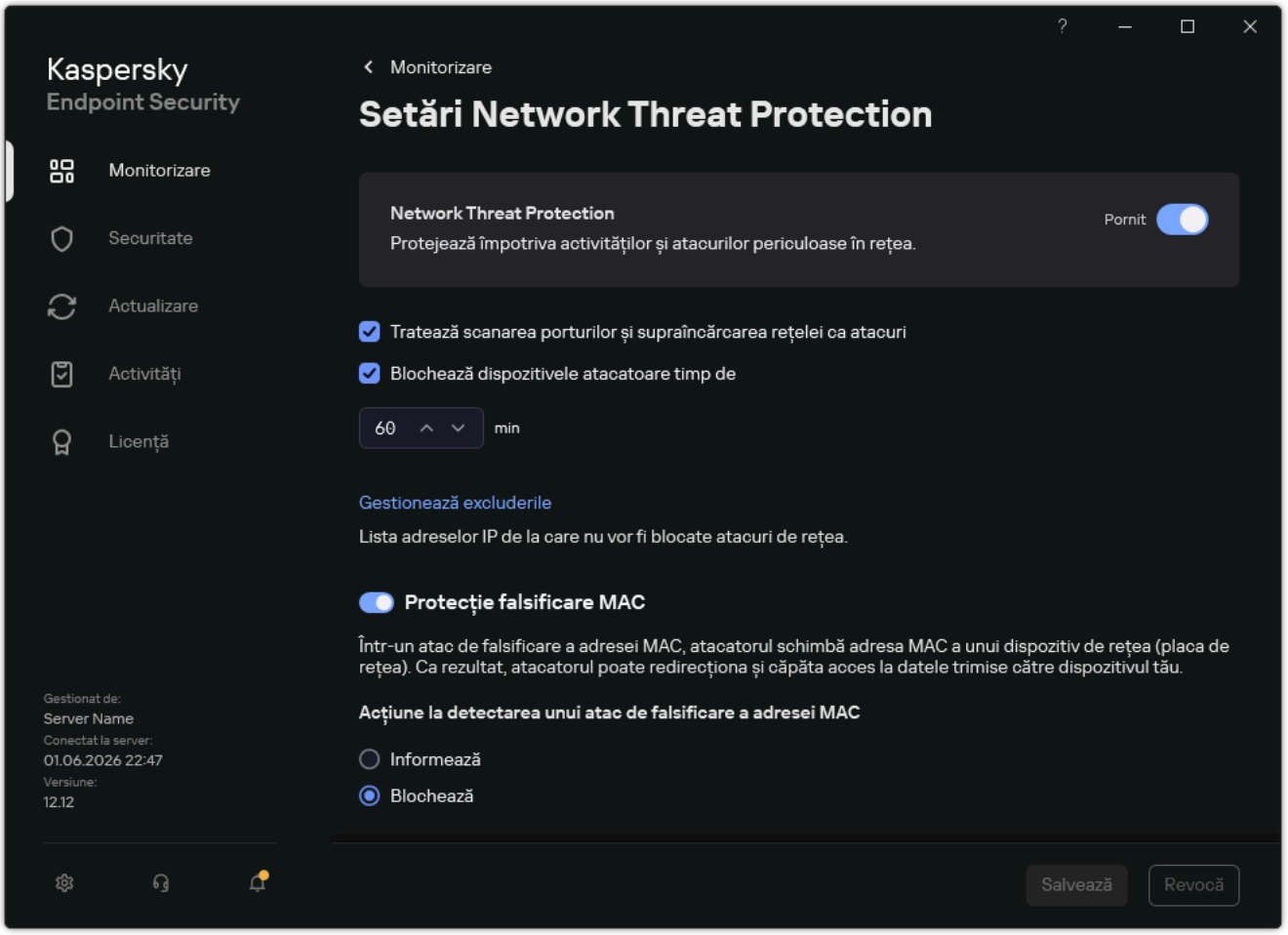
6. În blocul **MAC Spoofing Protection**, selectați una dintre următoarele opțiuni:

   - **MAC Spoofing Protection ENABLED**.
   - **Inform**.
   - **Block**.

7. Salvați-vă modificările.

Cum se configurează componenta Network Threat Protection în funcție de tip în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Essential Threat Protection → Network Threat Protection**.



Setări Network Threat Protection

3. Utilizați comutatorul **Tratează scanarea porturilor și supraîncărcarea rețelei ca atacuri** pentru a activa sau dezactiva detectarea acestor atacuri.

   Dacă această funcționalitate este activată, Kaspersky Endpoint Security monitorizează traficul de rețea pentru scanarea porturilor și inundarea rețelei. Dacă este detectat un astfel de comportament, aplicația notifică utilizatorul și trimite evenimentul corespunzător către Kaspersky Security Center. Aplicația furnizează informații despre computerul care face solicitările. Aceste informații sunt necesare pentru un răspuns în timp util. Cu toate acestea, Kaspersky Endpoint Security nu blochează computerul care face solicitările, deoarece un astfel de trafic poate fi un eveniment normal în rețeaua companiei.

4. Utilizați comutatorul **Protecție falsificare MAC** pentru a activa sau dezactiva detectarea acestor atacuri.
5. În blocul **Acțiune la detectarea unui atac de falsificare a adresei MAC**, selectați una dintre următoarele opțiuni:

   - **Informează**.
   - **Blochează**.

6. Salvați-vă modificările.

Firewall

Componenta Firewall blochează conexiunile neautorizate la un computer în timp ce lucrezi pe Internet sau într-o rețea locală. Firewall-ul controlează, de asemenea, activitatea de rețea a aplicațiilor de pe computer. Acest lucru vă permite să vă protejați rețeaua LANl corporativă împotriva furturilor de identitate și a altor atacuri. Componenta oferă protecție computerului cu ajutorul bazelor de date antivirus, a serviciului cloud Kaspersky Security Network și a *regulilor de rețea* predefinite.

Agentul de rețea este utilizat pentru interacțiunea cu Kaspersky Security Center. Firewall-ul creează automat regulile de rețea necesare pentru ca aplicația și Agentul de rețea să funcționeze. Ca urmare, componenta Firewall deschide mai multe porturi pe computer. Ce porturi sunt deschise depinde de rolul computerului (de exemplu, punct de distribuție). Pentru a afla mai multe despre porturile care vor fi deschise pe computer, consultă Ajutor Kaspersky Security Center.

Reguli rețea

Puteți configura regulile de rețea la următoarele niveluri:

- *Reguli pentru pachete de rețea*. Regulile pentru pachete de rețea impun restricții asupra pachetelor de rețea, indiferent de aplicație. Astfel de reguli restricționează traficul de rețea la intrare și la ieșire desfășurat prin anumite porturi ale protocolului de date selectat. Kaspersky Endpoint Security are reguli pentru pachetele de rețea predefinite cu permisiunile recomandate de experții Kaspersky.

- *Reguli de rețea pentru aplicații*. Regulile de rețea pentru aplicație impun restricții asupra activității de rețea a unei anumite aplicații. Ele iau în calcul nu numai caracteristicile pachetului de rețea, dar și aplicația căreia îi este adresat sau cea care a emis acest pachet de rețea.

Accesul controlat al aplicațiilor la resursele, procesele sistemului de operare și la datele cu caracter personal este oferit de componenta Host Intrusion Prevention prin utilizarea *drepturilor de aplicație*.

În timpul primei porniri a aplicației, Firewall-ul efectuează următoarele acțiuni:

1. Verifică securitatea aplicației folosind bazele de date antivirus descărcate.

2. Verifică securitatea aplicației în Kaspersky Security Network.

   Vă recomandăm să participați la Kaspersky Security Network pentru a ajuta componenta Firewall să funcționeze mai eficient.

3. Pune aplicația într-unul dintre grupurile de încredere: *De încredere*, *Restricționat la nivel inferior*, *Restricționat la nivel superior*, *Nu este de încredere*.

   Un grup de încredere definește drepturile la care se referă Kaspersky Endpoint Security atunci când controlează activitatea aplicațiilor. Kaspersky Endpoint Security plasează o aplicație într-un grup de încredere în funcție de nivelul de pericol pe care îl poate prezenta această aplicație pentru computer.

Kaspersky Endpoint Security plasează o aplicație într-un grup de încredere pentru componentele Firewall și Host Intrusion Prevention. Nu poți schimba grupul de încredere numai pentru componentele Firewall sau Host Intrusion Prevention.

Dacă ați refuzat să participați la KSN sau nu există o rețea, Kaspersky Endpoint Security plasează aplicația într-un grup de încredere, în funcție de setările componentei Host Intrusion Prevention. După primirea reputației aplicației de la KSN, grupul de încredere poate fi schimbat automat.

4. Blochează activitatea de rețea a aplicației în funcție de grupul de încredere. De exemplu, aplicațiile din grupul de încredere *Restricționat la nivel superior* nu au permisiunea să utilizeze conexiunile la rețea.

La următoarea pornire a aplicației, Kaspersky Endpoint Security verifică integritatea aplicației. Dacă aplicația este nemodificată, componenta folosește pentru aceasta regulile curente pentru rețea. Dacă aplicația a fost modificată, Kaspersky Endpoint Security analizează aplicația ca și cum ar fi fost pornită pentru prima dată.

Priorități ale regulilor de rețea

Fiecare regulă are o prioritate. Cu cât o regulă este mai sus în listă, cu atât prioritatea sa este mai mare. Dacă activitatea de rețea este adăugată la mai multe reguli, Firewall-ul reglementează activitatea de rețea în conformitate cu regula cu cea mai mare prioritate.

Regulile pentru pachete de rețea au o prioritate mai mare decât regulile de rețea pentru aplicații. Dacă pentru același tip de activitate de rețea sunt specificate atât reguli pentru pachete de rețea, cât și reguli de rețea pentru aplicații, activitatea de rețea este tratată conform regulilor pentru pachete de rețea.

Regulile de rețea pentru aplicații funcționează într-un anumit mod. Regula de rețea pentru aplicații include reguli de acces bazate pe starea rețelei: *Rețea publică*, *Rețea locală*, *Rețea de încredere*. De exemplu, aplicațiilor din grupul de încredere *Restricționat la nivel superior* nu le este permisă, mod implicit, nicio activitate de rețea în rețele cu toate stările. Dacă o regulă de rețea este specificată pentru o aplicație individuală (aplicație principală), atunci procesele secundare ale altor aplicații vor fi executate conform regulii de rețea a aplicației principale. Dacă nu există o regulă de rețea pentru aplicație, procesele secundare vor fi executate conform regulii de acces la rețea a grupului de încredere al aplicației.

De exemplu, ați interzis orice activitate de rețea în rețele cu toate stările pentru toate aplicațiile, cu excepția browserului X. Dacă începeți instalarea browserului Y (proces secundar) din browserul X (aplicația principală), atunci instalatorul browserului Y va accesa rețeaua și va descărca fișierele necesare. După instalare, browserului Y i se va refuza orice conexiuni la rețea conform setărilor Firewall. Pentru a interzice activitatea de rețea a instalatorului browserului Y ca proces secundar, trebuie să adăugați o regulă de rețea pentru instalatorul browserului Y.

Tipuri de conexiune la rețea

Firewall-ul îți permite să controlezi activitatea în rețea în funcție de tipul conexiunii la rețea. Kaspersky Endpoint Security primește tipul conexiunii la rețea de la sistemul de operare al computerului. Tipul conexiunii la rețea în sistemul de operare este setat de utilizator atunci când configurează conexiunea. Poți schimba tipul conexiunii la rețea în setările Kaspersky Endpoint Security. Firewall-ul va monitoriza activitatea rețelei în funcție de tipul rețelei specificat în setările Kaspersky Endpoint Security și nu în sistemul de operare.

Sunt disponibile următoarele tipuri de conexiune la rețea:

- **Rețea publică**. Rețeaua nu este protejată de aplicații antivirus, firewall-uri sau filtre (cum ar fi rețeaua Wi-Fi dintr-o cafenea). Când utilizatorul folosește un computer conectat la o astfel de rețea, Firewall blochează accesul la fișierele și imprimantele acestui computer. Utilizatorii externi nu pot accesa, de asemenea, date prin directoare partajate și acces la distanță la desktopul acestui computer. Firewall filtrează activitatea de rețea a fiecărei aplicații potrivit regulilor de rețea setate pentru ea.

  Firewall atribuie în mod implicit tipul *Rețea publică* Internetului. Nu poți modifica tipul pentru Internet.

- **Rețea locală**. Rețea pentru utilizatorii cu acces restricționat la fișierele și imprimantele de pe acest computer (cum ar fi pentru o rețea LAN sau o rețea de domiciliu).

- **Rețea de încredere**. Rețea securizată în care computerul nu este expus la atacuri sau încercări neautorizate de accesare a datelor. Firewall permite orice activitate de rețea în rețelele cu această stare.

Activarea sau dezactivarea Firewall

În mod implicit, Firewall este activat și funcționează într-un mod optim.

Cum se activează sau dezactivează componenta Firewall în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Essential Threat Protection → Firewall**.
4. Utilizează caseta de selectare **Firewall** pentru a activa sau a dezactiva componenta.
5. Salvați-vă modificările.

Cum se activează sau dezactivează componenta Firewall în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management → Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Selectați **Communication & Web Protection → Firewall**.
5. Utilizați comutatorul **Firewall ENABLED** pentru a activa sau a dezactiva componenta.
6. Salvați-vă modificările.

Cum se activează sau dezactivează componenta Firewall în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Essential Threat Protection → Firewall**.

3. Utilizați comutatorul **Firewall** pentru a activa sau a dezactiva componenta.

4. Salvați-vă modificările.

Drept urmare, dacă este activată componenta Firewall, Kaspersky Endpoint Security controlează activitatea de rețea și blochează conexiunile de rețea neautorizate la computerul dvs., precum și activitatea de rețea neautorizată a aplicațiilor de pe computerul dvs. Activitatea de rețea este, de asemenea, controlată de componenta Network Threat Protection. Componenta Network Threat Protection (numită și Intrusion Detection System, IDS) monitorizează traficul de rețea de intrare pentru activitatea caracteristică atacurilor de rețea.

Kaspersky Endpoint Security înregistrează evenimentele de atac de rețea în rapoartele sale, indiferent de setările Firewall-ului. Chiar dacă Firewall-ul blochează conexiunea la rețea folosind reguli și astfel previne un atac de rețea, componenta Network Threat Protection înregistrează evenimentele de atac de rețea. Este necesar pentru a genera informații statistice despre atacurile de rețea asupra computerelor din organizația dvs.

Modificarea tipului conexiunii la rețea

Firewall atribuie în mod implicit tipul *Rețea publică* Internetului. Nu poți modifica tipul pentru Internet.

Pentru a modifica tipul conexiunii la rețea:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **Firewall**.

3. Fă clic pe **Rețele disponibile**.

4. Selectează conexiunea la rețea a cărei tip dorești să îl modifici.

5. În coloana **Tip de rețea**, selectează tipul conexiunii la rețea:

   - **Rețea publică**. Rețeaua nu este protejată de aplicații antivirus, firewall-uri sau filtre (cum ar fi rețeaua Wi-Fi dintr-o cafenea). Când utilizatorul folosește un computer conectat la o astfel de rețea, Firewall blochează accesul la fișierele și imprimantele acestui computer. Utilizatorii externi nu pot accesa, de asemenea, date prin directoare partajate și acces la distanță la desktopul acestui computer. Firewall filtrează activitatea de rețea a fiecărei aplicații potrivit regulilor de rețea setate pentru ea.

   - **Rețea locală**. Rețea pentru utilizatorii cu acces restricționat la fișierele și imprimantele de pe acest computer (cum ar fi pentru o rețea LAN sau o rețea de domiciliu).

   - **Rețea de încredere**. Rețea securizată în care computerul nu este expus la atacuri sau încercări neautorizate de accesare a datelor. Firewall permite orice activitate de rețea în rețelele cu această stare.

6. Salvați-vă modificările.

Gestionarea regulilor pentru pachetele de rețea

Poți executa următoarele acțiuni atunci când gestionezi regulile pentru pachetele de rețea:

- Creează o regulă nouă pentru pachete de rețea.

  Poți crea o regulă nouă pentru pachete de rețea creând un set de condiții și de acțiuni care se aplică pachetelor de rețea și fluxurilor de date.

- Activează sau dezactivează o regulă pentru pachete de rețea.

  Toate regulile pentru pachete de rețea create de Firewall au în mod implicit starea *Activat*. Atunci când o regulă pentru pachete de rețea este activată, Firewall aplică această regulă.

  Poți dezactiva orice regulă pentru pachete de rețea selectată în lista de reguli pentru pachete de rețea. Atunci când o regulă pentru pachete de rețea este dezactivată, Firewall nu aplică temporar această regulă.

  > O regulă nouă particularizată pentru pachete de rețea este adăugată la lista de reguli pentru pachete de rețea cu starea *Activată* în mod implicit.

- Editează setările unei reguli pentru pachete de rețea existente.

  După ce creezi o regulă nouă pentru pachete de rețea, poți reveni oricând la editarea setărilor sale și le poți modifica după cum este nevoie.

- Modifică acțiunea Firewall pentru o regulă pentru pachete de rețea.

  În lista de reguli pentru pachete de rețea, poți edita acțiunea luată de Firewall la detectarea unei activități de rețea care corespunde unei anumite reguli pentru pachete de rețea.

- Modifică prioritatea unei reguli pentru pachete de rețea.

  Poți mări sau scădea prioritatea unei reguli pentru pachete de rețea care este selectată în listă.

- Elimină o regulă pentru pachete de rețea.

  Poți elimina o regulă pentru pachete de rețea pentru a opri aplicarea regulii respective de către Firewall la detectarea unei activități de rețea și pentru a opri afișarea acestei reguli în lista de reguli pentru pachete de rețea cu starea *Dezactivată*.

Crearea unei reguli pentru pachetul de rețea

Firewall-ul filtrează toată activitatea de rețea de pe computer în conformitate cu regulile pentru pachetele de rețea. Regulile pentru pachetele de rețea conțin condiții (de exemplu, direcția, protocolul) pe care Firewall-ul le aplică pentru a controla conexiunile de rețea ale computerului. Regulile pentru pachetele de rețea specifică, de asemenea, acțiunea pe care o efectuează Firewall-ul asupra conexiunii care corespunde regulii (permite sau blochează conexiunea).

Recomandări pentru crearea regulilor pentru pachete de rețea

Poți specifica o adresă IP sau o serie de adrese IP pentru a filtra activitatea în rețea. De asemenea, poți specifica un nume DNS, dar îți recomandăm să utilizezi adrese IP și intervale de adrese IP. Utilizarea numelor DNS în numele pachetelor de rețea poate fi nesigură, deoarece proprietarul serverului DNS poate modifica parametrii înregistrării DNS. O persoană rău intenționată poate, de asemenea, falsifica mesajele DNS și eluda regulile Firewall-ului.

Poți controla conexiunile de rețea prin nume DNS folosind regulile componentei Control Web. Dacă trebuie să specifici un nume DNS în regulile Firewall:

- Asigură securitatea rețelei LAN corporative.
- Asigură securitatea memoriei cache și a serverelor DNS autorizate.
- Activează protecția înregistrării DNS împotriva modificărilor.

La crearea de reguli pentru pachete de rețea, reține faptul că acestea au o prioritate mai mare decât regulile de rețea pentru aplicații.

Metode de creare a regulilor pentru pachetele de rețea

Puteți crea o regulă de rețea pentru pachetul de rețea în următoarele moduri:

- Utilizați instrumentul Monitor rețea.

  Monitorizare rețea este un instrument destinat vizualizării în timp real a informațiilor despre activitatea de rețea a computerului unui utilizator. Aceasta este o metodă convenabilă deoarece nu trebuie să configurați toate setările regulii. Unele setări ale componente Firewall vor fi introduse automat din datele Monitorului de rețea. Instrumentul Monitor rețea este disponibil în interfața aplicației.

- Configurați setările componentei Firewall.

  Aceasta ar trebui să vă permită să reglați fin setările Firewall-ului. Puteți crea reguli pentru orice activitate de rețea, chiar dacă nu există nicio activitate de rețea în prezent.

Cum se utilizează instrumentul Monitor rețea pentru a crea o regulă pentru pachetul de rețea în interfața aplicației

1. În fereastra principală a aplicației, în secțiunea **Monitorizare**, faceți clic pe dala **Monitor rețea**.
2. Accesați fila **Activitate în rețea**.

   Fila **Activitate în rețea** afișează toate conexiunile la rețea active în prezent pe computer. Se afișează atât conexiunile la rețea la ieșire, cât și cele la intrare.
3. În meniul contextual al conexiunii la rețea, selectați **Creare regulă pentru pachetul de rețea**.

   Aceasta deschide proprietățile regulii pentru rețea.
4. Setați starea **Activă** pentru regula de pachete.
5. Introdu manual numele serviciului de rețea în câmpul **Nume**.

6. Configurați setările regulii de rețea (consultați tabelul de mai jos).

   Puteți selecta un șablon de regulă predefinit făcând clic pe linkul **Șablon regulă de rețea**. Șabloanele de reguli descriu cele mai frecvent utilizate conexiuni de rețea.

   Toate setările regulilor de rețea vor fi completate automat.

7. Dacă dorești ca acțiunile regulii de rețea să fie reflectate în raport, bifați caseta de selectare **Înregistrează evenimentele în jurnal**.

8. Fă clic pe **Salvează**.

   Noua regulă de rețea va fi adăugată în listă.

9. Utilizați butoanele **Sus** / **Jos** pentru a seta prioritatea regulii de rețea.

10. Salvați-vă modificările.

Cum se utilizează setările componentei Firewall pentru a crea o regulă pentru pachetul de rețea în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **Firewall**.

3. Fă clic pe **Reguli de pachet**.

   Aceasta deschide o listă de reguli implicite setate de componenta Firewall.

4. Folosind lista verticală **Adaugă**, selectează locația regulii în listă: în partea de sus a listei, în partea de jos a listei sau lângă regula selectată.

   Poziția regulii în listă determină prioritatea regulii. Regula din partea de sus a listei are cea mai mare prioritate.

5. Setați starea **Activă** pentru regula de pachete.

6. Introdu manual numele serviciului de rețea în câmpul **Nume**.

7. Configurați setările regulii de rețea (consultați tabelul de mai jos).

   Puteți selecta un șablon de regulă predefinit făcând clic pe linkul **Șablon regulă de rețea**. Șabloanele de reguli descriu cele mai frecvent utilizate conexiuni de rețea.

   Toate setările regulilor de rețea vor fi completate automat.

8. Dacă dorești ca acțiunile regulii de rețea să fie reflectate în raport, bifați caseta de selectare **Înregistrează evenimentele în jurnal**.

9. Fă clic pe **Salvează**.

   Noua regulă de rețea va fi adăugată în listă.

10. Utilizați butoanele **Sus** / **Jos** pentru a seta prioritatea regulii de rețea.

11. Salvați-vă modificările.

Cum se creează o regulă pentru pachetul de rețea în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.

2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

3. În fereastra politicii, selectați **Essential Threat Protection** → **Firewall**.

4. În blocul **Setări Firewall**, fă clic pe butonul **Setări**.

   Aceasta deschide lista cu regulile pentru pachetele de rețea și lista regulilor de rețea pentru aplicații.

5. Accesați fila **Reguli pentru pachetele de rețea**.

   Aceasta deschide o listă de reguli implicite setate de componenta Firewall.

6. Folosind lista verticală **Adaugă**, selectează locația regulii în listă: în partea de sus a listei, în partea de jos a listei sau lângă regula selectată.

   Poziția regulii în listă determină prioritatea regulii. Regula din partea de sus a listei are cea mai mare prioritate.

7. Introdu manual numele serviciului de rețea în câmpul **Nume**.

8. Configurați setările regulii de rețea (consultați tabelul de mai jos).

   Puteți selecta un șablon de regulă predefinit făcând clic pe butonul . Șabloanele de reguli descriu cele mai frecvent utilizate conexiuni de rețea.

   Toate setările regulilor de rețea vor fi completate automat.

9. Dacă dorești ca acțiunile regulii de rețea să fie reflectate în raport, bifați caseta de selectare **Înregistrează evenimentele în jurnal**.

10. Salvează noua regulă de rețea.

11. Utilizați butoanele **Sus** / **Jos** pentru a seta prioritatea regulii de rețea.

12. Salvați-vă modificările.

Componenta Firewall va controla pachetele de rețea conform regulii. Puteți dezactiva o regulă pentru pachet din operațiunea componentei Firewall, fără să o ștergeți din listă. Pentru aceasta, debifați caseta de selectare de lângă obiect.

Cum se creează o regulă pentru pachete de rețea în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Selectați **Communication & Web Protection** → **Firewall**.

5. Selectați fila **Network packet rules**.

   Aceasta deschide o listă de reguli implicite setate de componenta Firewall.

6. Fă clic pe **Add**.

   Această acțiune deschide formularul pentru o nouă regulă de rețea.

7. Introdu manual numele serviciului de rețea în câmpul **Rule name**.

8. Configurați setările regulii de rețea (consultați tabelul de mai jos).

Puteți selecta un șablon de regulă predefinit făcând clic pe linkul **Select rule template**. Șabloanele de reguli descriu cele mai frecvent utilizate conexiuni de rețea.

Toate setările regulilor de rețea vor fi completate automat.

9. Dacă dorești ca acțiunile regulii de rețea să fie reflectate în raport, bifați caseta de selectare **Log events**.

10. Salvează regula de rețea.

    Noua regulă de rețea va fi adăugată în listă.

11. Utilizează butonul **Move** pentru a seta prioritatea regulii de rețea.

12. Salvați-vă modificările.

Componenta Firewall va controla pachetele de rețea conform regulii. Puteți dezactiva o regulă pentru pachet din operațiunea componentei Firewall, fără să o ștergeți din listă. Utilizați comutatorul din coloana **Status** pentru a activa sau a dezactiva regula pentru pachet.

Setări Reguli pentru pachetele de rețea

Parametru	Descriere
Acțiune	**Permite**. **Blochează**. **După regulile de aplicații**. Dacă este setată această opțiune, componenta Firewall aplică regulile de rețea pentru aplicații conexiunii la rețea.
Protocol	Controlați activitatea de rețea prin protocolul selectat: TCP, UDP, ICMP, ICMPv6, IGMP și GRE. Dacă selectați protocolul ICMP sau ICMPv6, puteți defini tipul și codul de pachet ICMP. Dacă este selectat tipul de protocol TCP sau UDP, poți specifica numerele de port pentru computerul local și computerul la distanță între care urmează să fie monitorizată conexiunea. Interval de valori posibile pentru numerele de port: 0-65535. În fiecare câmp, poți introduce mai multe valori separate prin `,` sau specifica un interval de valori folosind `-`. De exemplu: • `100,101` • `100-130` • `100,110-130`
Direcție	**Intrare (pachet)**. Componenta Firewall aplică regula de rețea tuturor pachetelor de rețea de intrare. **Intrare**. Componenta Firewall aplică regula de rețea tuturor pachetelor de rețea trimise printr-o conexiune care a fost inițiată de un computer la distanță. **Intrare/Ieșire**. Componenta Firewall aplică regula de rețea tuturor pachetelor de rețea de ieșire și de intrare. **Ieșire (pachet)**. Componenta Firewall aplică regula de rețea tuturor pachetelor de rețea de ieșire. **Ieșire**. Componenta Firewall aplică regula de rețea tuturor pachetelor de rețea trimise printr-o conexiune care a fost inițiată de computerul utilizatorului.
Plăci de rețea	Plăcile de rețea care pot trimite și/sau primi pachete de rețea. Specificarea setărilor pentru plăcile de rețea face posibilă diferențierea între pachete de rețea trimise sau primite de plăci de rețea cu adrese IP identice.
Timp de viață (TTL)	Limitarea controlului pachetelor de rețea în funcție de durata lor de viață (Time to Live, TTL).
Adrese la distanță	Adresele de rețea ale computerelor la distanță care pot trimite și/sau primi pachete de rețea. Componenta Firewall aplică o regulă de rețea pentru intervalul specificat de adrese de rețea la distanță. Puteți include toate adresele IP într-o regulă de rețea, puteți crea o listă separată de adrese IP, puteți specifica un interval de adrese IP sau puteți selecta o subrețea (Rețele de încredere, Rețele locale, Rețele publice). De asemenea, puteți specifica un nume DNS al unui computer în loc de adresa IP a acestuia. Trebuie să utilizați nume DNS numai pentru computerele LAN sau serviciile interne. Interacțiunea cu serviciile cloud (cum ar fi Microsoft Azure) și alte resurse de Internet trebuie gestionată de componenta Control web. Dacă în regula pentru pachetele de rețea ați adăugat un nume DNS pentru care adresa IP nu a putut fi determinată, Kaspersky Endpoint Security va afișa un avertisment. În lista de reguli pentru pachetele de rețea din Web Console este adăugată o coloană ce conține o descriere a erorii. În Consola de administrare (MMC), descrierea erorii nu este disponibilă. Astfel de reguli pentru pachete sunt evidențiate în culori.

Parametru	Descriere
Adrese locale	Adresele de rețea ale computerelor care pot trimite și/sau primi pachete de rețea. Componenta Firewall aplică o regulă de rețea pentru intervalul specificat de adrese de rețea locale. Puteți include toate adresele IP într-o regulă de rețea, puteți crea o listă separată de adrese IP sau puteți specifica un interval de adrese IP. Aplicația stochează adresele locale numai dacă este specificată o listă de adrese la distanță. Aceasta înseamnă că, valoarea **Adrese din listă** a fost selectată pentru **Adrese la distanță** și cel puțin o adresă a fost adăugată. Uneori adresele locale nu pot fi obținute pentru aplicații. Dacă aceasta este situația, acest parametru este ignorat.

Activarea sau dezactivarea unei reguli pentru pachete de rețea

Pentru a activa sau a dezactiva o regulă pentru pachete de rețea:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **Firewall**.
3. Fă clic pe **Reguli de pachet**.

   Aceasta deschide o listă de reguli implicite pentru pachete de rețea; aceste reguli sunt setate de componenta Firewall.
4. Selectați în listă regula pentru pachete de rețea necesară.
5. Utilizați comutatorul din coloana **Stare** pentru a activa sau a dezactiva regula.
6. Salvați-vă modificările.

Modificarea acțiunii Firewall pentru o regulă pentru pachete de rețea

Pentru a modifica acțiunea Firewallului aplicată unei reguli pentru pachete de rețea:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **Firewall**.
3. Fă clic pe **Reguli de pachet**.

   Aceasta deschide o listă de reguli implicite pentru pachete de rețea; aceste reguli sunt setate de componenta Firewall.
4. Selectați regula în lista de reguli pentru pachete de rețea și faceți clic pe butonul **Editează**.

5. În lista verticală **Acțiune**, selectați acțiunea de efectuat de componenta Firewall la detectarea acestui tip de activitate de rețea:

   - **Permite**.
   - **Blochează**.
   - **După regulile de aplicații**. Dacă este setată această opțiune, componenta Firewall aplică regulile de rețea pentru aplicații conexiunii la rețea.

6. Salvați-vă modificările.

Modificarea priorității unei reguli pentru pachete de rețea

Prioritatea unei reguli pentru pachete de rețea este stabilită de poziția regulii în lista de reguli pentru pachete de rețea. Prioritatea cea mai mare o are regula pentru pachete de rețea din partea superioară a listei de reguli pentru pachete de rețea.

Fiecare regulă pentru pachete de rețea creată manual este adăugată la sfârșitul listei de reguli pentru pachete de rețea și are prioritatea cea mai mică.

Componenta Firewall execută regulile în ordinea în care acestea apar în lista de reguli pentru pachete de rețea, de sus în jos. În funcție de fiecare regulă pentru pachete de rețea procesată care se aplică unei anumite conexiuni de rețea, componenta Firewall fie permite, fie blochează accesul la adresa și la portul specificate în setările conexiunii de rețea respective.

Pentru a schimba prioritatea regulii pentru pachete de rețea:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **Firewall**.
3. Fă clic pe **Reguli de pachet**.

   Aceasta deschide o listă de reguli implicite pentru pachete de rețea; aceste reguli sunt setate de componenta Firewall.

4. În listă, selectați regula pentru pachete de rețea a cărei prioritate dorești să o schimbi.
5. Utilizați butoanele **Sus** / **Jos** pentru a seta prioritatea regulii de rețea.
6. Salvați-vă modificările.

Exportul și importul regulilor de pachete de rețea

Puteți exporta lista de reguli de pachete de rețea într-un fișier XML. Apoi puteți modifica fișierul pentru a adăuga, de exemplu, un număr mare de reguli de același tip. Puteți utiliza funcția de export/import pentru a face o copie de rezervă a listei de reguli de pachete de rețea sau pentru a migra lista pe un alt server.

Cum se exportă și se importă o listă de reguli de pachete de rețea în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Essential Threat Protection** → **Firewall**.
4. În blocul **Setări Firewall**, fă clic pe butonul **Setări**.

   Aceasta deschide lista cu regulile pentru pachetele de rețea și lista regulilor de rețea pentru aplicații.
5. Accesați fila **Reguli pentru pachetele de rețea**.
6. Pentru a exporta lista de reguli de pachete de rețea:

   a. Selectați regulile pe care doriți să le exportați. Pentru a selecta mai multe porturi, utilizați tastele **CTRL** sau **SHIFT**.

   Dacă nu ați selectat nicio regulă, Kaspersky Endpoint Security va exporta toate regulile.

   b. Faceți clic pe linkul **Exportă**.

   c. În fereastra care se deschide, specificați numele fișierului XML în care doriți să exporți lista de reguli și selectați directorul în care doriți să salvați acest fișier.

   d. Salvați fișierul.

   Kaspersky Endpoint Security exportă lista de reguli în fișierul XML.
7. Pentru a importa o listă de reguli de pachete de rețea:

   a. Faceți clic pe linkul **Importă**.

   În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de reguli.

   b. Deschideți fișierul.

   În cazul în care computerul are deja o listă de reguli, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul XML.
8. Salvați-vă modificările.

Cum se exportă și se importă o listă de reguli de pachete de rețea în Consola Web și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Selectați **Communication & Web Protection** → **Firewall**.

5. Pentru a exporta lista de reguli, în blocul **Network packet rules**:

   a. Selectați regulile pe care doriți să le exportați.

   b. Fă clic pe butonul → **Export**.

      Kaspersky Endpoint Security exportă lista de reguli într-un fișier JSON în directorul de descărcări implicit.

6. Pentru a importa lista de reguli, în blocul **Network packet rules**:

   a. Fă clic pe butonul → **Import**.

      În fereastra care se deschide, selectați fișierul JSON din care doriți să importați lista de reguli.

   b. Deschideți fișierul.

      În cazul în care computerul are deja o listă de reguli, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul JSON.

7. Salvați-vă modificările.

Definirea regulilor pentru pachetele de rețea în XML

Componenta Firewall permite exportul regulilor pentru pachetele de rețea în format XML. Apoi puteți modifica fișierul pentru a adăuga, de exemplu, un număr mare de reguli de același tip.

Fișierul XML conține două noduri principale: `Rules` și `Resources`. Nodul `Rules` conține reguli pentru pachetele de rețea. Acest nod conține reguli configurate implicit (*reguli predefinite*), precum și reguli adăugate de utilizator (*reguli particularizate*).

Indicatorii regulii pentru pachetele de rețea

```
<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>
```

Setările regulii pentru pachetele de rețea în format XML

Parametru	Descriere	Valoare
`<key name="0000">`	Prioritatea regulii. Cu cât valoarea este mai mică, cu atât prioritatea este mai mare.	Număr întreg Valoarea priorității trebuie să conțină 4 cifre. Nodurile din fișierul XML trebuie ordonate după valoarea priorității, începând cu `0000`.
`RuleId`	ID-ul regulii.	**Reguli predefinite** `100` – **Solicitări către serverul DNS prin TCP**. `101` – **Solicitări către serverul DNS prin UDP**. `102` – **Trimitere mesaje de e-mail**. `110` – **Orice activitate în rețea** (Rețele de încredere). `125` – **Orice activitate în rețea** (Rețele locale). `130` – **Activitate în rețea Remote Desktop**. `131` – **Conexiuni TCP prin porturi locale**. `132` – **Conexiuni UDP prin porturi locale**. `133` – **Flux TCP de intrare**. `134` – **Flux UDP de intrare**. `137` – **Răspunsuri de intrare ICMP Destination Unreachable**. `138` – **Pachete de intrare ICMP Echo Reply**. `140` – **Răspunsuri de intrare ICMP Time Exceeded**. `142` – **Flux ICMP de intrare**. `266` – **Pachete de intrare ICMPv6 Echo Request**.
`RuleState`	Starea regulii.	`0` – regula predefinită este dezactivată `1` – regula predefinită este activată `2` – regula personalizată este dezactivată `3` – regula personalizată este activată
`RuleTypeId`	ID-ul tipului regulii.	`4` – regula pentru pachete de rețea.
`AppIdEx`	ID-ul aplicației căreia îi aparține regula pentru pachete de rețea.	Dacă regula nu aparține niciunei aplicații, valoarea este `0`.
`ResIdEx`	ID-ul principal al resursei cu setările regulii. Poți folosi acest identificator pentru a localiza un bloc cu setările regulii în nodul `Resources`.	Număr întreg
`ResIdEx2`	ID-ul tipului rețelei.	`0` – **Orice adresă**. `50` – **Rețele de încredere**. `51` – **Rețele locale**. `52` – **Rețele publice**. `<Network Identifier>` – **Adrese din listă** (adresele sunt definite manual).
`AccessFlag`	Valoarea parametrului **Acțiune**.	`0` – **Permite**. `2` – **După regulile de aplicații**. `3` – **Blochează**. `4` – **Permite** și **Înregistrează evenimentele în jurnal**. `6` – **După regulile de aplicații** și **Înregistrează evenimentele în jurnal**. `7` – **Blochează** și **Înregistrează evenimentele în jurnal**.
`</key>`		

Nodul `Resources` conține setările regulii pentru pachetele de rețea. Setările regulii pentru pachetele de rețea personalizate se găsesc în blocul `<key name="0004">`.

Indicatorii regulii pentru pachetele de rețea personalizată

```
<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>
```

Setările regulii pentru pachetele de rețea personalizate

Parametru	Descriere	Valoare
`<key name="Data">`	ID-ul blocului parametrului.	Număr întreg
`RemotePorts`	Valoarea parametrului **Porturi la distanță**.	Lista intervalelor porturilor la distanță.
`LocalPorts`	Valoarea parametrului **Porturi locale**.	Lista intervalelor porturilor locale.

Parametru	Descriere	Valoare
`AdapterBindings`	Valoarea parametrului **Plăci de rețea**.	`IpAddresses` – valoarea parametrului **Adrese IP**. `MacAddresses` – valoarea parametrului **Adrese MAC**. `AdapterName` – numele plăcii de rețea. `InterfaceType` – valoarea parametrului **Tip interfață**: • `0` – **Altele**. • `1` – **LoopBack**. • `2` – **Rețea cu fir (Ethernet)**. • `3` – **Rețea fără fir (Wi-Fi)**. • `4` – **Tunel**. • `5` – **Conexiune PPP**. • `6` – **Conexiune PPPoE**. • `7` – **Conexiune VPN**. • `8` – **Conexiune modem**.
`unique`	ID-ul intern al structurii.	Număr întreg Se recomandă ca acest parametru să nu fie modificat.
`Proto`	Valoarea parametrului **Protocol**.	`0` – dezactivat. `1` – **ICMP**. `2` – **IGMP**. `6` – **TCP**. `17` – **UDP**. `47` – **GRE**. `58` – **ICMPv6**.
`Direction`	Valoarea parametrului **Direcție**.	`1` – **Intrare (pachet)**. `2` – **Ieșire (pachet)**. `3` – **Intrare/Ieșire**. `4` – **Intrare**. `5` – **Ieșire**.

Parametru	Descriere	Valoare
`IcmpType`	Valoarea parametrului **Tip de ICMP**.	**Protocolul ICMP** `0` – **Răspuns cu ecou** (ICMP) sau dezactivat. `3` – **Destinație inaccesibilă** (ICMP). `4` – **Stingere sursă**. `5` – **Redirecționare**. `6` – **Adresă alternativă gazdă**. `8` – **Solicitare ecou**. `9` – **Anunț ruter**. `10` – **Solicitare ruter**. `11` – **Timp depășit**. `12` – **Problemă parametru**. `13` – **Marcă de timp**. `14` – **Răspuns cu marcă de timp**. `15` – **Solicitare de informații**. `16` – **Răspuns la informații**. `17` – **Solicitare mască adresă**. `18` – **Răspuns mască de adresă**. `30` – **Rută de urmărire**. `31` – **Eroare conversie diagramă de informații**. `32` – **Redirecționare gazdă mobilă**. `33` – **IPv6 Where-Are-You**. `34` – **IPv6 I-Am-Here**. `35` – **Solicitare înregistrare mobilă**. `36` – **Răspuns la înregistrare mobilă**. `37` – **Solicitare nume domeniu**. `38` – **Răspuns nume domeniu**. `40` – **Photuris**. **Protocolul ICMPv6** `1` – **Destinație inaccesibilă**. `2` – **Pachet prea mare**. `3` – **Timp depășit**. `4` – **Problemă parametru**. `128` – **Solicitare ecou**. `129` – **Răspuns cu ecou**. `130` – **Interogare listener cu difuzare multiplă**. `131` – **Raport listener cu difuzare multiplă**. `132` – **Listener cu difuzare multiplă terminat**. `133` – **Solicitare ruter**. `134` – **Anunț ruter**. `135` – **Solicitare de la vecin**. `136` – **Anunț de la vecin**. `137` – **Redirecționare mesaj**. `138` – **Renumerotare ruter**. `139` – **Interogare informații nod ICMP**. `141` – **Mesaj de solicitare descoperire vecin inversă**. `142` – **Mesaj de semnalizare descoperire vecin inversă**. `143` – **Raport listener cu difuzare multiplă versiunea 2**.

Parametru	Descriere	Valoare
		`144` – **Mesaj de solicitare descoperire adresă agent la domiciliu**. `145` – **Mesaj de răspuns la descoperire adresă agent la domiciliu**. `146` – **Solicitare cu prefix mobil**. `147` – **Anunț cu prefix mobil**. `148` – **Mesaj de solicitare cale de certificare**. `149` – **Mesaj de anunț cale de certificare**. `151` – **Anunț ruter cu difuzare multiplă**. `152` – **Solicitare ruter cu difuzare multiplă**. `153` – **Terminare ruter cu difuzare multiplă**.
`IcmpCode`	Valoarea parametrului **Cod ICMP**.	`0` – **Cod 0** sau dezactivat. `1` – **Cod 1**. `2` – **Cod 2**.
`Flags`	Indicator atribut structură.	Număr întreg Se recomandă ca acest parametru să nu fie modificat.
`TTL`	Valoarea parametrului **Timp de viață (TTL)**.	Valoarea în secunde. Dacă este dezactivat, valoarea este `0`.
`</key>`		
`Id`	ID-ul principal al resursei (vezi și nodul `Rules`).	Număr întreg
`ParentID`	ID-ul grupului principal.	Număr întreg Se recomandă ca acest parametru să nu fie modificat.
`Flags`	Starea regulii.	`6` – regula este dezactivată. `38` – regula este acivată.
`Name`	Numele regulii pentru pachetele de rețea.	Șir

Administrarea regulilor de rețea ale aplicației

În mod implicit, Kaspersky Endpoint Security grupează toate aplicațiile instalate pe computer după numele distribuitorului software-ului ale căror fișiere sau activități de rețea le monitorizează. Grupurile de aplicații sunt, la rândul lor, clasificate în grupuri de încredere. Toate aplicațiile și grupurile de aplicații moștenesc proprietățile de la grupul lor părinte: reguli Application Control, reguli de rețea pentru aplicație și prioritatea în execuție.

În mod asemănător componentei Host Intrusion Prevention, în mod implicit componenta Firewall aplică regulile de rețea pentru un grup de aplicații atunci când filtrează activitățile de rețea ale tuturor aplicațiilor din cadrul grupului. Regulile de rețea pentru grupurile de aplicații definesc drepturile aplicațiilor din cadrul grupului de a accesa diferite conexiuni de rețea.

În mod implicit, Firewall creează un set de reguli de rețea pentru fiecare grup de aplicații care este detectat de Kaspersky Endpoint Security pe computer. Poți modifica acțiunea Firewallului care este aplicată regulilor de rețea ale grupului de aplicații create în mod implicit. Nu poți edita, elimina, dezactiva sau modifica prioritatea regulilor de rețea pentru grupurile de aplicații care sunt create în mod implicit.

De asemenea, poți crea o regulă de rețea pentru o aplicație individuală. Această regulă va avea o prioritate mai mare decât regula de rețea pentru grupul căreia îi aparține aplicația.

Crearea unei reguli de rețea pentru aplicație

În mod implicit, activitatea aplicațiilor este controlată de reguli de rețea definite pentru grupul de încredere la care Kaspersky Endpoint Security a atribuit aplicația când a pornit pentru prima dată. Dacă este necesar, poți crea reguli de rețea pentru un întreg grup de încredere, pentru o aplicație individuală sau pentru un grup de aplicații dintr-un grup de încredere.

Regulile de rețea definite manual au o prioritate mai mare decât regulile de rețea care au fost determinate pentru un grup de încredere. Cu alte cuvinte, dacă regulile pentru aplicații definite manual diferă de regulile pentru aplicații determinate pentru un grup de încredere, componenta Firewall controlează activitatea aplicației conform regulilor pentru aplicații definite manual.

În mod implicit, Firewall creează următoarele reguli de rețea pentru fiecare aplicație:

- orice activitate de rețea în Rețele de încredere;
- orice activitate de rețea în Rețele locale;
- orice activitate de rețea în Rețele publice.

Kaspersky Endpoint Security controlează activitatea de rețea a aplicațiilor în funcție de regulile de rețea predefinite, după cum urmează:

- De încredere și Restricționat la nivel inferior: toate activitatea de rețea este permisă.
- Restricționat la nivel superior și Nu este de încredere: toată activitatea de rețea este blocată.

Regulile predefinite pentru aplicații nu pot fi editate sau șterse.

Puteți crea o regulă de rețea pentru aplicație în următoarele moduri:

- Utilizați instrumentul Monitor rețea.

  Monitorizare rețea este un instrument destinat vizualizării în timp real a informațiilor despre activitatea de rețea a computerului unui utilizator. Aceasta este o metodă convenabilă deoarece nu trebuie să configurați toate setările regulii. Unele setări ale componente Firewall vor fi introduse automat din datele Monitorului de rețea. Instrumentul Monitor rețea este disponibil în interfața aplicației.

- Configurați setările componentei Firewall.

  Aceasta ar trebui să vă permită să reglați fin setările Firewall-ului. Puteți crea reguli pentru orice activitate de rețea, chiar dacă nu există nicio activitate de rețea în prezent.

Când creați reguli de rețea pentru aplicații, nu uitați că regulile pachetului de rețea au prioritate mai mare față de regulile de rețea pentru aplicații.

Cum se utilizează instrumentul Monitor rețea pentru a crea o regulă de rețea pentru aplicație în interfața aplicației

1. În fereastra principală a aplicației, în secțiunea **Monitorizare**, faceți clic pe dala **Monitor rețea**.
2. Accesați fila **Activitate în rețea** sau **Porturi deschise**.

   Fila **Activitate în rețea** afișează toate conexiunile la rețea active în prezent pe computer. Se afișează atât conexiunile la rețea la ieșire, cât și cele la intrare.

   Fila **Porturi deschise** listează toate porturile de rețea deschise ale computerului.
3. În meniul contextual al conexiunii la rețea, selectați **Creați o regulă de rețea pentru aplicație**.

   Se deschide fereastra de reguli și proprietăți a aplicației.
4. Selectați fila **Reguli de rețea**.

   Aceasta deschide o listă de reguli implicite setate de componenta Firewall.
5. Fă clic pe **Adaugă**.

   Aceasta deschide proprietățile regulii pentru rețea.
6. Introdu manual numele serviciului de rețea în câmpul **Nume**.
7. Configurați setările regulii de rețea (consultați tabelul de mai jos).

   Puteți selecta un șablon de regulă predefinit făcând clic pe linkul **Șablon regulă de rețea**. Șabloanele de reguli descriu cele mai frecvent utilizate conexiuni de rețea.

   Toate setările regulilor de rețea vor fi completate automat.
8. Dacă dorești ca acțiunile regulii de rețea să fie reflectate în raport, bifați caseta de selectare **Înregistrează evenimentele în jurnal**.
9. Fă clic pe **Salvează**.

   Noua regulă de rețea va fi adăugată în listă.
10. Utilizați butoanele **Sus** / **Jos** pentru a seta prioritatea regulii de rețea.
11. Salvați-vă modificările.

Cum se utilizează setările componentei Firewall pentru a crea o regulă de rețea pentru aplicație în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **Firewall**.
3. Fă clic pe **Reguli pentru aplicații**.

   Aceasta deschide o listă de reguli implicite setate de componenta Firewall.
4. În lista de aplicații, selectați aplicația sau grupul de aplicații pentru care dorești să creezi o regulă de rețea.
5. Faceți clic dreapta pentru a deschide meniul contextual și selectați **Detalii și reguli**.

   Se deschide fereastra de reguli și proprietăți a aplicației.
6. Selectați fila **Reguli de rețea**.

7. Fă clic pe **Adaugă**.

   Aceasta deschide proprietățile regulii pentru rețea.

8. Introdu manual numele serviciului de rețea în câmpul **Nume**.

9. Configurați setările regulii de rețea (consultați tabelul de mai jos).

   Puteți selecta un șablon de regulă predefinit făcând clic pe linkul **Șablon regulă de rețea**. Șabloanele de reguli descriu cele mai frecvent utilizate conexiuni de rețea.

   Toate setările regulilor de rețea vor fi completate automat.

10. Dacă dorești ca acțiunile regulii de rețea să fie reflectate în raport, bifați caseta de selectare **Înregistrează evenimentele în jurnal**.

11. Fă clic pe **Salvează**.

    Noua regulă de rețea va fi adăugată în listă.

12. Utilizați butoanele **Sus** / **Jos** pentru a seta prioritatea regulii de rețea.

13. Salvați-vă modificările.

Cum se creează o regulă de rețea pentru aplicații în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.

2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

3. În fereastra politicii, selectați **Essential Threat Protection** → **Firewall**.

4. În blocul **Setări Firewall**, fă clic pe butonul **Setări**.

   Aceasta deschide lista cu regulile pentru pachetele de rețea și lista regulilor de rețea pentru aplicații.

5. Accesați fila **Reguli de rețea pentru aplicații**.

6. Fă clic pe **Adaugă**.

7. În fereastra care se deschide, selectează criteriul pentru căutarea aplicației pentru care dorești să creezi o regulă de rețea.

   Puteți introduce numele aplicației sau numele producătorului. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști.

8. Fă clic pe **Împrospătează**.

   Kaspersky Endpoint Security va căuta aplicația în lista consolidată de aplicații instalate pe computerele gestionate. Kaspersky Endpoint Security va afișa o listă cu aplicațiile care satisfac criteriul dvs. de căutare.

9. Selectați aplicația necesară.

10. În lista verticală **Adaugă aplicații selectate la grupul de încredere**, selectați **Grupuri implicite** și faceți clic pe **OK**.

    Aplicația va fi adăugată la grupul implicit.

11. Selectați aplicația relevantă și apoi selectați **Drepturi aplicație** din meniul contextual al aplicației.

    Se deschide fereastra de reguli și proprietăți a aplicației.

12. Selectați fila **Reguli de rețea**.

    Aceasta deschide o listă de reguli implicite setate de componenta Firewall.

13. Fă clic pe **Adaugă**.

    Aceasta deschide proprietățile regulii pentru rețea.

14. Introdu manual numele serviciului de rețea în câmpul **Nume**.

15. Configurați setările regulii de rețea (consultați tabelul de mai jos).

    Puteți selecta un șablon de regulă predefinit făcând clic pe butonul . Șabloanele de reguli descriu cele mai frecvent utilizate conexiuni de rețea.

    Toate setările regulilor de rețea vor fi completate automat.

16. Dacă dorești ca acțiunile regulii de rețea să fie reflectate în raport, bifați caseta de selectare **Înregistrează evenimentele în jurnal**.

17. Salvează noua regulă de rețea.

18. Utilizați butoanele **Sus** / **Jos** pentru a seta prioritatea regulii de rețea.

19. Salvați-vă modificările.

Cum se creează o regulă de rețea pentru aplicații în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Selectați **Communication & Web Protection** → **Firewall**.

5. În blocul **Application rights and protected resources**, faceți clic pe linkul **Application rights**.

   Tastfel se deschide fereastra de configurare a drepturilor aplicațiilor și lista resurselor protejate.

6. Accesați fila **Application rights**.

   Veți vedea o listă cu grupurile de încredere în partea stângă a ferestrei, iar proprietățile acestora în partea dreaptă.

7. În blocul **Applications**, fă clic pe butonul **Add**.

   Aceasta pornește Expertul pentru adăugarea unei aplicații la un grup de încredere.

8. Selectați grupul de încredere relevant pentru aplicație.

9. Selectați **Application**. Mergeți la pasul următor.

   Dacă doriți să creați o regulă de rețea pentru mai multe aplicații, selectați tipul pentru **Group** și definiți un nume pentru grupul de aplicații.

10. În lista de aplicații deschisă, selectați aplicațiile pentru care dorești să creezi o regulă de rețea.

    Utilizați un filtru. Puteți introduce numele aplicației sau numele producătorului. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele * și ? la introducerea unei măști.

11. Ieșiți din Expert.

    Aplicația va fi adăugată în grupul de încredere.

12. În partea stângă a ferestrei, selectați aplicația relevantă.

13. În partea dreaptă a ferestrei, selectați **Network rules** din lista verticală.

    Aceasta deschide o listă de reguli implicite setate de componenta Firewall.

14. Fă clic pe **Add**.

    Aceasta deschide proprietățile regulii pentru aplicație.

15. Introdu manual numele serviciului de rețea în câmpul **Rule name**.

16. Configurați setările regulii de rețea (consultați tabelul de mai jos).

    Puteți selecta un șablon de regulă predefinit făcând clic pe linkul **Select rule template**. Șabloanele de reguli descriu cele mai frecvent utilizate conexiuni de rețea.

    Toate setările regulilor de rețea vor fi completate automat.

17. Dacă dorești ca acțiunile regulii de rețea să fie reflectate în raport, bifați caseta de selectare **Log events**.

18. Salvează regula de rețea.

    Noua regulă de rețea va fi adăugată în listă.

19. Utilizează butonul **Move** pentru a seta prioritatea regulii de rețea.

20. Salvați-vă modificările.

Setări Regulă de rețea pentru aplicație

Parametru	Descriere
Acțiune	**Permite**. **Blochează**.
Protocol	Controlați activitatea de rețea prin protocolul selectat: TCP, UDP, ICMP, ICMPv6, IGMP și GRE. Dacă selectați protocolul ICMP sau ICMPv6, puteți defini tipul și codul de pachet ICMP. Dacă este selectat tipul de protocol TCP sau UDP, poți specifica numerele de port pentru computerul local și computerul la distanță între care urmează să fie monitorizată conexiunea. Interval de valori posibile pentru numerele de port: 0-65535. În fiecare câmp, poți introduce mai multe valori separate prin `,` sau specifica un interval de valori folosind `-`. De exemplu: • `100,101` • `100-130` • `100,110-130`
Direcție	**Intrare**. **Intrare/Ieșire**. **Ieșire**.
Adrese la distanță	Adresele de rețea ale computerelor la distanță care pot trimite și/sau primi pachete de rețea. Componenta Firewall aplică o regulă de rețea pentru intervalul specificat de adrese de rețea la distanță. Puteți include toate adresele IP într-o regulă de rețea, puteți crea o listă separată de adrese IP, puteți specifica un interval de adrese IP sau puteți selecta o subrețea (Rețele de încredere, Rețele locale, Rețele publice). De asemenea, puteți specifica un nume DNS al unui computer în loc de adresa IP a acestuia. Trebuie să utilizați nume DNS numai pentru computerele LAN sau serviciile interne. Interacțiunea cu serviciile cloud (cum ar fi Microsoft Azure) și alte resurse de Internet trebuie gestionată de componenta Control web. Dacă în regula pentru pachetele de rețea ați adăugat un nume DNS pentru care adresa IP nu a putut fi determinată, Kaspersky Endpoint Security va afișa un avertisment. În lista de reguli pentru pachetele de rețea din Web Console este adăugată o coloană ce conține o descriere a erorii. În Consola de administrare (MMC), descrierea erorii nu este disponibilă. Astfel de reguli pentru pachete sunt evidențiate în culori.

Parametru	Descriere
Adrese locale	Adresele de rețea ale computerelor care pot trimite și/sau primi pachete de rețea. Componenta Firewall aplică o regulă de rețea pentru intervalul specificat de adrese de rețea locale. Puteți include toate adresele IP într-o regulă de rețea, puteți crea o listă separată de adrese IP sau puteți specifica un interval de adrese IP. Aplicația stochează adresele locale numai dacă este specificată o listă de adrese la distanță. Aceasta înseamnă că, valoarea **Adrese din listă** a fost selectată pentru **Adrese la distanță** și cel puțin o adresă a fost adăugată. Uneori adresele locale nu pot fi obținute pentru aplicații. Dacă aceasta este situația, acest parametru este ignorat.

Activarea și dezactivarea unei reguli de rețea pentru o aplicație

Pentru a activa sau a dezactiva o regulă de rețea pentru o aplicație:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Essential Threat Protection → Firewall**.
3. Fă clic pe **Reguli pentru aplicații**.

   Aceasta deschide lista regulilor aplicației.
4. În lista de aplicații, selectați aplicația sau grupul de aplicații pentru care dorești să creezi sau să editezi o regulă de rețea.
5. Faceți clic dreapta pentru a deschide meniul contextual și selectați **Detalii și reguli**.

   Se deschide fereastra de reguli și proprietăți a aplicației.
6. Selectați fila **Reguli de rețea**.
7. În lista de reguli de rețea pentru un grup de aplicații, selectați regula de rețea relevantă.

   Se deschide fereastra de proprietăți a regulii de rețea.
8. Setați starea **Activă** sau **Inactivă** pentru regula de rețea.

   Nu poți dezactiva o regulă de rețea pentru un grup de aplicații care este creată de Firewall în mod implicit.
9. Salvați-vă modificările.

Modificarea acțiunii componentei Firewall pentru o regulă de rețea pentru o aplicație

Poți modifica acțiunea pe care componenta Firewall o aplică tuturor regulilor de rețea pentru o aplicație sau un grup de aplicații care au fost create în mod implicit și poți modifica acțiunea pe care componenta Firewall o aplică pentru o regulă de rețea individuală particularizată pentru o aplicație sau un grup de aplicații.

Pentru a modifica acțiunea componentei Firewall pentru toate regulile de rețea pentru o aplicație sau un grup de aplicații:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **Firewall**.
3. Fă clic pe **Reguli pentru aplicații**.

   Aceasta deschide lista regulilor aplicației.
4. Dacă dorești să modifici acțiunea aplicată de componenta Firewall tuturor regulilor de rețea care sunt create în mod implicit, selectați o aplicație sau un grup de aplicații în listă. Regulile de rețea create manual rămân nemodificate.
5. Faceți clic dreapta pentru a deschide meniul contextual, selectați **Reguli de rețea**, apoi selectați acțiunea pe care doriți să o atribuiți:
   - **Moștenește**.
   - **Permite**.
   - **Blochează**.
6. Salvați-vă modificările.

Pentru a modifica răspunsul componentei Firewall pentru o regulă de rețea pentru o aplicație sau un grup de aplicații:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **Firewall**.
3. Fă clic pe **Reguli pentru aplicații**.

   Aceasta deschide lista regulilor aplicației.
4. În listă, selectați aplicația sau grupul de aplicații pentru care dorești să modifici acțiunea pentru o regulă de rețea.
5. Faceți clic dreapta pentru a deschide meniul contextual și selectați **Detalii și reguli**.

   Se deschide fereastra de reguli și proprietăți a aplicației.
6. Selectați fila **Reguli de rețea**.
7. Selectați regula de rețea pentru care dorești să modifici acțiunea componentei Firewall.
8. În coloana **Permisiune**, faceți clic dreapta pentru a afișa meniul contextual și selectați acțiunea pe care dorești s-o atribui:
   - **Moștenește**.
   - **Permite**.

- **Refuză**.
- **Înregistrează evenimentele în jurnal**.

9. Salvați-vă modificările.

Modificarea priorității unei reguli de rețea pentru o aplicație

Prioritatea unei reguli de rețea este determinată de poziția sa în lista de reguli de rețea. Firewall execută regulile în ordinea în care ele apar în lista de reguli de rețea, de sus în jos. Potrivit fiecărei reguli de rețea procesate care se aplică unei anumite conexiuni de rețea, Firewall permite sau blochează accesul de rețea către adresa și portul indicate în setările acestei conexiuni de rețea.

Regulile de rețea create manual au o prioritate mai mare decât regulile de rețea implicite.

Nu poți modifica prioritatea regulilor de rețea pentru grupurile de aplicații care sunt create în mod implicit.

Pentru a modifica prioritatea unei reguli de rețea:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **Firewall**.
3. Fă clic pe **Reguli pentru aplicații**.

   Aceasta deschide lista regulilor aplicației.
4. În lista de aplicații, selectați aplicația sau grupul de aplicații pentru care dorești să modifici prioritatea pentru o regulă de rețea.
5. Faceți clic dreapta pentru a deschide meniul contextual și selectați **Detalii și reguli**.

   Se deschide fereastra de reguli și proprietăți a aplicației.
6. Selectați fila **Reguli de rețea**.
7. Selectați regula de rețea a cărei prioritate dorești să o modifici.
8. Utilizați butoanele **Sus** / **Jos** pentru a seta prioritatea regulii de rețea.
9. Salvați-vă modificările.

Monitorizare rețea

Monitorizare rețea este un instrument destinat vizualizării în timp real a informațiilor despre activitatea de rețea a computerului unui utilizator.

Pentru a porni instrumentul Monitorizare rețea:

În fereastra principală a aplicației, în secțiunea **Monitorizare**, faceți clic pe dala **Monitor rețea**.

Se deschide fereastra Monitorizare rețea. Informațiile despre activitatea de rețea a computerului sunt afișate în cele patru file ale acestei ferestre:

- Fila **Activitate în rețea** afișează toate conexiunile la rețea active în prezent pe computer. Se afișează atât conexiunile la rețea la ieșire, cât și cele la intrare. În această filă, puteți, de asemenea, crea reguli pentru pachetele de rețea pentru funcționarea componentei Firewall.
- Fila **Porturi deschise** listează toate porturile de rețea deschise ale computerului. În această filă, puteți, de asemenea, crea reguli pentru pachetele de rețea și reguli pentru aplicații pentru funcționarea componentei Firewall.
- Fila **Trafic rețea** afișează volumul de trafic de rețea la intrare și la ieșire între computerul utilizatorului și celelalte computere din rețeaua la care utilizatorul este conectat în prezent.
- Fila **Computere blocate** listează adresele IP ale computerelor la distanță a căror activitate de rețea a fost blocată de componenta Network Threat Protection după detectarea încercărilor de atacuri de rețea inițiate de la aceste adrese IP.

Exploit Prevention

Componenta Exploit Prevention detectează codul programului care profită de vulnerabilitățile de pe un computer pentru a exploata privilegiile de administrator sau pentru a efectua activități dăunătoare. De exemplu, exploiturile pot utiliza un atac de supraîncărcare a memoriei tampon. Pentru a face acest lucru, exploitul trimite o cantitate mare de date unei aplicații vulnerabile. Atunci când prelucrează aceste date, aplicația vulnerabilă execută un cod rău intenționat. În urma acestui atac, exploitul poate porni instalarea neautorizată a unui program malware. Atunci când se încearcă executarea unui fișier executabil al unei aplicații vulnerabile care nu a fost efectuată de utilizator, Kaspersky Endpoint Security blochează executarea acestui fișier sau notifică utilizatorul.

Componenta Exploit Prevention monitorizează suplimentar porturile de rețea pentru procese ale aplicațiilor care pot amenința securitatea computerului. Aplicația obține informații despre astfel de procese cu ajutorul bazelor de date antivirus.

Activarea și dezactivarea componentei Exploit Prevention

În mod implicit, componenta Exploit Prevention este activată și funcționează într-un mod optim. Kaspersky Endpoint Security monitorizează fișierele executabile rulate de aplicațiile vulnerabile. Dacă aplicația Kaspersky Endpoint Security detectează faptul că a fost rulat un fișier executabil de la o aplicație vulnerabilă de către oricine altcineva decât utilizatorul, Kaspersky Endpoint Security va executa acțiunea selectată (de exemplu, va bloca operația).

Cum se activează sau dezactivează componenta Exploit Prevention în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Advanced Threat Protection → Exploit Prevention**.
4. Utilizează caseta de selectare **Exploit Prevention** pentru a activa sau a dezactiva componenta.

5. Selectați acțiunea relevantă în blocul **La detectarea exploatării**:

   - **Blochează**. Dacă este selectat acest element, atunci când este detectat un exploit, Kaspersky Endpoint Security blochează operațiunile acestui exploit și înregistrează în jurnal informațiile despre acest exploit.

   - **Informează**. Dacă este selectat acest element, atunci când Kaspersky Endpoint Security detectează o exploatare, înregistrează în jurnal informațiile despre exploatare și adaugă informațiile despre aceasta în lista amenințărilor active.

6. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se activează sau dezactivează componenta Exploit Prevention în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **Host Threat Protection** → **Behavior Analysis** → **Exploit Prevention**.

5. Utilizați comutatorul **Exploit Prevention** pentru a activa sau a dezactiva componenta.

6. Selectați acțiunea relevantă în blocul **Action on threat detection**:

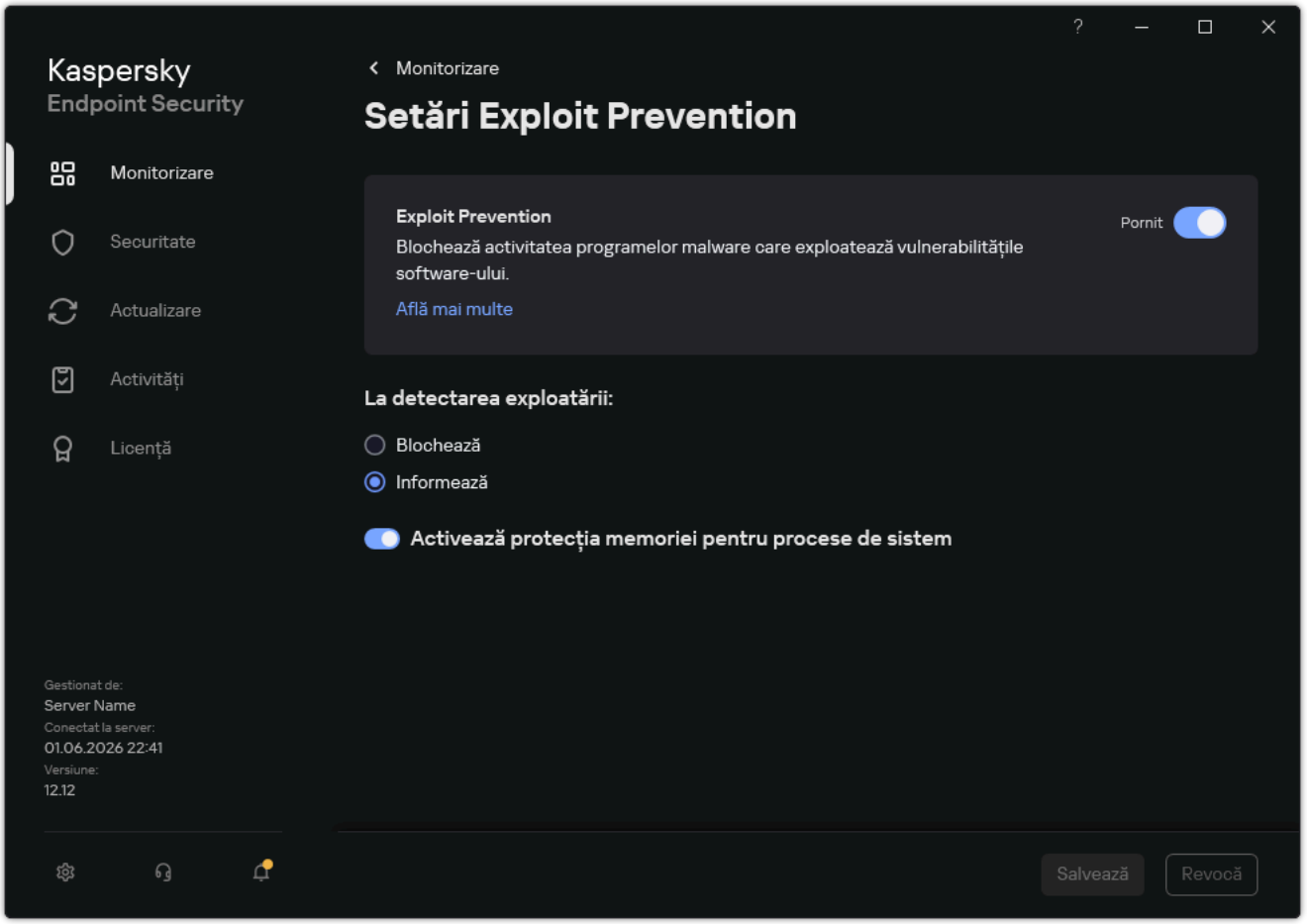
   - **Block**. Dacă este selectat acest element, atunci când este detectat un exploit, Kaspersky Endpoint Security blochează operațiunile acestui exploit și înregistrează în jurnal informațiile despre acest exploit.

   - **Inform**. Dacă este selectat acest element, atunci când Kaspersky Endpoint Security detectează o exploatare, înregistrează în jurnal informațiile despre exploatare și adaugă informațiile despre aceasta în lista amenințărilor active.

7. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se activează sau dezactivează componenta Exploit Prevention în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Advanced Threat Protection** → **Exploit Prevention**.



Setări Exploit Prevention

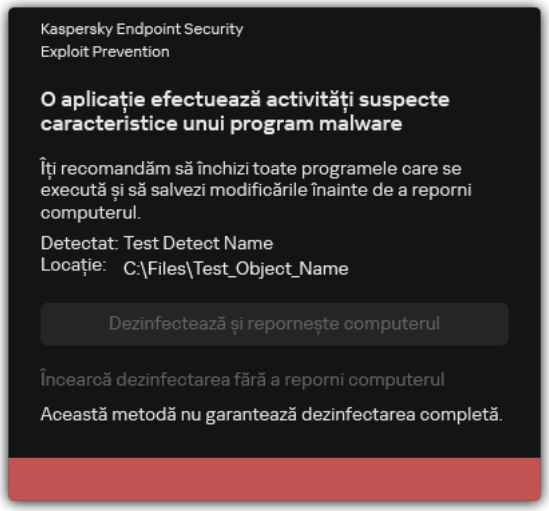
3. Utilizați comutatorul **Exploit Prevention** pentru a activa sau a dezactiva componenta.

4. Selectați acțiunea relevantă în blocul **La detectarea exploatării**:

   - **Blochează**. Dacă este selectat acest element, atunci când este detectat un exploit, Kaspersky Endpoint Security blochează operațiunile acestui exploit și înregistrează în jurnal informațiile despre acest exploit.

   - **Informează**. Dacă este selectat acest element, atunci când Kaspersky Endpoint Security detectează o exploatare, înregistrează în jurnal informațiile despre exploatare și adaugă informațiile despre aceasta în lista amenințărilor active.

5. Salvați-vă modificările.



Notificare cu privire la amenințarea activă

Protecție memorie pentru procese de sistem

În mod implicit, protecția memoriei pentru procese de sistem este activată. Kaspersky Endpoint Security blochează procesele externe care încearcă să obțină acces la procesele de sistem.

Cum se activează sau dezactivează protecția memoriei pentru procesele de sistem în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.

2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

3. În fereastra politicii, selectați **Advanced Threat Protection** → **Exploit Prevention**.

4. Utilizează caseta de selectare **Activează protecția memoriei pentru procese de sistem** pentru a activa sau a dezactiva opțiunea.

5. Salvați-vă modificările.

Cum se activează sau dezactivează protecția memoriei pentru procesele de sistem în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **Host Threat Protection** → **Behavior Analysis** → **Exploit Prevention**.

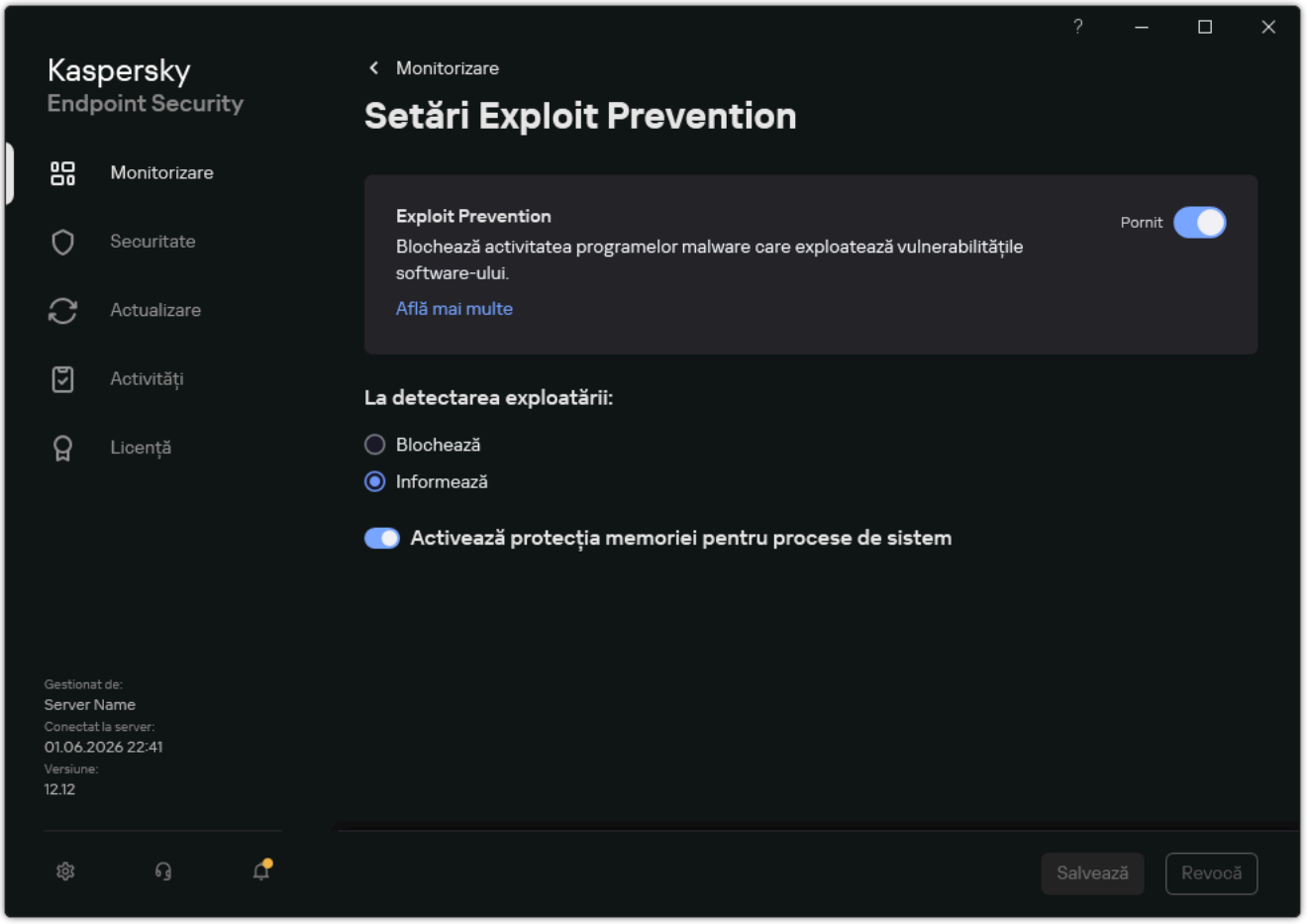
5. Utilizați comutatorul **System process memory protection ENABLED** pentru a activa sau a dezactiva această caracteristică.

6. Salvați-vă modificările.

Cum se activează sau dezactivează protecția memoriei pentru procesele de sistem în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul .

2. În fereastra cu setările aplicației, selectați **Advanced Threat Protection** → **Exploit Prevention**.



Setări Exploit Prevention

3. Utilizați comutatorul **Activează protecția memoriei pentru procese de sistem** pentru a activa sau a dezactiva această caracteristică.

4. Salvați-vă modificările.

Behavior Detection

Componenta Behavior Detection primește date despre acțiunile aplicațiilor de pe computer și transmite aceste informații altor componente de protecție pentru a le îmbunătăți performanța. Componenta Behavior Detection utilizează Semnăturile de flux de comportamental (Behavior Stream Signatures, BSS) pentru aplicații. Dacă activitatea aplicației corespunde unei semnături de șir comportamental, Kaspersky Endpoint Security execută acțiunea de răspuns selectată. Funcționalitatea Kaspersky Endpoint Security se bazează pe semnături de flux comportamental și oferă o apărare proactivă pentru computer.

Componenta Behavior Detection monitorizează suplimentar porturile de rețea pentru procese ale aplicațiilor care pot amenința securitatea computerului. Aplicația obține informații despre astfel de procese cu ajutorul bazelor de date antivirus.

În mod implicit, componenta Behavior Detection este activată și se execută în modul recomandat de experții Kaspersky. Atunci când este detectată o activitate rău intenționată, Kaspersky Endpoint Security șterge fișierul executabil al aplicației rău intenționate.

Nu vă recomandăm să dezactivați componenta Behavior Detection decât dacă acest lucru este absolut necesar, deoarece această acțiune ar reduce eficiența componentelor protecției. Componentele protecției pot solicita date colectate de componenta Behavior Detection pentru a detecta amenințări.

Cum se activează sau dezactivează componenta Behavior Detection în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați **Policies**.
3. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
4. În fereastra politicii, selectați **Advanced Threat Protection** → **Behavior Detection**.
5. Utilizează caseta de selectare **Behavior Detection** pentru a activa sau a dezactiva componenta.
6. Selectați acțiunea relevantă în blocul **Acțiune la detectarea activității malware**:
   - **Șterge**. Dacă este selectat acest element, atunci când detectează o activitate periculoasă, Kaspersky Endpoint Security șterge fișierul executabil al aplicației periculoase și creează o copie de rezervă a fișierului în Copie de rezervă.
   - **Blochează**. Dacă este selectat acest element, la detectarea unei activități rău intenționate Kaspersky Endpoint Security termină această aplicație.
   - **Informează**. Dacă este selectat acest element și se detectează activitate de tip malware a unei aplicații, Kaspersky Endpoint Security adaugă informații despre activitatea de tip malware a aplicației în lista de amenințări active.
7. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se activează sau dezactivează componenta Behavior Detection în Web Console și Cloud Console

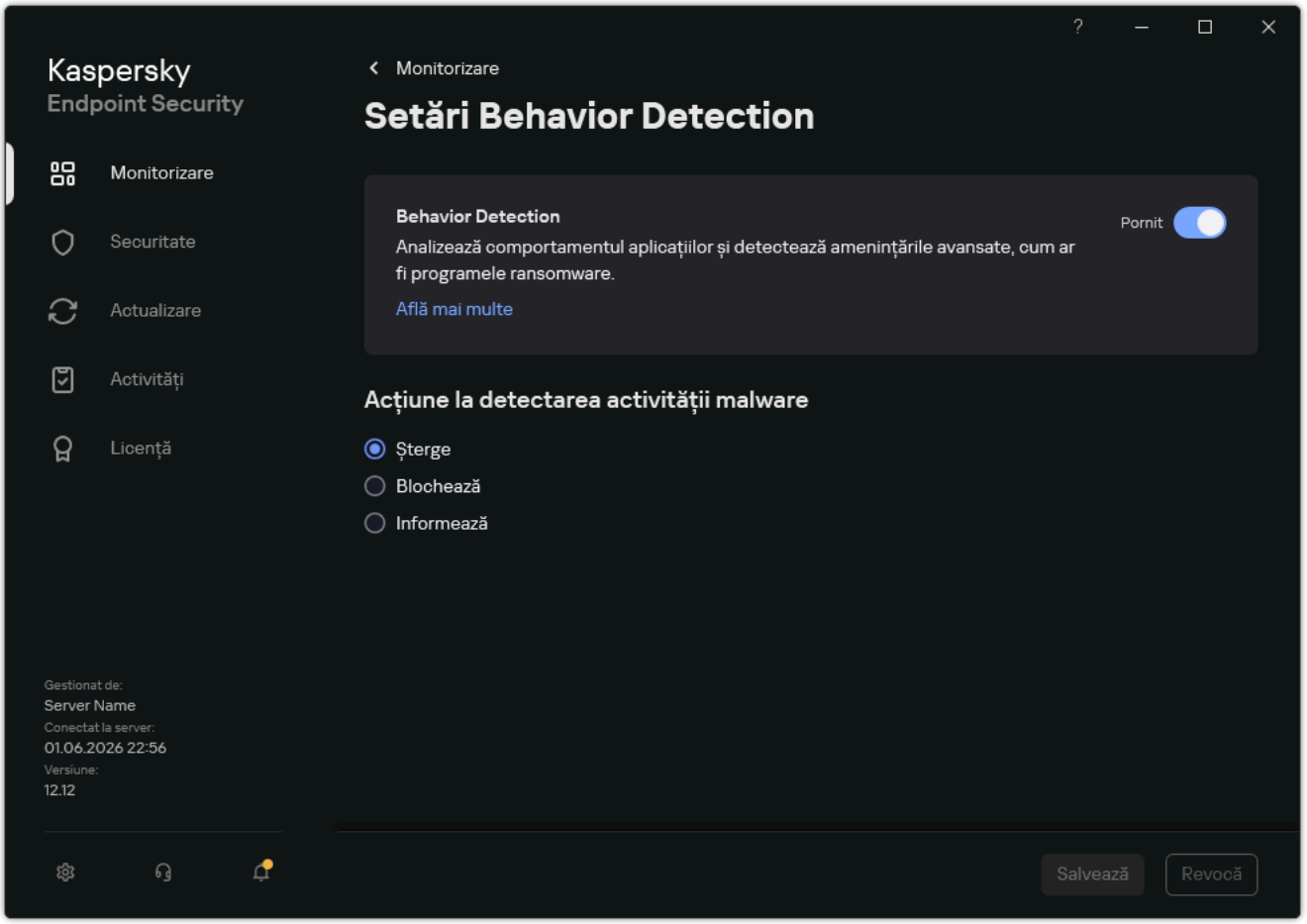
1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Host Threat Protection** → **Behavior Analysis** → **Behavior Detection**.
5. Utilizați comutatorul **Behavior Detection ENABLED** pentru a activa sau a dezactiva componenta.
6. Selectați acțiunea relevantă în blocul **Action on threat detection**:

   - **Delete**. Dacă este selectat acest element, atunci când detectează o activitate periculoasă, Kaspersky Endpoint Security șterge fișierul executabil al aplicației periculoase și creează o copie de rezervă a fișierului în Copie de rezervă.
   - **Block**. Dacă este selectat acest element, la detectarea unei activități rău intenționate Kaspersky Endpoint Security termină această aplicație.
   - **Inform**. Dacă este selectat acest element și se detectează activitate de tip malware a unei aplicații, Kaspersky Endpoint Security adaugă informații despre activitatea de tip malware a aplicației în lista de amenințări active.
7. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se activează sau dezactivează componenta Behavior Detection în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Advanced Threat Protection → Behavior Detection**.



Setări Behavior Detection

3. Utilizați comutatorul **Behavior Detection** pentru a activa sau a dezactiva componenta.
4. Selectați acțiunea relevantă în blocul **Acțiune la detectarea activității malware**:
   - **Șterge**. Dacă este selectat acest element, atunci când detectează o activitate periculoasă, Kaspersky Endpoint Security șterge fișierul executabil al aplicației periculoase și creează o copie de rezervă a fișierului în Copie de rezervă.
   - **Blochează**. Dacă este selectat acest element, la detectarea unei activități rău intenționate Kaspersky Endpoint Security termină această aplicație.
   - **Informează**. Dacă este selectat acest element și se detectează activitate de tip malware a unei aplicații, Kaspersky Endpoint Security adaugă informații despre activitatea de tip malware a aplicației în lista de amenințări active.
5. Salvați-vă modificările.

Ca rezultat, dacă Behavior Detection este activat, Kaspersky Endpoint Security va utiliza semnături de flux de comportament pentru a analiza activitatea aplicațiilor din sistemul de operare.

Anti-Cryptor

Începând cu Kaspersky Endpoint Security 12.12 pentru Windows, protecția directoarelor partajate împotriva criptării externe care făcea parte din componenta Behavior Detection este o componentă separată, Anti-Cryptor.

Componenta monitorizează operațiunile efectuate numai cu fișierele stocate pe dispozitivele de stocare în masă cu sistem de fișiere NTFS și care nu sunt criptate cu EFS.

Componenta Anti-Cryptor analizează activitatea din directoarele partajate. Dacă această activitate corespunde unei semnături de flux comportamental care este tipică pentru criptare externă, Kaspersky Endpoint Security execută acțiunea selectată.

Pentru ca componenta Anti-Cryptor să funcționeze, trebuie să activezi componenta Behavior Detection.

Dacă Kaspersky Endpoint Security detectează o încercare de modificare a fișierelor din directoarele partajate, aceasta efectuează următoarele acțiuni:

- Blochează accesul la modificarea fișierului pentru sesiunea care a inițiat activitatea rău intenționată.
- Creează copii de rezervă ale fișierelor care sunt modificate.
- Adaugă o intrare la rapoartele interfeței aplicației locale și trimite informații despre activitatea rău intenționată detectată către Kaspersky Security Center.
- De asemenea, în cazul în care componenta Remediation Engine este activată, fișierele modificate sunt restaurate din copiile de rezervă.

Activarea sau dezactivarea protecției directoarelor partajate împotriva criptării externe

În mod implicit, protecția directoarelor partajate împotriva criptării externe este activată și funcționează conform recomandărilor experților Kaspersky. Pentru a configura această funcționalitate, poți crea un domeniu de protecție și poți configura excluderi, dacă este necesar. În mod implicit, aplicația identifică automat directoarele partajate și monitorizează activitatea fișierelor din toate directoarele. Când este detectată o încercare criptare externă a fișierele din directoarele partajate, Kaspersky Endpoint Security blochează sesiunea utilizatorului la distanță timp de o oră (în mod implicit).

După instalarea Kaspersky Endpoint Security, protecția directoarelor partajate împotriva criptării externe va fi limitată până la repornirea computerului.

Cum se activează sau dezactivează protecția directoarelor partajate împotriva criptării externe în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Advanced Threat Protection** → **Anti-Cryptor**.
4. Utilizează caseta de selectare **Anti-Cryptor** pentru a activa sau a dezactiva detectarea activității tipice criptării externe.
5. Selectează acțiunea relevantă pe care o va întreprinde aplicația atunci când este detectată o încercare de modificare a fișierelor din directoarele partajate:
   - **Blochează conexiunea pentru N min**. Dacă această opțiune este selectată, atunci când Kaspersky Endpoint Security detectează o încercare de modificare a fișierelor din directoarele partajate, acesta blochează accesul la modificarea fișierelor pentru sesiunea care a inițiat activitatea rău intenționată și creează copii de rezervă ale fișierelor modificate.

     Dacă activată componenta Remediation Engine este și este selectată opțiunea **Blochează conexiunea pentru N min**, fișierele modificate sunt restaurate din copiile de rezervă.

   - **Informează**. Dacă această opțiune este selectată, la detectarea unei încercări de modificare a fișierelor din directoarele partajate, Kaspersky Endpoint Security adaugă informații despre această încercare în lista amenințărilor active, adaugă o intrare în rapoartele interfeței aplicației locale și trimite informații despre activitatea rău intenționată detectată către Kaspersky Security Center.
6. Dacă este necesar, editează un domeniu de protecție și definește excluderile.
7. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se activează sau dezactivează protecția directoarelor partajate împotriva criptării externe în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Host Threat Protection** → **Behavior Analysis** → **Anti-Cryptor**.
5. Utilizați comutatorul **Anti-Cryptor ENABLED** pentru a activa sau a dezactiva detectarea activității tipice criptării externe.

6. Selectează acțiunea relevantă pe care o va întreprinde aplicația atunci când este detectată o încercare de modificare a fișierelor din directoarele partajate:

   - **Block connection for (min) N min**. Dacă această opțiune este selectată, atunci când Kaspersky Endpoint Security detectează o încercare de modificare a fișierelor din directoarele partajate, acesta blochează accesul la modificarea fișierelor pentru sesiunea care a inițiat activitatea rău intenționată și creează copii de rezervă ale fișierelor modificate.

     Dacă activată componenta Remediation Engine este și este selectată opțiunea **Block connection for (min) N min**, fișierele modificate sunt restaurate din copiile de rezervă.

   - **Inform**. Dacă această opțiune este selectată, la detectarea unei încercări de modificare a fișierelor din directoarele partajate, Kaspersky Endpoint Security adaugă informații despre această încercare în lista amenințărilor active, adaugă o intrare în rapoartele interfeței aplicației locale și trimite informații despre activitatea rău intenționată detectată către Kaspersky Security Center.

7. Dacă este necesar, editează un domeniu de protecție și definește excluderile.

8. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se activează sau dezactivează protecția directoarelor partajate împotriva criptării externe în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Advanced Threat Protection** → **Anti-Cryptor**.

3. Utilizează caseta de selectare **Protecția directoarelor partajate împotriva criptării externe** pentru a activa sau a dezactiva detectarea activității tipice criptării externe.

4. Utilizează caseta de selectare **Protecția directoarelor partajate împotriva criptării externe** pentru a activa sau a dezactiva detectarea activității tipice criptării externe.

5. Selectează acțiunea relevantă pe care o va întreprinde aplicația atunci când este detectată o încercare de modificare a fișierelor din directoarele partajate:

   - **Blochează conexiunea pentru (min) N min**. Dacă această opțiune este selectată, atunci când Kaspersky Endpoint Security detectează o încercare de modificare a fișierelor din directoarele partajate, acesta blochează accesul la modificarea fișierelor pentru sesiunea care a inițiat activitatea rău intenționată și creează copii de rezervă ale fișierelor modificate.

     Dacă activată componenta Remediation Engine este și este selectată opțiunea **Blochează conexiunea pentru (min) N min**, fișierele modificate sunt restaurate din copiile de rezervă.

   - **Informează**. Dacă această opțiune este selectată, la detectarea unei încercări de modificare a fișierelor din directoarele partajate, Kaspersky Endpoint Security adaugă informații despre această încercare în lista amenințărilor active, adaugă o intrare în rapoartele interfeței aplicației locale și trimite informații despre activitatea rău intenționată detectată către Kaspersky Security Center.

6. Dacă este necesar, editează un domeniu de protecție și definește excluderile.

7. Salvați-vă modificările.

Configurarea perioadei de blocare a unui computer care nu are încredere

Un *computer care nu este de încredere* este un computer la distanță care se implică în activități rău intenționate sau în criptarea datelor. În mod implicit, Kaspersky Endpoint Security blochează sesiunea utilizatorului la distanță timp de o oră. Când perioada de blocare expiră, Kaspersky Endpoint Security elimină computerul din lista de blocate și restabilește accesul la directoryl partajat.

Cum se configurează perioada de blocare a unui computer care nu este de încredere în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Advanced Threat Protection** → **Anti-Cryptor**.
4. În blocul **Acțiune la detectarea amenințării**, selectează **Blochează conexiunea pentru N min**.
5. Configurează perioada de blocare a unui computer care nu este de încredere care se implică în activități rău intenționate sau în criptarea datelor.
6. Salvați-vă modificările.

Cum se configurează perioada de blocare a unui computer care nu este de încredere în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Host Threat Protection** → **Behavior Analysis** → **Anti-Cryptor**.
5. în **Action on threat detection**, configurează perioada de blocare a unui computer care nu este de încredere care se implică în activități rău intenționate sau în criptarea datelor.
6. Salvați-vă modificările.

Cum se configurează perioada de blocare a unui computer care nu este de încredere în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Advanced Threat Protection** → **Anti-Cryptor**.
3. În secțiunea **Acțiune la detectarea amenințării**, selectați **Blochează conexiunea pentru (min)**.

4. Configurează perioada de blocare a unui computer care nu este de încredere care se implică în activități rău intenționate sau în criptarea datelor.

5. Salvați-vă modificările.

Ca rezultat, computerul la distanță va fi blocat. Pentru a debloca computerul la distanță, poți reporni Kaspersky Endpoint Security.

Editarea domeniului de protecție

Domeniul de protecție este o listă de căi către directoarele partajate în care Kaspersky Endpoint Security monitorizează activitatea fișierelor. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști. În mod implicit, aplicația identifică automat directoarele partajate și monitorizează activitatea fișierelor din toate directoarele.

Excluderea unui director de la domeniul de protecție poate reduce numărul de alarme false dacă organizația ta folosește criptarea datelor atunci când face schimb de fișiere utilizând directoarele partajate. De exemplu, Behavior Detection poate declanșa alarme false atunci când utilizatorul lucrează cu fișiere cu extensia ENC într-un director partajat. O astfel de activitate corespunde unui model de comportament care este tipic pentru criptarea externă. Dacă ai criptat fișierele dintr-un director pentru protejarea datelor, adaugă acel director la excluderi.

> De asemenea, poți exclude computerele de la care încercările de criptare externă nu trebuie gestionate.

Cum se editează un domeniu de protecție în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.

2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

3. În fereastra politicii, selectați **Advanced Threat Protection** → **Anti-Cryptor**.

4. În secțiunea **Domeniu de protecție**, selectați **Numai directoarele partajate specificate**.

5. În lista cu directoare, fă clic pe **Adaugă**.

6. Această acțiune deschide o fereastră; în acea fereastră, introdu calea către directorul partajat pe care dorești să îl incluzi în domeniul de protecție (de exemplu, `C:\Share`).

   > Pentru a adăuga un director partajat la domeniul de protecție, utilizează o cale locală.

7. Fă clic pe **OK**.

8. Dacă este necesar, definește excluderile de la domeniul de protecție:

   a. În blocul **Excluderi de la scanare**, fă clic pe butonul **După mască**.

   b. În fereastra care se deschide, faceți clic pe butonul **Adaugă**.

c. În fereastra afișată, specifică o extensie de fișier în formatul `*.<file extension>` format sau o cale către fișier. Kaspersky Endpoint Security acceptă caracterele `*` și `?` la introducerea unei măști.

Aplicația nu acceptă unele extensii de fișiere de excludere. Astfel, poți specifica o excludere ca `*.docx` sau `**\Folder\**`.

Poți exclude un obiect de la scanare fără a-l șterge din lista de obiecte din domeniul de protecție. Pentru aceasta, debifați caseta de selectare de lângă obiect.

9. Salvați-vă modificările.

Cum se editează un domeniu de protecție în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Host Threat Protection** → **Behavior Analysis** → **Anti-Cryptor**.
5. În secțiunea **Protection scope**, selectați **Only specified shared folders**.
6. În lista cu directoare, fă clic pe **Add**.
7. Această acțiune deschide o fereastră; în acea fereastră, introdu calea către directorul partajat pe care dorești să îl incluzi în domeniul de protecție (de exemplu, `C:\Share`).

   Pentru a adăuga un director partajat la domeniul de protecție, utilizează o cale locală.
8. Fă clic pe **OK**.
9. Dacă este necesar, definește excluderile de la domeniul de protecție:

   a. În partea superioară a ferestrei, fă clic pe linkul **Scan exclusions**.

   b. În fereastra care se deschide, faceți clic pe butonul **Add**.

   c. În fereastra afișată, specifică o extensie de fișier în formatul `*.<file extension>` format sau o cale către fișier. Kaspersky Endpoint Security acceptă caracterele `*` și `?` la introducerea unei măști.

   Aplicația nu acceptă unele extensii de fișiere de excludere. Astfel, poți specifica o excludere ca `*.docx` sau `**\Folder\**`.

   Poți exclude un obiect de la scanare fără a-l șterge din lista de obiecte din domeniul de protecție. Pentru aceasta, debifați caseta de selectare de lângă obiect.
10. Salvați-vă modificările.

Cum se editează un domeniu de protecție în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Advanced Threat Protection** → **Anti-Cryptor**.

3. În secțiunea **Domeniu de protecție**, selectați **Numai directoarele partajate specificate**.

4. În lista cu directoare, fă clic pe **Adaugă**.

5. Această acțiune deschide o fereastră; în acea fereastră, introdu calea către directorul partajat pe care dorești să îl incluzi în domeniul de protecție (de exemplu, `C:\Share`).

   > Pentru a adăuga un director partajat la domeniul de protecție, utilizează o cale locală.

6. Fă clic pe **OK**.

7. Dacă este necesar, definește excluderile de la domeniul de protecție:

   a. În partea superioară a ferestrei, fă clic pe linkul **Excluderi după mască**.

   b. În fereastra care se deschide, faceți clic pe butonul **Adaugă**.

   c. În fereastra afișată, specifică o extensie de fișier în formatul `*.<file extension>` format sau o cale către fișier. Kaspersky Endpoint Security acceptă caracterele `*` și `?` la introducerea unei măști.

      Aplicația nu acceptă unele extensii de fișiere de excludere. Astfel, poți specifica o excludere ca `*.docx` sau `**\Folder\**`.

   Poți exclude un obiect de la scanare fără a-l șterge din lista de obiecte din domeniul de protecție. Pentru aceasta, debifați caseta de selectare de lângă obiect.

8. Salvați-vă modificările.

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Setări generale** → **Excluderi și tipuri de obiecte detectate**.

3. În blocul **Excluderi**, faceți clic pe linkul **Gestionează excluderile**.

4. Fă clic pe **Adaugă**.

5. Faceți clic pe **Răsfoiește** și selectați directorul partajat.

De asemenea, puteți introduce calea manual. Kaspersky Endpoint Security acceptă caracterele `*` și `?` la introducerea unei măști:

- Caracterul `*` (asterisc) ține locul oricărui set de caractere, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\*\*.txt` va include toate căile către fișierele cu extensia TXT din directoarele de pe unitatea C:, dar nu și din subdirectoare.

- Două caractere `*` consecutive țin locul oricărui set de caractere (inclusiv un set gol) din numele de fișier sau director, inclusiv caracterele `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\**\*.txt` va include toate căile către fișierele cu extensia TXT localizată în directoarele imbricate în `Folder`, cu excepția `Folder` în sine. Masca trebuie să includă cel puțin un nivel de imbricare. Masca `C:\**\*.txt` nu este o mască validă.

- `?` (semn de întrebare) ține locul oricărui caracter individual, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\???.txt` va include căi pentru toate fișierele din directorul denumit `Folder` care au extensia TXT și un nume format din trei caractere.

Puteți utiliza măști la începutul, la mijlocul sau la sfârșitul căii fișierului. De exemplu, dacă doriți să adăugați un director pentru toți utilizatorii la excluderi, introduceți masca `?:\Users\*\Folder\`.

6. În blocul **Componente de protecție**, selectați componenta **Behavior Detection**.

7. Dacă este necesar, în câmpul **Comentariu**, introdu o descriere succintă a excluderii de la scanare pe care o creezi.

8. Selectați starea **Activă** pentru excludere.

   Puteți utiliza comutatorul pentru a stop an exclusion în orice moment.

9. Salvați-vă modificările.

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesează secțiunea **Trusted Zone**.

5. În fereastra care se deschide, fă clic pe linkul **Malware Scan exclusions**.

6. Bifați caseta de selectare **Merge values when inheriting** dacă doriți să creați o listă consolidată a excluderilor pentru toate computerele companiei. Listele excluderilor din politicile principale și secundare vor fi îmbinate. Listele vor fi îmbinate dacă funcția de îmbinare a valorilor în momentul moștenirii este activată. Excluderile de la din politica principală sunt afișate în politicile secundare într-o vizualizare numai citire. Nu este posibilă modificarea sau ștergerea excluderilor din politica principală.

7. Bifați caseta de selectare **Allow use of local exclusions** dacă doriți să permiteți utilizatorului să creeze o listă locală de excluderi. În acest fel, un utilizator își poate crea propria listă locală de excluderi pe lângă lista generală de excluderi generate în politică. Un administrator poate utiliza Kaspersky Security Center pentru a vizualiza, adăuga, edita sau șterge elemente de listă din proprietățile computerului.

   În cazul în care caseta de selectare este debifată, utilizatorul poate accesa doar lista generală a excluderilor generate în politică. De asemenea, dacă această casetă de selectare este debifată, Kaspersky Endpoint Security ascunde lista consolidată a excluderilor de la scanare în interfața de utilizator a aplicației.

8. Faceți clic pe **Add** și selectați o acțiune:

   - **Category**. Puteți grupa excluderile de la scanare în categorii separate. Pentru a crea o categorie nouă, introduceți numele categoriei și adăugați cel puțin o excludere de la scanare la categorie.
   - **New exclusion**. Kaspersky Endpoint Security adaugă o nouă excludere de la scanare la rădăcina listei.
   - **Select exclusion from list**. Pentru a configura rapid Kaspersky Endpoint Security pe serverele SQL, serverele Microsoft Exchange și System Center Configuration Manager, aplicația include *excluderi de la scanare predefinite*. De asemenea, au fost adăugate excluderi de la scanare predefinite pentru a sprijini configurarea aplicațiilor în mediile virtuale Citrix și VMware. Trebuie să selectați excluderile de la scanare predefinite, în funcție de scopul serverului protejat.

9. Selectați modul în care doriți să adăugați excluderea **Path to the file or folder**.

10. Introdu calea către directorul partajat.

    De asemenea, puteți introduce calea manual. Kaspersky Endpoint Security acceptă caracterele `*` și `?` la introducerea unei măști:

    - Caracterul `*` (asterisc) ține locul oricărui set de caractere, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\*\*.txt` va include toate căile către fișierele cu extensia TXT din directoarele de pe unitatea C:, dar nu și din subdirectoare.
    - Două caractere `*` consecutive țin locul oricărui set de caractere (inclusiv un set gol) din numele de fișier sau director, inclusiv caracterele `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\**\*.txt` va include toate căile către fișierele cu extensia TXT localizată în directoarele imbricate în `Folder`, cu excepția `Folder` în sine. Masca trebuie să includă cel puțin un nivel de imbricare. Masca `C:\**\*.txt` nu este o mască validă.
    - `?` (semn de întrebare) ține locul oricărui caracter individual, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\???.txt` va include căi pentru toate fișierele din directorul denumit `Folder` care au extensia TXT și un nume format din trei caractere.

    Puteți utiliza măști la începutul, la mijlocul sau la sfârșitul căii fișierului. De exemplu, dacă doriți să adăugați un director pentru toți utilizatorii la excluderi, introduceți masca `C:\Users\*\Folder\`.

11. În blocul **Apply exclusion to**, selectați componenta **Behavior Detection**.

12. Dacă este necesar, în câmpul **Comment**, introdu o descriere succintă a excluderii de la scanare pe care o creezi.

13. Selectați starea **Add to exclusions** pentru excludere.

    Puteți utiliza comutatorul pentru a stop an exclusion în orice moment.

14. Salvați-vă modificările.

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Setări generale** → **Excluderi și tipuri de obiecte**.
4. În blocul **Excluderi de la scanare și aplicații de încredere** → **Excluderi de la scanare**, fă clic pe butonul **Setări**.

   Acest lucru va deschide o fereastră care conține lista excluderilor.
5. Bifați caseta de selectare **Îmbină valorile în momentul moștenirii** dacă doriți să creați o listă consolidată a excluderilor pentru toate computerele companiei. Listele excluderilor din politicile principale și secundare vor fi îmbinate. Listele vor fi îmbinate dacă funcția de îmbinare a valorilor în momentul moștenirii este activată. Excluderile de la din politica principală sunt afișate în politicile secundare într-o vizualizare numai citire. Nu este posibilă modificarea sau ștergerea excluderilor din politica principală.
6. Bifați caseta de selectare **Permite utilizarea excluderilor locale** dacă doriți să permiteți utilizatorului să creeze o listă locală de excluderi. În acest fel, un utilizator își poate crea propria listă locală de excluderi pe lângă lista generală de excluderi generate în politică. Un administrator poate utiliza Kaspersky Security Center pentru a vizualiza, adăuga, edita sau șterge elemente de listă din proprietățile computerului.

   În cazul în care caseta de selectare este debifată, utilizatorul poate accesa doar lista generală a excluderilor generate în politică. De asemenea, dacă această casetă de selectare este debifată, Kaspersky Endpoint Security ascunde lista consolidată a excluderilor de la scanare în interfața de utilizator a aplicației.
7. Faceți clic pe **Adaugă** și selectați o acțiune:

   - **Categorie**. Puteți grupa excluderile de la scanare în categorii separate. Pentru a crea o categorie nouă, introduceți numele categoriei și adăugați cel puțin o excludere de la scanare la categorie.
   - **Excludere nouă**. Kaspersky Endpoint Security adaugă o nouă excludere de la scanare la rădăcina listei.
   - **Selectează excluderea din listă**. Pentru a configura rapid Kaspersky Endpoint Security pe serverele SQL, serverele Microsoft Exchange și System Center Configuration Manager, aplicația include *excluderi de la scanare predefinite*. De asemenea, au fost adăugate excluderi de la scanare predefinite pentru a sprijini configurarea aplicațiilor în mediile virtuale Citrix și VMware. Trebuie să selectați excluderile de la scanare predefinite, în funcție de scopul serverului protejat.
8. Fă clic pe **Adaugă**.
9. În blocul **Proprietăți**, bifați caseta de selectare **Fișier sau director**.
10. Fă clic pe linkul **Selectează fișier sau director** din blocul **Descriere excludere de la scanare (fă clic pe elementele subliniate pentru a le edita)** pentru a deschide fereastra **Nume al fișierului sau al directorului**.
11. Faceți clic pe **Răsfoiește** și selectați directorul partajat.

De asemenea, puteți introduce calea manual. Kaspersky Endpoint Security acceptă caracterele `*` și `?` la introducerea unei măști:

- Caracterul `*` (asterisc) ține locul oricărui set de caractere, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\*\*.txt` va include toate căile către fișierele cu extensia TXT din directoarele de pe unitatea C:, dar nu și din subdirectoare.

- Două caractere `*` consecutive țin locul oricărui set de caractere (inclusiv un set gol) din numele de fișier sau director, inclusiv caracterele `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\**\*.txt` va include toate căile către fișierele cu extensia TXT localizată în directoarele imbricate în `Folder`, cu excepția `Folder` în sine. Masca trebuie să includă cel puțin un nivel de imbricare. Masca `C:\**\*.txt` nu este o mască validă.

- `?` (semn de întrebare) ține locul oricărui caracter individual, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\???.txt` va include căi pentru toate fișierele din directorul denumit `Folder` care au extensia TXT și un nume format din trei caractere.

Puteți utiliza măști la începutul, la mijlocul sau la sfârșitul căii fișierului. De exemplu, dacă doriți să adăugați un director pentru toți utilizatorii la excluderi, introduceți masca `?:\Users\*\Folder\`.

12. Dacă este necesar, în câmpul **Comentariu**, introdu o descriere succintă a excluderii de la scanare pe care o creezi.

13. Fă clic pe linkul din blocul **Descriere excludere de la scanare (fă clic pe elementele subliniate pentru a le edita)** pentru a deschide fereastra **Componente de protecție**.

14. Bifează caseta de selectare de lângă componenta **Behavior Detection**.

15. Salvați-vă modificările.

Adăugarea de computere de încredere pentru criptarea datelor externe

Dacă organizația ta utilizează criptarea datelor externe în fluxul său de lucru pentru schimbul de fișiere, trebuie să creezi o listă de computere de încredere. Kaspersky Endpoint Security nu monitorizează criptarea datelor de către computerele de încredere.

Serviciul Audit Logon trebuie să fie activat pentru a permite excluderile adreselor de la protecția directoarelor partajate împotriva criptării externe. Serviciul Audit Logon este dezactivat în mod implicit (pentru informații detaliate despre activarea serviciului Audit Logon, vizitează site-ul web Microsoft).

Funcționalitatea de excludere a adreselor de la protecția directoarelor partajate nu se aplică pe un computer aflat la distanță dacă respectivul computer a fost pornit înainte de a porni Kaspersky Endpoint Security. Poți reporni computerul aflat la distanță după ce pornește Kaspersky Endpoint Security ca să te asiguri că funcționalitatea de excludere a adreselor de la protecția directoarelor partajate se aplică pe computerul aflat la distanță.

Modificarea listei de computere de încredere poate fi blocată de proprietățile politicii principale. Pentru a modifica lista, trebuie să permiteți modificarea setărilor zonei de încredere în Web Console („lacătul" trebuie să fie deblocat).

Zonele de încredere sunt grupate diferit în Consola de administrare (MMC) și în Web Console. De asemenea, modul în care se împiedică modificarea parametrilor zonei de încredere este diferit („lacăte" diferite). Vă recomandăm să utilizați exclusiv Web Console pentru gestionarea aplicației. În cazul în care configurați zona de încredere pe console diferite, este posibil ca plug-inul de gestionare să reseteze „lacătul" la starea implicită.

Cum se adaugă un computer de încredere pentru criptarea datelor externe în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Advanced Threat Protection** → **Anti-Cryptor**.
4. În blocul **Excluderi de la scanare**, fă clic pe butonul **După nume sau adresă IP**.
5. În fereastra care se deschide, faceți clic pe butonul **După nume sau adresă IP**.
6. Introdu adresa IP, intervalul de adrese IP sau numele computerelor de la care nu trebuie gestionate încercările de criptare externă.

   Exemple:

   - `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. Salvați-vă modificările.

Cum se adaugă un computer de încredere pentru criptarea datelor externe în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Host Threat Protection** → **Behavior Analysis** → **Anti-Cryptor**.
5. În partea superioară a ferestrei, fă clic pe linkul **Exclusions by name or IP address**.
6. În fereastra care se deschide, faceți clic pe butonul **Add**.
7. Introdu adresa IP, intervalul de adrese IP sau numele computerelor de la care nu trebuie gestionate încercările de criptare externă.

   Exemple:

   - `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. Salvați-vă modificările.

Cum se adaugă un computer de încredere pentru criptarea datelor externe în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Advanced Threat Protection** → **Anti-Cryptor**.
3. În partea superioară a ferestrei, fă clic pe linkul **Excluderi după nume sau adresă IP**.
4. În fereastra care se deschide, faceți clic pe butonul **Adaugă**.
5. Introdu adresa IP, intervalul de adrese IP sau numele computerelor de la care nu trebuie gestionate încercările de criptare externă.

Exemple:

- `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. Salvați-vă modificările.

Exportarea și importarea unei liste de excluderi de la protecția directoarelor partajate împotriva criptării externe

Poți exporta lista de excluderi într-un fișier XML. Apoi puteți modifica fișierul pentru a adăuga, de exemplu, un număr mare de adrese de același tip. De asemenea, puteți utiliza funcția de export/import pentru a face o copie de rezervă a listei de excluderi sau pentru a migra lista pe un alt server.

Cum se exportă și se importă o listă de excluderi în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Advanced Threat Protection** → **Anti-Cryptor**.
4. În blocul **Excluderi de la scanare**, fă clic pe butonul **După nume sau adresă IP**.
5. Pentru a exporta lista de reguli:
   a. Selectați excluderile pe care doriți să le exportați. Pentru a selecta mai multe porturi, utilizați tastele **CTRL** sau **SHIFT**.
      Dacă nu ați selectat nicio excludere, Kaspersky Endpoint Security va exporta toate excluderile.
   b. Fă clic pe butonul → **Exportă**.
   c. În fereastra care se deschide, specificați numele fișierului XML în care doriți să exporți lista de excluderi și selectați directorul în care doriți să salvați acest fișier.
   d. Salvați fișierul.
      Kaspersky Endpoint Security exportă întreaga listă de excluderi în fișierul XML.
6. Pentru a importa lista de excluderi:
   a. Fă clic pe butonul → **Importă**.
   b. În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de excluderi.

c. Deschideți fișierul.

În cazul în care computerul are deja o listă de excluderi, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul XML.

7. Salvați-vă modificările.

Cum se exportă și se importă o listă de excluderi în Consola Web și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Host Threat Protection** → **Behavior Analysis** → **Anti-Cryptor**.
5. Faceți clic pe linkul **Exclusions by name or IP address**.
6. Pentru a exporta lista de reguli:

   a. Selectați excluderile pe care doriți să le exportați.

   b. Fă clic pe butonul → **Export**.

   Kaspersky Endpoint Security exportă lista de excluderi într-un fișier JSON în directorul pentru descărcări implicit.
7. Pentru a importa lista de excluderi:

   a. Fă clic pe butonul → **Import**.

   În fereastra care se deschide, selectați fișierul JSON din care doriți să importați lista de excluderi.

   b. Deschideți fișierul.

   În cazul în care computerul are deja o listă de excluderi, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul JSON.
8. Salvați-vă modificările.

Remediation Engine

Componenta Remediation Engine permite Kaspersky Endpoint Security să deruleze înapoi acțiuni care au fost executate de către programe malware în sistemul de operare.

Atunci când se derulează înapoi activitatea programelor malware în sistemul de operare, Kaspersky Endpoint Security tratează următoarele tipuri de activități ale programelor malware:

- **Activitate cu fișiere**

Kaspersky Endpoint Security efectuează următoarele acțiuni:

- Șterge fișierele executabile create de malware (pe toate suporturile, cu excepția unităților de rețea).
- Șterge fișierele executabile create de programe infiltrate de malware.
- Restaurează fișierele modificate sau șterse de malware.

Caracteristica de recuperare a fișierelor are un număr de limitări.

- **Activitate de registry**

  Kaspersky Endpoint Security efectuează următoarele acțiuni:

  - Șterge cheile de registru create de malware.
  - Nu restaurează cheile de registru modificate sau șterse de malware.

- **Activitate de sistem**

  Kaspersky Endpoint Security efectuează următoarele acțiuni:

  - Termină procesele care au fost inițiate de malware.
  - Termină procesele în care a pătruns o aplicație rău intenționată.
  - Nu reia procesele care au fost oprite de malware.

- **Activitate în rețea**

  Kaspersky Endpoint Security efectuează următoarele acțiuni:

  - Blochează activitatea de rețea a programelor malware.
  - Blochează activitatea de rețea a proceselor care au fost infiltrate de malware.

O derulare înapoi a acțiunilor unui malware poate fi pornită de componenta File Threat Protection sau Behavior Detection sau în cursul unei scanări malware.

Derularea înapoi a operațiunilor programelor malware afectează un set de date strict definit. Restaurarea nu are efecte adverse asupra sistemului de operare sau asupra integrității datelor computerului tău.

Cum se activează sau dezactivează componenta Remediation Engine în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Advanced Threat Protection** → **Remediation Engine**.
4. Utilizează caseta de selectare **Remediation Engine** pentru a activa sau a dezactiva componenta.
5. Salvați-vă modificările.

Cum se activează sau dezactivează componenta Remediation Engine în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.
   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Host Threat Protection** → **Behavior Analysis** → **Remediation Engine**.
5. Utilizați comutatorul **Remediation Engine ENABLED** pentru a activa sau a dezactiva componenta.
6. Salvați-vă modificările.

Cum se activează sau dezactivează componenta Remediation Engine în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul .
2. În fereastra cu setările aplicației, selectați **Advanced Threat Protection** → **Remediation Engine**.
3. Utilizați comutatorul **Remediation Engine** pentru a activa sau a dezactiva componenta.
4. Salvați-vă modificările.

Prin urmare, dacă Remediation Engine este activat, Kaspersky Endpoint Security va derula înapoi acțiunile întreprinse de aplicațiile dăunătoare din sistemul de operare.

Kaspersky Security Network

Pentru a-ți proteja mai eficient computerul, Kaspersky Endpoint Security folosește informații primite de la utilizatori de pe întregul glob. Kaspersky Security Network este conceput pentru a obține aceste date.

Este posibil ca funcționalitatea KSN să nu fie disponibilă în software în SUA.

Kaspersky Security Network (KSN) este o infrastructură de servicii în cloud care oferă acces la Baza de cunoștințe online Kaspersky, care conține informații despre reputația fișierelor, a resurselor Web și a programelor software. Utilizarea datelor de la Kaspersky Security Network asigură răspunsul mai rapid prin Kaspersky Endpoint Security la noile amenințări, îmbunătățește eficiența unor componente ale protecției și reduce posibilitatea alarmelor false. Dacă participați la Kaspersky Security Network, serviciile KSN furnizează componentei Kaspersky Endpoint Security informații despre reputația adreselor web scanate, precum și informații despre categoria și reputația fișierelor scanate. Pentru mai multe detalii despre configurarea accesului la KSN, consultă Ajutor pentru Kaspersky Security Center.

Utilizarea Kaspersky Security Network este facultativă. Aplicația îți solicită să utilizezi KSN în cursul configurării inițiale a aplicației. Utilizatorii pot începe sau pot întrerupe participarea la KSN în orice moment.

Pentru informații mai detaliate despre trimiterea informațiilor statistice Kaspersky generate în cursul participării la KSN și despre stocarea și distrugerea acestor informații, consultați Kaspersky Security Network Statement și site-ul Web Kaspersky. Fișierul ksn_<ID limbă>.txt care conține textul Declarației Kaspersky Security Network este inclus în kitul de distribuție al aplicației.

Infrastructura bazelor de date Kaspersky privind reputația

Kaspersky Endpoint Security acceptă următoarele soluții de infrastructură pentru lucrul cu bazele de date Kaspersky privind reputația:

- *Kaspersky Security Network (KSN)* este soluția folosită de majoritatea aplicațiilor Kaspersky. Participanții KSN primesc informații de la Kaspersky Security Network și trimit către Kaspersky informații despre obiecte detectate pe computerul utilizatorului, pentru a fi analizate suplimentar de analiștii Kaspersky și pentru a fi incluse în bazele de date privind reputația și în cele statistice.
- *Kaspersky Private Security Network (KPSN)* este o soluție care permite utilizatorilor de computere care găzduiesc Kaspersky Endpoint Security sau alte aplicații Kaspersky să obțină acces la bazele de date privind reputația ale Kaspersky și la alte date statistice, fără a trimite date către Kaspersky de la propriile lor computere. KPSN este conceput pentru clienții corporativi care nu pot participa la Kaspersky Security Network din oricare dintre următoarele motive:
  - Stațiile de lucru locale nu sunt conectate la Internet.
  - Transmiterea oricăror date în afara țării sau în afara rețelei locale corporative este interzisă prin lege sau restricționată de politicile de securitate corporativă.

Activarea și dezactivarea utilizării Kaspersky Security Network

În mod implicit, Kaspersky Endpoint Security utilizează modul KSN extins. *Mod KSN extins* este un mod în care Kaspersky Endpoint Security trimite date suplimentare către Kaspersky.

Cum se activează sau dezactivează componenta Utilizare KSN în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Advanced Threat Protection** → **Kaspersky Security Network**.
4. Utilizați comutatorul **Kaspersky Security Network** pentru a activa sau a dezactiva componenta.

   Dacă ați activat utilizarea KSN, Kaspersky Endpoint Security va afișa Declarația Kaspersky Security Network. Vă rugăm să citiți și să acceptați condițiile de utilizare ale Declarației Kaspersky Security Network (KSN) dacă sunteți de acord cu acestea.
5. Dacă este necesar, debifați caseta de selectare **Activează modul KSN extins**. În mod implicit, modul extins KSN este activat.
6. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se activează sau dezactivează componenta Utilizare KSN în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **General Settings** → **Kaspersky Security Network**.
5. Utilizați comutatorul **Use of Kaspersky Security Network (KSN) ENABLED** pentru a activa sau a dezactiva componenta.

   Dacă ați activat utilizarea KSN, Kaspersky Endpoint Security va afișa Declarația Kaspersky Security Network. Vă rugăm să citiți și să acceptați condițiile de utilizare ale Declarației Kaspersky Security Network (KSN) dacă sunteți de acord cu acestea.
6. Dacă este necesar, dezactivați comutatorul **Use extended KSN mode**. În mod implicit, modul extins KSN este activat.
7. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se activează sau dezactivează componenta Utilizare KSN în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul .
2. În fereastra cu setările aplicației, selectați **Advanced Threat Protection** → **Kaspersky Security Network**.
3. Utilizați comutatorul **Kaspersky Security Network** pentru a activa sau a dezactiva componenta.

   Dacă ați activat utilizarea KSN, Kaspersky Endpoint Security va afișa Declarația Kaspersky Security Network. Vă rugăm să citiți și să acceptați condițiile de utilizare ale Declarației Kaspersky Security Network (KSN) dacă sunteți de acord cu acestea.
4. Dacă este necesar, dezactivați comutatorul **Activează modul KSN extins**. În mod implicit, modul extins KSN este activat.
5. Salvați-vă modificările.

Ca urmare, dacă utilizarea KSN este activată, Kaspersky Endpoint Security folosește informații despre reputația fișierelor, resurselor web și aplicațiilor primite de la Kaspersky Security Network.

Limitări ale Kaspersky Private Security Network

Kaspersky Private Security Network (KPSN) este o soluție care permite utilizatorilor de computere care găzduiesc Kaspersky Endpoint Security sau alte aplicații Kaspersky să obțină acces la bazele de date privind reputația ale Kaspersky și la alte date statistice, fără a trimite date către Kaspersky de la propriile lor computere. Kaspersky Private Security Network vă permite să utilizați propria bază de date locală privind reputația pentru a verifica reputația obiectelor (fișiere sau adrese URL). Reputația unui obiect adăugat la baza de date locală de reputație are o prioritate mai mare decât una adăugată la KSN/KPSN. De exemplu, imaginați-vă că Kaspersky Endpoint Security scanează un computer și solicită reputația unui fișier în KSN/KPSN. Dacă fișierul are o reputație *Nu este de încredere* în baza de date locală de reputație, dar are o reputație *De încredere* în KSN/KPSN, Kaspersky Endpoint Security va detecta fișierul ca fiind *Nu este de încredere* și va întreprinde acțiunea definită pentru amenințările detectate.

Cu toate acestea, în unele cazuri, Kaspersky Endpoint Security ar putea să nu solicite reputația unui obiect în KSN/KPSN. În acest caz, Kaspersky Endpoint Security nu va primi date din baza de date locală a reputației a KPSN. Este posibil ca Kaspersky Endpoint Security să nu solicite reputația unui obiect în KSN/KPSN din următoarele motive:

- Aplicațiile Kaspersky utilizează baze de date de reputație offline. Bazele de date de reputație offline sunt concepute pentru a optimiza resursele în timpul funcționării aplicațiilor Kaspersky și pentru a proteja obiectele importante de pe computer. Bazele de date de reputație offline sunt create de experți Kaspersky pe baza datelor din Kaspersky Security Network. Aplicațiile Kaspersky actualizează bazele de date de reputație offline cu baze de date antivirus ale aplicației respective. Dacă bazele de date de reputație offline conțin informații despre un obiect scanat, aplicația nu solicită reputația acestui obiect de la KSN/KPSN.

- Excluderile de la scanare (zona de încredere) sunt configurate în setările aplicației. În acest caz, aplicația nu ia în considerare reputația obiectului din baza de date locală de reputație.

- Aplicația utilizează tehnologii de optimizare a scanării, cum ar fi iSwift sau iChecker, sau memorează în cache cererile de reputație în KSN/KPSN. În acest caz, este posibil ca aplicația să nu solicite reputația obiectelor scanate anterior.

- Pentru a-și optimiza volumul de lucru, aplicația scanează fișiere cu un anumit format și dimensiune. Lista formatelor relevante și a limitelor de dimensiune sunt stabilite de experții Kaspersky. Această listă este actualizată cu bazele de date antivirus ale aplicației. De asemenea, puteți configura setările de optimizare a scanării în interfața aplicației, de exemplu, pentru componenta File Threat Protection.

- Kaspersky Endpoint Security în modul Light Agent comunică cu serverele KSN printr-un server proxy KSN. Comunicarea directă cu KSN nu este acceptată.

Activarea și dezactivarea modului cloud pentru componentele de protecție

Mod cloud se referă la modul de operare al aplicației în care Kaspersky Endpoint Security utilizează o versiune light a bazelor de date antivirus. Kaspersky Security Network acceptă funcționarea aplicației atunci când sunt utilizate baze de date antivirus light. Versiunea light a bazelor de date antivirus vă permite să utilizați aproximativ jumătate din memoria RAM a computerului care ar fi, altfel, utilizată cu bazele de date obișnuite. Dacă nu participați la Kaspersky Security Network sau dacă modul cloud este dezactivat, Kaspersky Endpoint Security descarcă versiunea completă a bazelor de date antivirus de pe serverele Kaspersky.

Când folosești Kaspersky Private Security Network, funcționalitatea modului cloud este disponibilă începând cu Kaspersky Private Security Network versiunea 3.0.

Dacă aplicația funcționează în modul Light Agent, modul Cloud nu este disponibil.

Cum se activează sau dezactivează modul cloud pentru componentele de protecție în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.

2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

3. În fereastra politicii, selectați **Advanced Threat Protection** → **Kaspersky Security Network**.

4. Utilizează caseta de selectare **Activează modul Cloud** pentru a activa sau a dezactiva componenta.

5. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se activează sau dezactivează modul cloud pentru componentele de protecție în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **General Settings** → **Kaspersky Security Network**.

5. Utilizați comutatorul **Use cloud mode** pentru a activa sau a dezactiva componenta.

6. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se activează sau dezactivează modul cloud pentru componentele de protecție în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul .

2. În fereastra cu setările aplicației, selectați **Advanced Threat Protection** → **Kaspersky Security Network**.

3. Utilizați comutatorul **Activează modul Cloud** pentru a activa sau a dezactiva componenta.

4. Salvați-vă modificările.

Drept urmare, Kaspersky Endpoint Security descarcă o versiune simplă sau o versiune completă a bazelor de date antivirus în următoarea actualizare.

Dacă nu este disponibilă spre utilizare versiunea redusă a bazelor de date antivirus, Kaspersky Endpoint Security trece automat la versiunea premium a bazelor de date antivirus.

Setări proxy KSN

Computerele utilizatorilor gestionate de Serverul de administrare Kaspersky Security Center pot interacționa cu KSN fie direct, fie prin serviciul KSN Proxy.

Dacă aplicația rulează în modul Light Agent, comunicarea directă cu KSN nu este acceptată. Kaspersky Endpoint Security comunică cu serverele KSN printr-un server proxy KSN.

Serviciul KSN Proxy oferă următoarele funcționalități:

- Computerul utilizatorului poate interoga KSN și poate trimite informații către KSN, chiar și fără acces direct la Internet.

- Serviciul KSN Proxy stochează în memoria cache datele procesate, reducând astfel încărcarea asupra canalului de comunicare în rețeaua externă și accelerând recepția informațiilor solicitate de computerul utilizatorului.

În mod implicit, după ce KSN este activat și Declarația KSN este acceptată, aplicația folosește un server proxy pentru a se conecta la Kaspersky Security Network. Serverul proxy utilizat de aplicație este Kaspersky Security Center Administration Server prin portul TCP 13111. Prin urmare, dacă Proxy KSN nu este disponibil, trebuie să verificați următoarele:

- Serviciul `ksnproxy` se execută pe Serverul de administrare.
- Firewall-ul de pe computer nu blochează portul 13111.

Puteți configura utilizarea KSN Proxy după cum urmează: activați sau dezactivați KSN Proxy și configurați portul pentru conexiune. Pentru a face acest lucru, trebuie să deschideți proprietățile Serverului de administrare. Pentru mai multe detalii despre configurarea componentei KSN Proxy, consultați Ajutor pentru Kaspersky Security Center. De asemenea, puteți activa sau dezactiva KSN Proxy pentru computere individuale în politica Kaspersky Endpoint Security.

Cum se activează sau dezactivează componenta Proxy KSN în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Advanced Threat Protection → Kaspersky Security Network**.
4. În blocul **Setări proxy KSN**, utilizați caseta de selectare **Utilizează Serverul de administrare ca server proxy KSN** pentru a activa sau dezactiva KSN Proxy.
5. Dacă este necesar, bifați caseta de selectare **Utilizează serverele Kaspersky Security Network dacă serverul proxy KSN este indisponibil**.

   În cazul în care caseta de selectare este bifată, Kaspersky Endpoint Security folosește servere KSN atunci când serviciul KSN Proxy este indisponibil. Serverele KSN pot fi localizate atât la Kaspersky, cât și la terți (atunci când se folosește Kaspersky Private Security Network).
6. Salvați-vă modificările.

Cum se activează sau dezactivează componenta Proxy KSN în Web Console

1. În fereastra principală a Web Console, selectați **Asset management → Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **General Settings → Kaspersky Security Network**.
5. Utilizați caseta de selectare **Use Administration Server as a KSN proxy server** pentru a activa sau a dezactiva KSN Proxy.
6. Dacă este necesar, bifați caseta de selectare **Use Kaspersky Security Network servers if the KSN proxy server is unavailable**.

   În cazul în care caseta de selectare este bifată, Kaspersky Endpoint Security folosește servere KSN atunci când serviciul KSN Proxy este indisponibil. Serverele KSN pot fi localizate atât la Kaspersky, cât și la terți (atunci când se folosește Kaspersky Private Security Network). În mod implicit, caseta de selectare este debifată.
7. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Adresa KSN Proxy se potrivește cu adresa Serverului de administrare. Când numele de domeniu al Serverului de administrare este schimbat, trebuie să actualizați manual adresa componentei KSN Proxy.

Pentru a configura adresa Proxy KSN:

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectează directorul **Advanced** → **Remote installation** → **Installation packages**.
3. În meniul contextual al directorului **Installation packages**, selectați **Properties**.
4. În fila **General** din fereastra deschisă, specificați noua adresă a serverului Proxy KSN.
5. Salvați-vă modificările.

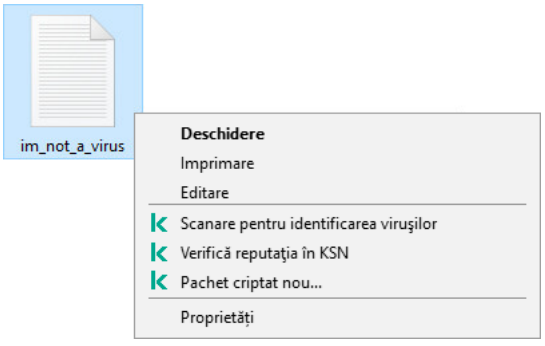
Verificarea reputației unui fișier în Kaspersky Security Network

Dacă aveți îndoieli cu privire la securitatea unui fișier, puteți verifica reputația acestuia în Kaspersky Security Network.

Puteți verifica reputația unui fișier dacă ați acceptat termenii din Kaspersky Security Network Statement.

Pentru a verifica reputația unui fișier în Kaspersky Security Network:

Deschideți meniul contextual al fișierului și selectați opțiunea **Verificare reputație în KSN** (consultați figura de mai jos).



Meniu contextual fișier

Kaspersky Endpoint Security afișează reputația fișierului:

De încredere (Kaspersky Security Network). Aplicația consideră un fișier de încredere dacă sunt îndeplinite una sau mai multe dintre următoarele condiții:

- fișierul este semnat digital de un furnizor de încredere;
- fișierul are o reputație de încredere în Kaspersky Security Network;
- utilizatorul a plasat aplicația în grupul De încredere.

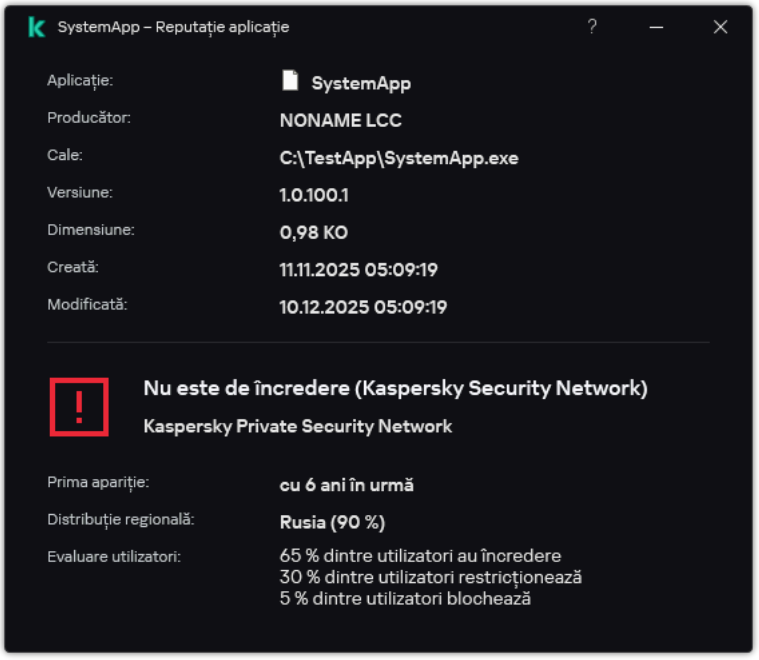
Software legitim care poate fi utilizat de intruși pentru a aduce daune computerului sau datelor personale Cu toate că nu au funcții rău intenționate, astfel de aplicații pot fi exploatate de intruși. Pentru detalii despre software-urile legale care pot fi folosite de infractori pentru a prejudicia computerul sau datele cu caracter personal ale unui utilizator, vizitați site-ul web Enciclopedia IT Kaspersky. Puteți adăuga aceste aplicații la lista de încredere.

Nu este de încredere (Kaspersky Security Network). Un virus sau o altă aplicație care reprezintă o amenințare.

Necunoscută (Kaspersky Security Network). Kaspersky Security Network nu are informații despre fișier. Puteți scana un fișier utilizând bazele de date antivirus (opțiunea **Scanează de viruși** din meniul contextual).

Kaspersky Endpoint Security afișează soluția KSN care a fost utilizată pentru a determina reputația fișierului: *Kaspersky Security Network* sau *Kaspersky Private Security Network*.

Kaspersky Endpoint Security afișează, de asemenea, informații suplimentare despre fișier (consultați figura de mai jos).



Reputația unui fișier în Kaspersky Security Network

Scanare conexiuni criptate

După instalare, Kaspersky Endpoint Security adaugă certificatul Kaspersky la stocarea de sistem a certificatelor de încredere (depozitul de certificate Windows). Kaspersky Endpoint Security utilizează acest certificat pentru a scana conexiunile criptate. Kaspersky Endpoint Security include și utilizarea stocării de sistem a certificatelor de încredere în Firefox și Thunderbird pentru a scana traficul acestor aplicații.

Componentele Control Web, Mail Threat Protection, Web Threat Protection, Behavior Detection și Exploit Prevention pot decripta și scana traficul de rețea transmis prin conexiuni criptate care folosesc următoarele protocoale:

- SSL 3.0.
- TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.

Activarea scanării conexiunii criptate

În mod implicit, Kaspersky Endpoint Security nu scanează întotdeauna conexiunile criptate, ci numai atunci când sunt solicitate de componentele de protecție.

Cum se activează scanarea conexiunilor criptate în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați **Policies**.
3. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
4. În fereastra politicii, selectați **Setări generale** → **Setări rețea**.
5. În blocul **Scanare conexiuni criptate**, selectați modul de scanare a conexiunii criptate:
   - **Scanează conexiunile criptate**. Kaspersky Endpoint Security nu va avea acces la conținutul site-urilor web ale căror adrese încep cu `https://`.
   - **Scanează conexiunile criptate la cererea componentelor de protecție**. Kaspersky Endpoint Security va scana traficul criptat numai la solicitarea componentelor Web Threat Protection, Mail Threat Protection și Control Web.
   - **Scanează întotdeauna conexiunile criptate**. Kaspersky Endpoint Security va scana traficul de rețea criptat chiar dacă componentele de protecție sunt dezactivate.

   Kaspersky Endpoint Security nu scanează conexiunile criptate care au fost stabilite de aplicații de încredere pentru care scanarea traficului este dezactivată. Kaspersky Endpoint Security nu scanează conexiunile criptate din lista predefinită de site-uri web de încredere. Lista predefinită de site-uri web de încredere este creată de experții Kaspersky. Această listă este actualizată cu bazele de date antivirus ale aplicației. Puteți vizualiza lista predefinită de site-uri web de încredere numai în interfața Kaspersky Endpoint Security. Nu puteți vizualiza lista în consola Kaspersky Security Center.
6. Dacă este necesar, adăugați excluderi de la scanare: adrese și aplicații de încredere.
7. Configurați setările pentru scanarea conexiunilor criptate (consultați tabelul de mai jos).
8. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se activează scanarea conexiunilor criptate în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați fila **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **General Settings** → **Network Settings**.
5. În **Encrypted Connections Scan**, activează comutatorul **Encrypted Connections Scan ENABLED**.

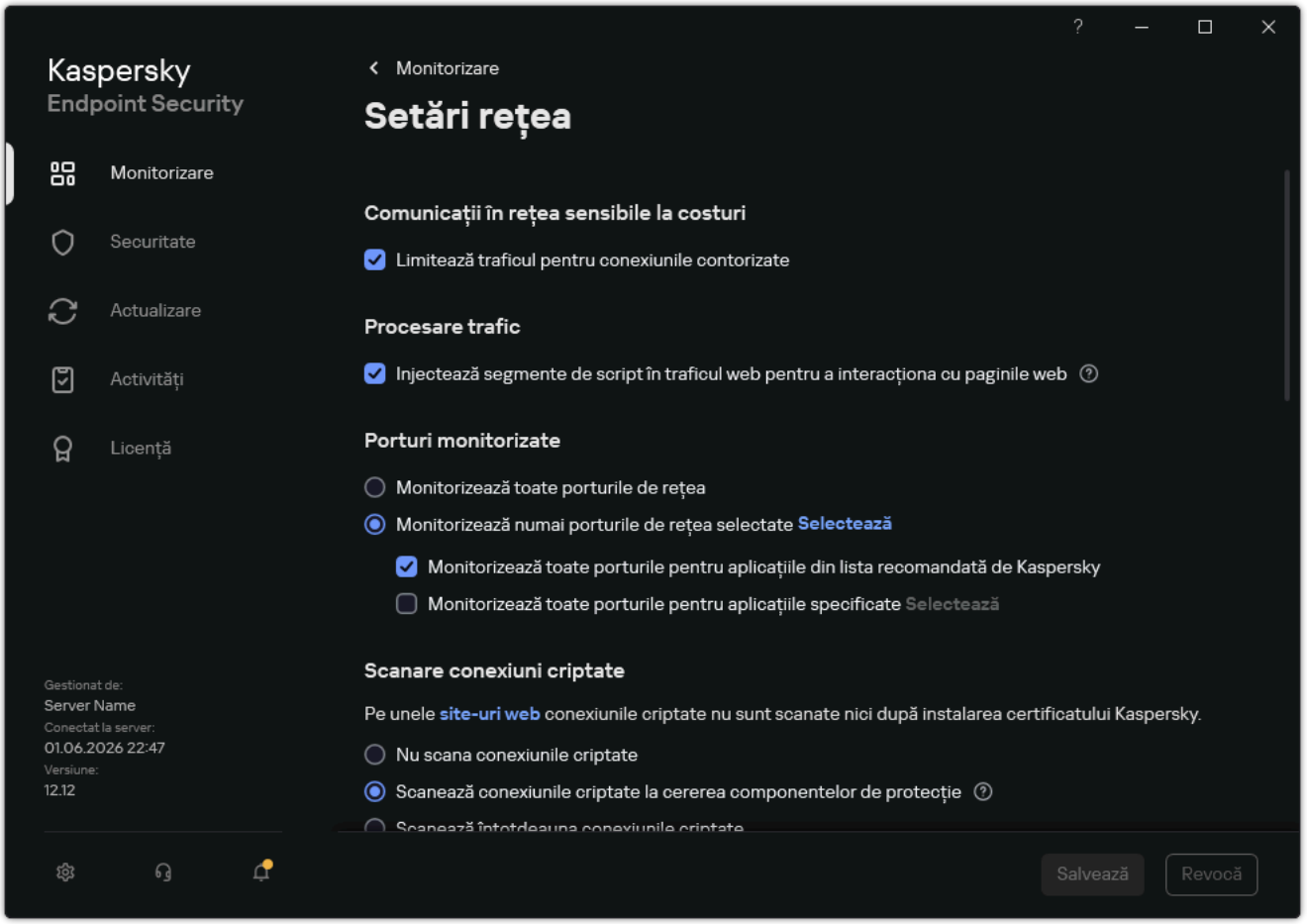
   În cazul în care comutatorul este dezactivat, Kaspersky Endpoint Security nu va avea acces la conținutul site-urilor web ale căror adrese încep cu `https://`.
6. Fă clic pe **Settings** și selectează modul de scanare a conexiunii criptate:

   - **Scan encrypted connections upon request from protection components**. Kaspersky Endpoint Security va scana traficul criptat numai la solicitarea componentelor Web Threat Protection, Mail Threat Protection și Control Web.
   - **Always scan encrypted connections**. Kaspersky Endpoint Security va scana traficul de rețea criptat chiar dacă componentele de protecție sunt dezactivate.

   > Kaspersky Endpoint Security nu scanează conexiunile criptate care au fost stabilite de aplicații de încredere pentru care scanarea traficului este dezactivată. Kaspersky Endpoint Security nu scanează conexiunile criptate din lista predefinită de site-uri web de încredere. Lista predefinită de site-uri web de încredere este creată de experții Kaspersky. Această listă este actualizată cu bazele de date antivirus ale aplicației. Puteți vizualiza lista predefinită de site-uri web de încredere numai în interfața Kaspersky Endpoint Security. Nu puteți vizualiza lista în consola Kaspersky Security Center.
7. Dacă este necesar, adăugați excluderi de la scanare: adrese și aplicații de încredere.
8. Configurați setările pentru scanarea conexiunilor criptate (consultați tabelul de mai jos).
9. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se activează scanarea conexiunilor criptate în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Setări generale** → **Setări rețea**.



Setări scanare conexiuni criptate

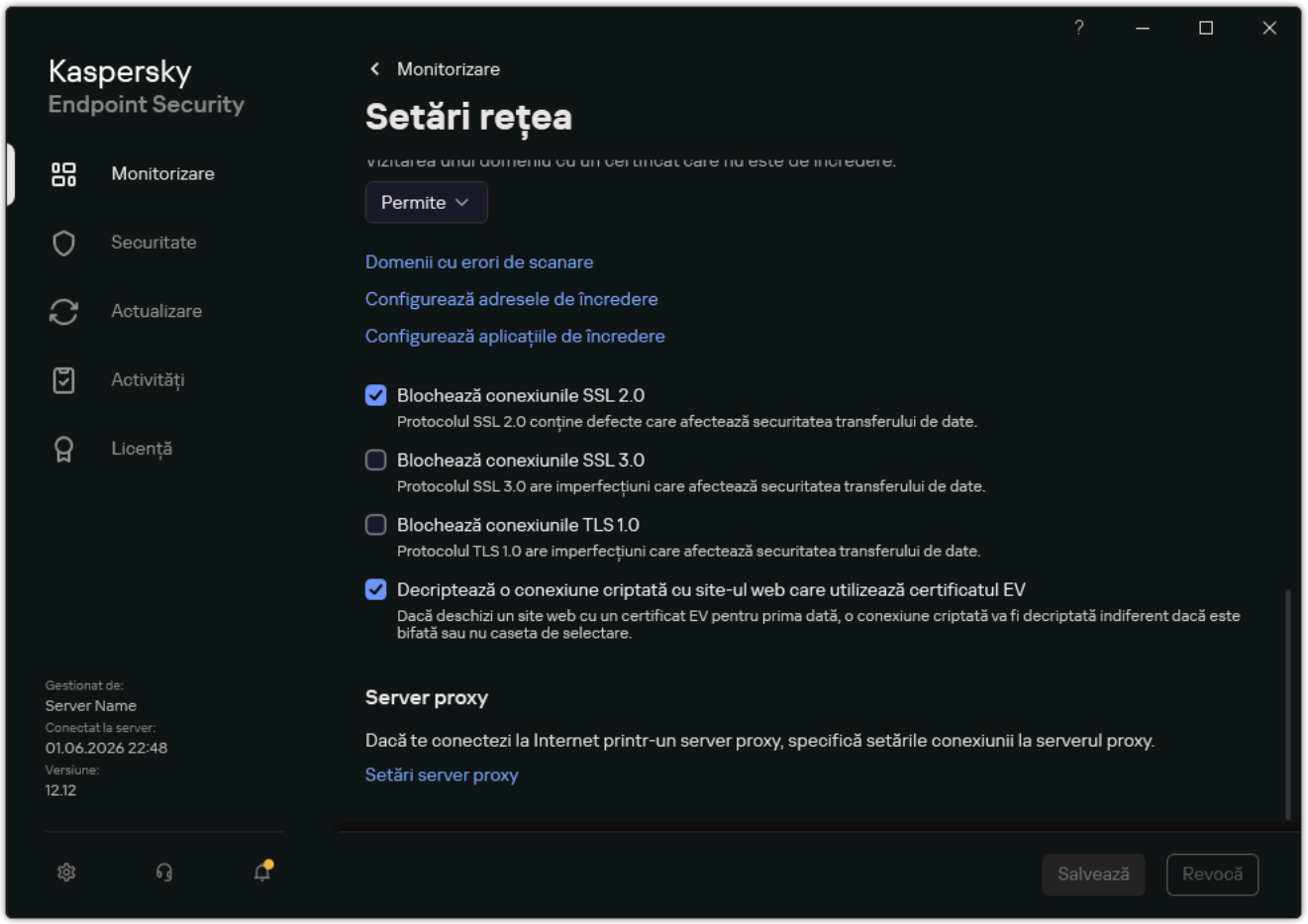
3. În blocul **Scanare conexiuni criptate**, selectați modul de scanare a conexiunii criptate:

   - **Nu scana conexiunile criptate**. Kaspersky Endpoint Security nu va avea acces la conținutul site-urilor web ale căror adrese încep cu `https://`.
   - **Scanează conexiunile criptate la cererea componentelor de protecție**. Kaspersky Endpoint Security va scana traficul criptat numai la solicitarea componentelor Web Threat Protection, Mail Threat Protection și Control Web.
   - **Scanează întotdeauna conexiunile criptate**. Kaspersky Endpoint Security va scana traficul de rețea criptat chiar dacă componentele de protecție sunt dezactivate.

   Kaspersky Endpoint Security nu scanează conexiunile criptate care au fost stabilite de aplicații de încredere pentru care scanarea traficului este dezactivată. Kaspersky Endpoint Security nu scanează conexiunile criptate din lista predefinită de site-uri web de încredere. Lista predefinită de site-uri web de încredere este creată de experții Kaspersky. Această listă este actualizată cu bazele de date antivirus ale aplicației. Puteți vizualiza lista predefinită de site-uri web de încredere numai în interfața Kaspersky Endpoint Security. Nu puteți vizualiza lista în consola Kaspersky Security Center.

4. Dacă este necesar, adăugați excluderi de la scanare: adrese și aplicații de încredere.

5. Configurați setările pentru scanarea conexiunilor criptate (consultați tabelul de mai jos).



Setări suplimentare pentru scanarea conexiunilor criptate

6. Salvați-vă modificările.

Setări scanare conexiuni criptate

Parametru	Descriere
Certificate rădăcină de încredere	Lista cu certificatele rădăcină de încredere. Kaspersky Endpoint Security vă permite să instalați certificate rădăcină de încredere pe computerele utilizatorilor dacă, de exemplu, trebuie să implementați un nou centru de certificare. Aplicația vă permite să adăugați un certificat într-un magazin special de certificate Kaspersky Endpoint Security. În acest caz, certificatul este considerat de încredere numai pentru aplicația Kaspersky Endpoint Security. Cu alte cuvinte, utilizatorul poate obține acces la un site web cu certificatul nou în browser. Dacă aplicația încearcă să obțină acces la site-ul web, poate să apară o eroare de conexiune din cauza unei probleme delate de certificat. Pentru a adăuga la magazinul de certificate de sistem, puteți utiliza politicile de grup Director activ.
Vizitarea unui domeniu cu un certificat care nu este de încredere	• **Permite**. La vizitarea unui domeniu cu un certificat care nu este de încredere, Kaspersky Endpoint Security permite conectarea la rețea. Atunci când se deschide un domeniu cu un certificat neautorizat într-un browser, Kaspersky Endpoint Security afișează o pagină HTML cu un avertisment prin care nu se recomandă vizitarea domeniului respectiv. Un utilizator poate face clic pe linkul din pagina de avertizare HTML pentru a obține accesul la resursa web solicitată. Dacă o aplicație terță sau un serviciu terț stabilește o conexiune cu un domeniu cu un certificat care nu este de încredere, Kaspersky Endpoint Security își creează propriul certificat pentru a scana traficul. Noul certificat are starea *Nu este de încredere*. Acest lucru este necesar pentru a avertiza aplicația terță despre conexiunea care nu este de încredere, deoarece pagina HTML nu poate fi afișată în acest caz și conexiunea poate fi stabilită în modul în fundal. • **Blochează**. La vizitarea unui domeniu cu un certificat care nu este de încredere, Kaspersky Endpoint Security blochează conexiunea la rețea. Atunci când se deschide un domeniu cu un certificat neautorizat într-un browser, Kaspersky Endpoint Security afișează o pagină HTML cu informații privind motivul pentru care domeniul respectiv este blocat.
Vizitarea unui domeniu cu o eroare de scanare a conexiunilor criptate	• **Blochează**. Dacă apare o eroare la scanarea conexiunii criptate, Kaspersky Endpoint Security blochează conexiunea la rețea. • **Permite și adaugă domeniul la excluderi**. Dacă apare o eroare la scanarea conexiunii criptate, Kaspersky Endpoint Security adaugă domeniul care a generat eroarea în lista domeniilor cu erori la scanare și nu monitorizează traficul de rețea criptat atunci când acest domeniu este vizitat. Puteți vizualiza o listă de domenii cu erori de scanare a conexiunilor sigure numai în interfața locală a aplicației. Pentru a șterge conținutul listei, trebuie să selectați **Blochează**. Kaspersky Endpoint Security generează, de asemenea, un eveniment pentru eroarea de scanare a conexiunii criptate.

Parametru	Descriere
Blochează conexiunile SSL 2.0	Dacă această casetă de selectare este bifată, aplicația monitorizează și blochează conexiunile la rețea stabilite prin protocolul SSL 2.0. Dacă caseta de selectare este debifată, aplicația nu blochează conexiunile de rețea stabilite prin protocolul SSL 2.0. Cu toate acestea, aplicația nu monitorizează traficul de rețea prin acest protocol.
Blochează conexiunile SSL 3.0	Dacă această casetă de selectare este bifată, aplicația blochează conexiunile la rețea stabilite prin protocolul SSL 3.0. Dacă caseta de selectare este debifată, aplicația nu blochează conexiunile de rețea stabilite prin protocolul SSL 3.0. Aplicația monitorizează traficul de rețea prin acest protocol. Toate componentele aplicației funcționează fără restricții.
Blochează conexiunile TLS 1.0	Dacă această casetă de selectare este bifată, aplicația blochează conexiunile la rețea stabilite prin protocolul TLS 1.0. Dacă caseta de selectare este debifată, aplicația nu blochează conexiunile de rețea stabilite prin protocolul TLS 1.0. Aplicația monitorizează traficul de rețea prin acest protocol. Toate componentele aplicației funcționează fără restricții.
Decriptează o conexiune criptată cu site-ul web care utilizează certificatul EV	Certificatele EV (Extended Validation Certificate) confirmă autenticitatea site-urilor web și îmbunătățesc securitatea conexiunii. Browserele folosesc o pictogramă cu un lacăt în bara de adrese pentru a indica faptul că un site web are un certificat EV. De asemenea, browserele pot colora complet sau parțial bara de adrese în verde. În cazul în care caseta de selectare este bifată, aplicația decriptează și monitorizează conexiunile criptate cu site-uri web care utilizează un certificat EV. În cazul în care caseta de selectare este debifată, aplicația nu are acces la conținutul traficului HTTPS. Din acest motiv, aplicația monitorizează traficul HTTPS doar pe baza adresei site-ului web, de exemplu, `https://bing.com`. Dacă deschideți pentru prima dată un site web cu certificat EV, conexiunea criptată va fi decriptată indiferent dacă este bifată sau nu caseta de selectare.

Instalarea certificatelor rădăcină de încredere

Kaspersky Endpoint Security vă permite să instalați certificate rădăcină de încredere pe computerele utilizatorilor dacă, de exemplu, trebuie să implementați un nou centru de certificare. Aplicația vă permite să adăugați un certificat într-un magazin special de certificate Kaspersky Endpoint Security. În acest caz, certificatul este considerat de încredere numai pentru aplicația Kaspersky Endpoint Security. Cu alte cuvinte, utilizatorul poate obține acces la un site web cu certificatul nou în browser. Dacă aplicația încearcă să obțină acces la site-ul web, poate să apară o eroare de conexiune din cauza unei probleme delate de certificat. Pentru a adăuga la magazinul de certificate de sistem, puteți utiliza politicile de grup Director activ.

Modificarea listei certificatelor rădăcină de încredere poate fi blocată de proprietățile politicii principale. Pentru a modifica lista, trebuie să permiteți modificarea setărilor zonei de încredere în Web Console („lacătul" trebuie să fie deblocat).

Zonele de încredere sunt grupate diferit în Consola de administrare (MMC) și în Web Console. De asemenea, modul în care se împiedică modificarea parametrilor zonei de încredere este diferit („lacăte" diferite). Vă recomandăm să utilizați exclusiv Web Console pentru gestionarea aplicației. În cazul în care configurați zona de încredere pe console diferite, este posibil ca plug-inul de gestionare să reseteze „lacătul" la starea implicită.

Cum se instalează certificatele rădăcină de încredere în Consola de Administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Setări generale** → **Setări rețea**.
4. În blocul **Certificate rădăcină de încredere**, fă clic pe butonul **Adaugă**.

5. Se deschide o fereastră; în acea fereastră, selectați un certificat rădăcină de încredere.
   Kaspersky Endpoint Security aceptă certificate cu extensii PEM, DER și CRT.
6. Salvați-vă modificările.

Cum se instalează certificatele rădăcină de încredere în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.
   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **General Settings** → **Network Settings**.
5. Faceți clic pe linkul **Trusted root certificates**.
6. Se deschide o fereastră; în acea fereastră, faceți clic pe **Add** și selectați un certificat rădăcină de încredere.
   Kaspersky Endpoint Security aceptă certificate cu extensii PEM, DER și CRT.
7. Salvați-vă modificările.

Cum se instalează certificatele rădăcină de încredere în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul .
2. În fereastra cu setările aplicației, selectați **Setări generale** → **Setări rețea**.
3. În blocul **Scanare conexiuni criptate**, fă clic pe butonul **Afișează certificatele**.
4. Se deschide o fereastră; în acea fereastră, faceți clic pe **Adaugă** și selectați un certificat rădăcină de încredere.
   Kaspersky Endpoint Security aceptă certificate cu extensii PEM, DER și CRT.
5. Salvați-vă modificările.

Ca rezultat, la scanarea traficului, pe lângă magazinul cu certificate de sistem, Kaspersky Endpoint Security folosește propriul magazin de certificate.

Scanarea conexiunilor criptate cu un certificat care nu este de încredere

După instalare, Kaspersky Endpoint Security adaugă certificatul Kaspersky la stocarea de sistem a certificatelor de încredere (depozitul de certificate Windows). Kaspersky Endpoint Security utilizează acest certificat pentru a scana conexiunile criptate. La vizitarea unui domeniu cu un certificat care nu este de încredere, puteți permite sau interzi accesul utilizatorului la acel domeniu (consultați instrucțiunile de mai jos).

Dacă ați permis utilizatorului să viziteze domenii cu certificate care nu sunt de încredere, Kaspersky Endpoint Security efectuează următoarele acțiuni:

- La vizitarea unui domeniu cu un certificat care nu este de încredere în *browser*, Kaspersky Endpoint Security utilizează certificatul Kaspersky pentru a scana traficul. Kaspersky Endpoint Security afișează o pagină HTML cu un avertisment și informații despre motivul pentru care nu este recomandată vizitarea domeniului relevant (consultă figura de mai jos). Un utilizator poate face clic pe linkul din pagina de avertizare HTML pentru a obține accesul la resursa web solicitată. După accesarea acestui link, în cursul orei următoare, Kaspersky Endpoint Security nu va afișa avertismente referitoare la certificate neautorizate atunci când se vizitează alte resurse din același domeniu. Kaspersky Endpoint Security generează, de asemenea, un eveniment despre stabilirea unei conexiuni criptate cu un certificat care nu are încredere.

  În unele cazuri, Kaspersky Endpoint Security nu poate afișa din punct de vedere tehnic o pagină HTML cu un avertisment în browser (a se vedea figura de mai jos). De exemplu, dacă o resursă web utilizează o versiune învechită a unui protocol de rețea și un port non-standard. În aceste cazuri, Kaspersky Endpoint Security blochează accesul la acest domeniu, iar browserul va afișa fereastra standard `ERR_CONNECTION_RESET`. Pentru a accesa o resursă web, poți adăuga domeniul la excluderi sau poți utiliza un certificat de încredere.

- Dacă *o aplicație terță sau un serviciu terț* stabilește o conexiune cu un domeniu cu un certificat care nu este de încredere, Kaspersky Endpoint Security își creează propriul certificat pentru a scana traficul. Noul certificat are starea *Nu este de încredere*. Acest lucru este necesar pentru a avertiza aplicația terță despre conexiunea care nu este de încredere, deoarece pagina HTML nu poate fi afișată în acest caz și conexiunea poate fi stabilită în modul în fundal. Prin urmare, dacă o aplicație terță are instrumente de verificare a certificatelor încorporate, conexiunea poate fi terminată. În acest caz, trebuie să contactezi proprietarul domeniului și să configurezi o conexiune de încredere. În cazul în care configurarea unei conexiuni de încredere este imposibilă, poți adăuga acea aplicație terță în lista de aplicații de încredere. Kaspersky Endpoint Security generează, de asemenea, un eveniment despre stabilirea unei conexiuni criptate cu un certificat care nu are încredere.

Cum se configurează scanarea conexiunilor criptate cu un certificat care nu este de încredere în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Setări generale** → **Setări rețea**.
4. În blocul **Scanare conexiuni criptate**, fă clic pe butonul **Setări avansate**.
5. În fereastra care se deschide, selectează modul de funcționare a aplicației atunci când vizitezi un domeniu cu un certificat care nu este de încredere: **Permite** sau **Blochează**.
6. Salvați-vă modificările.

Cum se configurează scanarea conexiunilor criptate cu un certificat care nu este de încredere în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.

4. Accesați **General Settings** → **Network Settings**.

5. În blocul **Encrypted Connections Scan**, faceți clic pe linkul **Settings**.

6. În fereastra care se deschide, selectează modul de funcționare a aplicației atunci când vizitezi un domeniu cu un certificat care nu este de încredere: **Allow connection** sau **Block connection**.

7. Salvați-vă modificările.

Cum se configurează scanarea conexiunilor criptate cu un certificat care nu este de încredere în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Setări generale** → **Setări rețea**.

3. În blocul **Scanare conexiuni criptate**, selectează modul de funcționare a aplicației atunci când vizitezi un domeniu cu un certificat care nu este de încredere: **Permite** sau **Blochează**.

4. Salvați-vă modificările.



Avertizare cu privire la vizitarea unui domeniu cu un certificat care nu este de încredere

Adăugarea certificatului Kaspersky la propriul magazin de certificate

Browserele și clienții de e-mail utilizează certificatul pentru a verifica securitatea și autenticitatea resurselor web. Certificatul asigură, de asemenea, criptarea datelor între resursele web și utilizator. Majoritatea browserelor și a clienților de e-mail utilizează depozitul de certificate de încredere (depozitul de certificate Windows). De exemplu, Google Chrome. Unele browsere și unii clienți de e-mail utilizează în mod implicit propriul depozit de certificate în locul depozitului de certificate Windows. De exemplu, Firefox și Thunderbird.

După instalare, Kaspersky Endpoint Security adaugă certificatul Kaspersky la stocarea de sistem a certificatelor de încredere (depozitul de certificate Windows). Dacă Kaspersky Security Center este implementat în organizația ta și o politică este aplicată unui computer, Kaspersky Endpoint Security activează automat utilizarea depozitului de certificate Windows în browserele și clienții de e-mail pentru a scana traficul acestor aplicații. Dacă nu este aplicată o politică pe computer, poți alege depozitul de certificate care va fi utilizat de browsere și de clienții de e-mail. Dacă ai selectat depozitul de certificate propriu, adaugă manual certificatul Kaspersky în depozit. Acest lucru va ajuta la evitarea erorilor atunci când lucrați cu trafic HTTPS.

Pentru a scana traficul în browserul Mozilla Firefox și în clientul de e-mail Thunderbird, trebuie să activați opțiunea Scanare conexiune criptată. Dacă Scanare conexiune criptată este dezactivată, aplicația nu scanează traficul din browserul Mozilla Firefox și clientul de e-mail Thunderbird. Scanarea conexiunilor criptate trebuie, de asemenea, să fie activată pentru a scana traficul în clienții de e-mail MyOffice Mail și R7-Office Organizer.

Înainte de a adăuga un certificat în depozitul de certificate al browserului sau al agentului de e-mail, exportați certificatul Kaspersky din Panoul de control Windows (proprietăți Internet). Poți afla mai multe despre adăugarea unui certificat în depozit, de exemplu, pe site-ul web pentru suport tehnic Mozilla.

Puteți alege depozitul de certificate numai în interfața locală a aplicației.

Pentru a alege un depozit de certificate pentru scanarea conexiunilor criptate în browsere și clienți de e-mail:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Setări generale** → **Setări rețea**.
3. În blocul **Scanare conexiuni criptate**, bifați caseta de selectare **Pentru a scana conexiunile criptate în aplicații cu propriul depozit de certificate, folosește**.
4. Selectați un depozit de certificate:
   - **Depozitul de certificate Windows (recomandat)**. Certificatul rădăcină Kaspersky este adăugat la acest depozit în timpul instalării Kaspersky Endpoint Security.
   - **Depozitul de certificate propriu**. Mozilla Firefox și Thunderbird folosesc propriile depozite de certificate. Dacă este selectat depozitul de certificate Mozilla, trebuie să adăugați manual certificatul rădăcină Kaspersky la acest depozit prin proprietățile browserului.

     Clienții de e-mail MyOffice Mail și R7-Office Organizer folosesc, de asemenea, propriul lor depozit de certificate.
5. Salvați-vă modificările.

Excluderea conexiunilor criptate de la scanare

Majoritatea resurselor web folosesc conexiuni criptate. Experții Kaspersky vă recomandă să activați funcția Scanare conexiuni criptate. Dacă scanarea conexiunilor criptate interferează cu activitatea dvs., puteți adăuga un site web la excluderile considerate *adrese de încredere*. În acest caz, Kaspersky Endpoint Security nu scanează traficul HTTPS al adreselor web de încredere atunci când componentele Web Threat Protection, Mail Threat Protection și Control Web își fac treaba.

Dacă o aplicație de încredere folosește o conexiune criptată, puteți dezactiva scanarea conexiunilor criptate pentru această aplicație. De exemplu, puteți dezactiva scanarea conexiunilor criptate pentru aplicațiile de stocare în cloud care utilizează autentificarea cu doi factori cu propriul certificat.

Modificarea listei de adrese de încredere poate fi blocată de proprietățile politicii principale. Pentru a modifica lista, trebuie să permiteți modificarea setărilor zonei de încredere în Web Console („lacătul" trebuie să fie deblocat).

Zonele de încredere sunt grupate diferit în Consola de administrare (MMC) și în Web Console. De asemenea, modul în care se împiedică modificarea parametrilor zonei de încredere este diferit („lacăte" diferite). Vă recomandăm să utilizați exclusiv Web Console pentru gestionarea aplicației. În cazul în care configurați zona de încredere pe console diferite, este posibil ca plug-inul de gestionare să reseteze „lacătul" la starea implicită.

Cum excludeți o adresă web din scanările conexiunilor criptate în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Setări generale** → **Setări rețea**.
4. În blocul **Scanare conexiuni criptate**, fă clic pe butonul **Configurează adresele de încredere**.
5. Fă clic pe **Adaugă**.
6. Introduceți un nume de domeniu sau o adresă IP dacă nu doriți ca Kaspersky Endpoint Security să scaneze conexiunile criptate stabilite la vizitarea respectivului domeniu.

   Kaspersky Endpoint Security acceptă caracterul `*` pentru introducerea unei măști în numele domeniului.

   Kaspersky Endpoint Security nu acceptă simbolul `*` pentru adresele IP. Puteți selecta un interval de adrese IP folosind o mască de subrețea (de exemplu, 198.51.100.0/24).

   Exemple:

   - `domain.com` – dosarul include următoarele adrese: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Înregistrarea este exclusiv pentru subdomenii (de exemplu, `subdomain.domain.com`).
   - `subdomain.domain.com` – dosarul include următoarele adrese: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Înregistrarea este exclusiv pentru domeniul `domain.com`.
   - `*.domain.com` – dosarul include următoarele adrese: `https://movies.domain.com`, `https://images.domain.com/page123`. Înregistrarea este exclusiv pentru domeniul `domain.com`.
7. Salvați-vă modificările.

Cum excludeți o adresă web din scanările conexiunilor criptate în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **General Settings** → **Network Settings**.
5. În blocul **Encrypted Connections Scan**, fă clic pe butonul **Trusted domains**.
6. Fă clic pe **Add**.
7. Introduceți un nume de domeniu sau o adresă IP dacă nu doriți ca Kaspersky Endpoint Security să scaneze conexiunile criptate stabilite la vizitarea respectivului domeniu.

   Kaspersky Endpoint Security acceptă caracterul `*` pentru introducerea unei măști în numele domeniului.

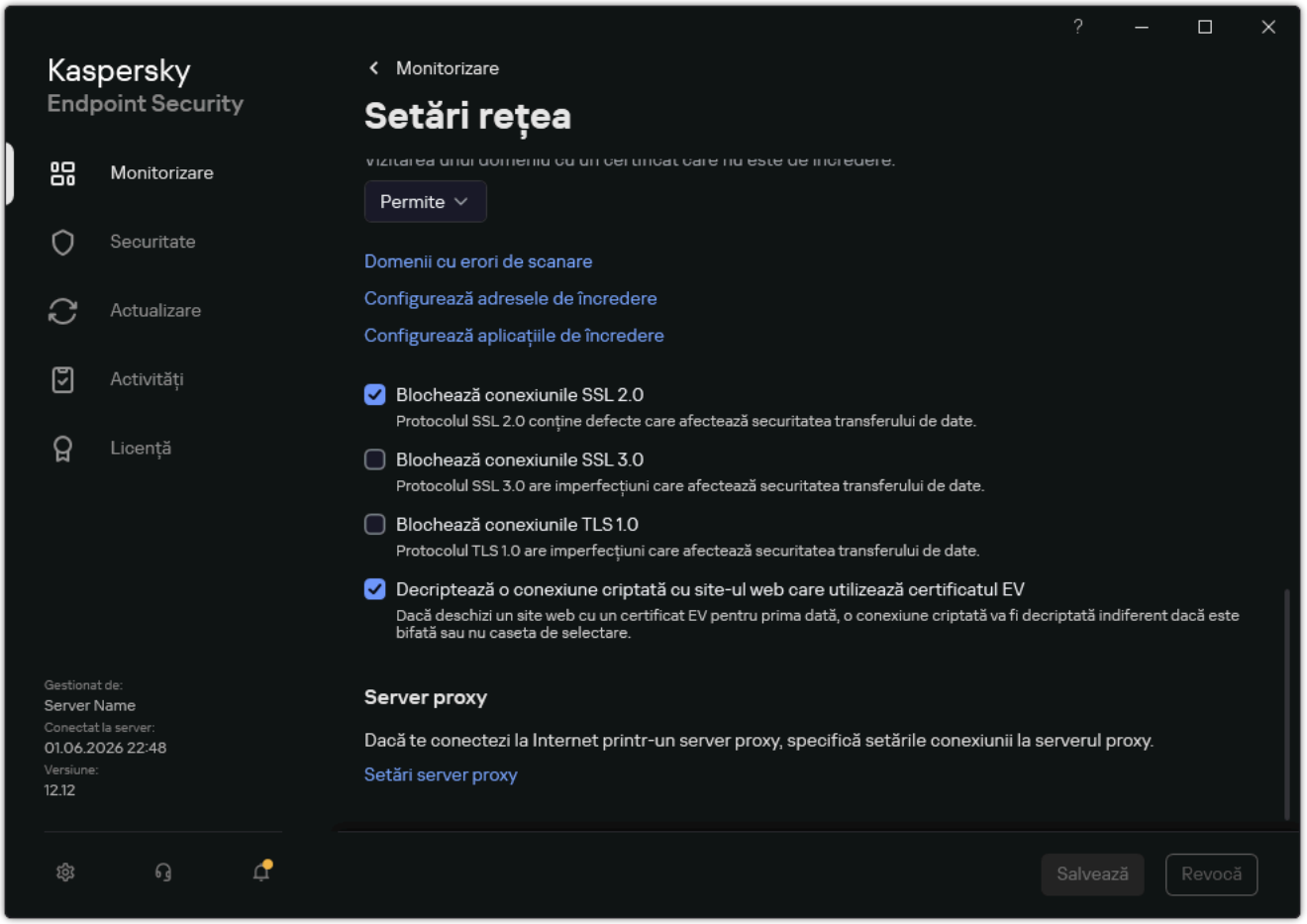
   > Kaspersky Endpoint Security nu acceptă simbolul `*` pentru adresele IP. Puteți selecta un interval de adrese IP folosind o mască de subrețea (de exemplu, 198.51.100.0/24).

   Exemple:

   - `domain.com` – dosarul include următoarele adrese: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Înregistrarea este exclusiv pentru subdomenii (de exemplu, `subdomain.domain.com`).
   - `subdomain.domain.com` – dosarul include următoarele adrese: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Înregistrarea este exclusiv pentru domeniul `domain.com`.
   - `*.domain.com` – dosarul include următoarele adrese: `https://movies.domain.com`, `https://images.domain.com/page123`. Înregistrarea este exclusiv pentru domeniul `domain.com`.
8. Salvați-vă modificările.

Cum excludeți o adresă web din scanările conexiunilor criptate în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Setări generale** → **Setări rețea**.



Setări de rețea pentru aplicație

3. În blocul **Scanare conexiuni criptate**, fă clic pe butonul **Configurează adresele de încredere**.
4. Fă clic pe **Adaugă**.
5. Introduceți un nume de domeniu sau o adresă IP dacă nu doriți ca Kaspersky Endpoint Security să scaneze conexiunile criptate stabilite la vizitarea respectivului domeniu.

   Kaspersky Endpoint Security acceptă caracterul `*` pentru introducerea unei măști în numele domeniului.

   > Kaspersky Endpoint Security nu acceptă simbolul `*` pentru adresele IP. Puteți selecta un interval de adrese IP folosind o mască de subrețea (de exemplu, 198.51.100.0/24).

Exemple:

- `domain.com` – dosarul include următoarele adrese: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Înregistrarea este exclusiv pentru subdomenii (de exemplu, `subdomain.domain.com`).
- `subdomain.domain.com` – dosarul include următoarele adrese: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Înregistrarea este exclusiv pentru domeniul `domain.com`.
- `*.domain.com` – dosarul include următoarele adrese: `https://movies.domain.com`, `https://images.domain.com/page123`. Înregistrarea este exclusiv pentru domeniul `domain.com`.

6. Salvați-vă modificările.

În mod implicit, Kaspersky Endpoint Security nu scanează conexiunile criptate atunci când apar erori și adaugă site-ul web la o listă specială de *Domenii cu erori de scanare*. Kaspersky Endpoint Security întocmește o listă separată pentru fiecare utilizator și nu trimite date către Kaspersky Security Center. Puteți activa blocarea conexiunii atunci când apare o eroare de scanare. Puteți vizualiza o listă de domenii cu erori de scanare a conexiunilor sigure numai în interfața locală a aplicației.

Pentru a vizualiza lista de domenii cu erori de scanare:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Setări generale** → **Setări rețea**.
3. În blocul **Scanare conexiuni criptate**, fă clic pe butonul **Domenii cu erori de scanare**.

   Se deschide o listă de domenii cu erori de scanare. Pentru a reseta lista, activați blocarea conexiunii atunci când apar erori de scanare în politică, aplicați politica, apoi resetați parametrul la valoarea inițială și aplicați din nou politica.

Specialiștii Kaspersky fac o listă de *excepții globale* - site-uri web de încredere pe care Kaspersky Endpoint Security nu le verifică indiferent de setările aplicației.

Pentru a vizualiza excluderile globale de la scanări ale traficului criptat:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Setări generale** → **Setări rețea**.
3. În blocul **Scanare conexiuni criptate**, faceți clic pe linkul listei cu site-uri web de încredere.

   Aceasta deschide o listă de site-uri web compilate de experții Kaspersky. Kaspersky Endpoint Security nu scanează conexiunile protejate pentru site-urile web din listă. Lista poate fi actualizată atunci când sunt actualizate bazele de date Kaspersky Endpoint Security.

Ștergere date

Kaspersky Endpoint Security vă permite să utilizați o activitate pentru a șterge de la distanță datele de pe computerele utilizatorilor.

Kaspersky Endpoint Security șterge datele astfel:

- În modul silențios;
- Pe unități de hard disk și unități amovibile;
- Pentru toate conturile de utilizator de pe computer.

Kaspersky Endpoint Security execută activitatea *Șterge datele* indiferent de tipul de licență utilizat, chiar și după expirarea licenței.

Moduri de Ștergere date

Această activitate vă permite să ștergeți datele în următoarele moduri:

- Ștergere imediată a datelor.

  În acest mod, puteți, de exemplu, să ștergeți date vechi pentru a elibera spațiu pe disc.

- Ștergere amânată a datelor.

  Acest mod este destinat, de exemplu, protejării datelor de pe un laptop în cazul în care acesta este pierdut sau furat. Puteți configura ștergerea automată a datelor dacă laptopul depășește limitele rețelei corporative și nu a fost sincronizat cu Kaspersky Security Center de mult timp.

Nu este posibil să setați un program pentru ștergerea datelor în proprietățile activității. Puteți șterge datele doar imediat după pornirea manuală a activității sau puteți configura ștergerea întârziată a datelor dacă nu există nicio conexiune cu Kaspersky Security Center.

Limitări

Activitatea Ștergere date are următoarele limitări:

- Doar un administrator Kaspersky Security Center poate gestiona activitatea *Șterge datele*. Nu puteți configura sau porni o activitate în interfața locală a Kaspersky Endpoint Security.
- Pentru sistemul de fișiere NTFS, Kaspersky Endpoint Security șterge doar numele principalelor fluxuri de date. Numele alternative ale fluxului de date nu pot fi șterse.
- Când ștergeți un fișier de legături simbolice, Kaspersky Endpoint Security șterge și fișierele ale căror căi sunt specificate în legătura simbolică.

Crearea unei activități de ștergere a datelor

Pentru a șterge datele de pe computerele utilizatorilor:

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **Add**.

   Expertul de activitate pornește.

3. Configurați setările pentru activitate:

   a. În lista verticală **Application**, selectează **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. În lista verticală **Task type**, selectează **Wipe data**.

   c. În câmpul **Task name**, introduceți o descriere succintă, de exemplu *Wipe data (Anti-Theft)*.

   d. În blocul **Devices to which the task will be assigned**, selectați domeniul activității.

4. Selectați dispozitive în funcție de opțiunea selectată pentru domeniul activității. Mergeți la pasul următor.

   Dacă se adaugă noi computere la un grup de administrare din domeniul activității, activitatea de ștergere imediată a datelor este executată pe noile calculatoare numai dacă activitatea este finalizată în termen de 5 minute de la adăugarea noilor computere.

5. Ieșiți din Expert.

   Se va afișa o activitate nouă în lista de activități.

6. Faceți clic pe activitatea **Wipe data** a Kaspersky Endpoint Security.

   Se va deschide fereastra de proprietăți a activității.

7. Selectați fila **Application settings**.

8. Selectați metoda de ștergere a datelor:

   - **Delete by means of the operating system**. Kaspersky Endpoint Security folosește resursele sistemului de operare pentru a șterge fișierele, fără a le trimite la coșul de reciclare.

   - **Delete completely, no recovery possible**. Kaspersky Endpoint Security suprascrie fișierele cu date aleatorii. Este, practic, imposibil să restaurați datele după ce acestea sunt șterse.

9. Dacă doriți să amânați ștergerea datelor, bifați caseta de selectare **Automatically wipe data when there is no connection to Kaspersky Security Center for more than N days** Stabiliți numărul de zile.

   Activitatea de ștergere amânată a datelor va fi efectuată de fiecare dată când o conexiune cu Kaspersky Security Center lipsește pentru perioada de timp definită.

Când configurezi ștergerea amânată a datelor, reține că angajații pot avea programe de lucru diferite. Luați în considerare și programul de lucru al utilizatorilor offline. Pentru mai multe detalii despre lucrul cu computere offline și utilizatori absenți de la birou, consultați Ajutor pentru Kaspersky Security Center.

În cazul în care computerul este oprit și conexiunea a fost absentă pentru o perioadă mai lungă decât durata configurată, după pornirea computerului, Kaspersky Endpoint Security nu șterge datele imediat. Aplicația așteaptă sincronizarea cu Kaspersky Security Center timp de o oră. Acest lucru este necesar pentru a preveni ștergerea neautorizată a datelor de pe computerele utilizatorilor care și-au oprit computerele, de exemplu, înainte de a pleca în vacanță.

În cazul în care caseta de selectare este debifată, activitatea se va efectua imediat după sincronizarea cu Kaspersky Security Center.

10. Creați o listă de obiecte de șters:

- **Directoare**. Kaspersky Endpoint Security șterge toate fișierele din director și subdirectoarele sale. Kaspersky Endpoint Security nu acceptă măști și variabile de mediu la introducerea unei căi către director.
- **Fișiere după extensie**. Kaspersky Endpoint Security caută fișierele cu extensiile specificate pe toate unitățile computerului, inclusiv pe unitățile amovibile. Folosiți caracterul „`;`” sau „`,`” pentru a specifica mai multe extensii.
- **Domeniu predefinit**. Kaspersky Endpoint Security va șterge fișierele din următoarele zone:
  - **Documents**. Fișiere din directorul standard *Documente* al sistemului de operare și subdirectoarele sale.
  - **Cookies**. Fișiere în care browserul salvează date de pe site-urile web vizitate de utilizator (cum ar fi datele de autorizare ale utilizatorului).
  - **Desktop**. Fișiere din directorul standard *Desktop* al sistemului de operare și subdirectoarele sale.
  - **Temporary Internet Explorer files**. Fișiere temporare legate de funcționarea Internet Explorer, precum copii ale paginilor web, imagini și fișiere media.
  - **Temporary files**. Fișiere temporare legate de funcționarea aplicațiilor instalate pe computer. De exemplu, aplicațiile Microsoft Office creează fișiere temporare care conțin copii de rezervă ale documentelor.
  - **Outlook files**. Fișiere legate de funcționarea clientului de e-mail Outlook: fișiere de date (PST), fișiere de date offline (OST), fișiere offline address book (OAB) și fișiere personal address book (PAB).
  - **User profile**. Set de fișiere și directoare care stochează setările sistemului de operare pentru contul de utilizator local.

Puteți crea o listă de obiecte de șters pe fiecare filă. Kaspersky Endpoint Security va crea o listă consolidată și va șterge fișierele din această listă atunci când o activitate este finalizată.

Nu puteți șterge fișierele necesare pentru funcționarea Kaspersky Endpoint Security.

11. Salvați-vă modificările.
12. Bifați caseta de selectare de lângă activitate.
13. Fă clic pe **Start**.

Drept urmare, datele de pe computerele utilizatorilor vor fi șterse în funcție de modul selectat: imediat sau în absența unei conexiuni. Dacă Kaspersky Endpoint Security nu poate șterge un fișier, cum ar fi atunci când un utilizator folosește în prezent un fișier, aplicația nu încearcă să-l șteargă din nou. Pentru a finaliza ștergerea datelor, executați activitatea din nou.

Controlul computerului

Control Web

Componenta Control Web gestionează accesul utilizatorilor la resursele web. Acest lucru ajută la reducerea traficului și la utilizarea necorespunzătoare a timpului de muncă. Când un utilizator încearcă să deschidă un site web care este restricționat de Control Web, Kaspersky Endpoint Security va bloca accesul sau va afișa un avertisment (vedeți figura de mai jos).

Pentru a utiliza componenta Control Web, trebuie să finalizezi configurarea inițială a aplicației:

- Pentru monitorizarea traficului HTTPS, activează scanarea conexiunilor criptate (activată în mod implicit).
- Selectează porturile pe care Kaspersky Endpoint Security trebuie să monitorizeze (implicit, aplicația monitorizează toate porturile).
- Selectează aplicațiile al căror trafic dorești să îl monitorizeze Kaspersky Endpoint Security. Majoritatea browserelor sunt deja prezente în lista de aplicații recomandate de Kaspersky. Dacă browserul tău lipsește din listă, adaugă-l manual.
- Îți recomandăm să injectezi un script de interacțiune a paginii web în traficul web (în mod implicit, injectarea de script este dezactivată). Acest script permite înregistrarea evenimentelor Control Web pentru jurnalul de evenimente al aplicației, jurnalul de evenimente al sistemului de operare și rapoarte.

Metode de gestionare a accesului la site-uri web

Componenta Control Web vă permite să configurați accesul la site-uri web folosind următoarele metode:

- **Categorie site web**. Site-urile web sunt clasificate în funcție de serviciul cloud Kaspersky Security Network, analiza euristică și baza de date a site-urilor web cunoscute (incluse în bazele de date ale aplicațiilor). De exemplu, puteți restricționa accesul utilizatorului la categoria *Rețele de socializare* sau la alte categorii.
- **Tipul de date**. Poți restricționa accesul utilizatorilor la datele de pe un site web și poți ascunde imaginile, de exemplu. Kaspersky Endpoint Security determină tipul de date pe baza formatului fișierului și nu pe baza extensiei sale.

  > Kaspersky Endpoint Security nu scanează fișierele din arhive. De exemplu, dacă fișierele imagine au fost plasate într-o arhivă, Kaspersky Endpoint Security identifică tipul de date *Arhive* și nu *Grafică*.

- **Adresă individuală**. Puteți introduce o adresă web sau puteți folosi măști.

Puteți utiliza simultan mai multe metode pentru reglementarea accesului la site-uri web. De exemplu, poți restricționa accesul la tipul de date *Fișiere ale aplicațiilor Office* doar pentru categoria de site-uri web *E-mail bazat pe web*.

Regulile de acces la site-urile web

Componenta Control Web gestionează accesul utilizatorilor la site-urile web utilizând *reguli de acces*. Puteți configura următoarele setări avansate pentru o regulă de acces la site-urile web:

- Utilizatori cărora li se aplică regula.

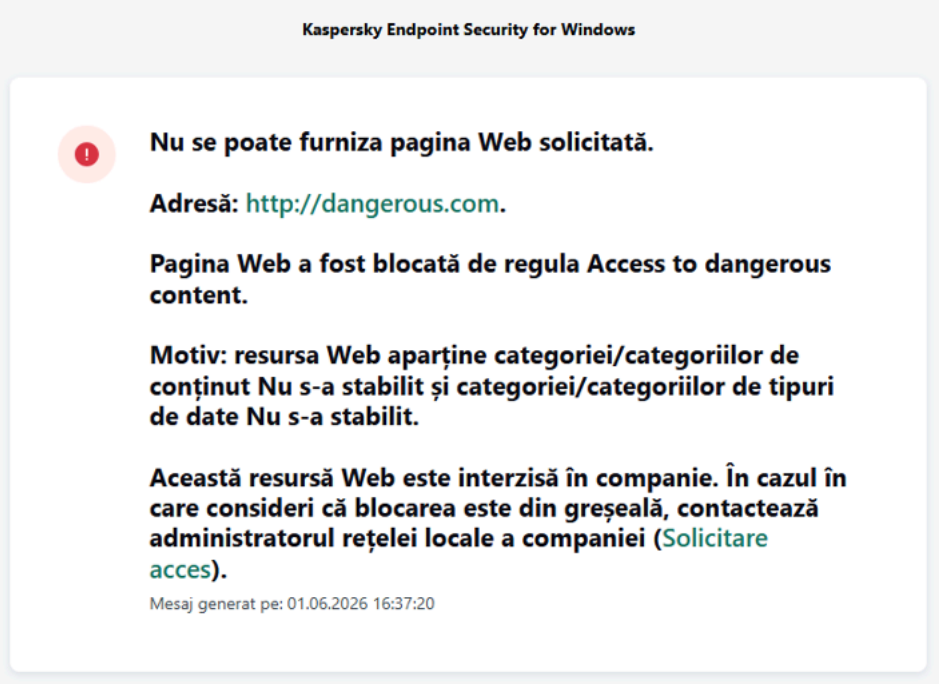
  De exemplu, puteți restricționa accesul la Internet printr-un browser pentru toți utilizatorii companiei, cu excepția departamentului IT.

- Planificare regulă.

  De exemplu, puteți restricționa accesul la Internet printr-un browser doar în timpul programului de lucru.

Priorități pentru reguli de acces

Fiecare regulă are o prioritate. Cu cât o regulă este mai sus în listă, cu atât prioritatea sa este mai mare. Dacă un site web a fost adăugat mai multor reguli, componenta Control Web reglementează accesul la site-ul web pe baza regulii cu cea mai mare prioritate. De exemplu, Kaspersky Endpoint Security poate identifica un portal corporativ ca o rețea socială. Pentru a restricționa accesul la rețelele sociale și a oferi acces la portalul web corporativ, creați două reguli: o regulă de blocare pentru categoria site-urilor web *Rețele de socializare* și una de permitere pentru portalul web corporativ. Regula de acces pentru portalul web corporativ trebuie să aibă o prioritate mai mare decât regula de acces pentru rețelele sociale.





Mesajele componentei Control Web

Adăugarea unei reguli de acces la resursele web

O *regulă de acces la resurse web* este un set de filtre și acțiuni pe care Kaspersky Endpoint Security le aplică atunci când utilizatorii vizitează resurse web. Regulile de acces pot include o planificare a regulilor.

Nu se recomandă crearea a mai mult de 1.000 de reguli de acces la resurse Web, deoarece aceasta poate cauza sistemul să devină instabil.

O regulă de acces la resurse Web este un set de filtre și acțiuni efectuate de Kaspersky Endpoint Security când utilizatorul vizitează resurse Web descrise în regulă în intervalul de timp indicat în planificarea regulii. Filtrele îți permit să specifici cu precizie un set de resurse Web la care accesul este controlat de componenta Control Web.

Sunt disponibile următoarele filtre:

- **Filtrare după conținut**. Componenta Control Web împarte resursele Web în categorii în funcție de conținut și tipul datelor. Poți controla accesul utilizatorului la resurse Web cu conținut și date care se încadrează în tipurile definite de aceste categorii. Când utilizatorii vizitează resurse Web care aparțin categoriei de conținut și/sau categoriei de tip de date selectate, Kaspersky Endpoint Security efectuează acțiunea specificată în regulă.

- **Filtrare după adresele resurselor Web**. Poți controla accesul utilizatorului la toate adresele de resurse Web sau la adrese de resurse Web individuale și/sau la grupuri de adrese de resurse Web.

  Dacă sunt specificate filtrarea după conținut și filtrarea după adresele resurselor Web și adresele specificate pentru resurse Web și/sau grupuri de resurse Web aparțin categoriilor de conținut sau categoriilor de tipuri de date selectate, Kaspersky Endpoint Security nu controlează accesul la toate resursele Web din categoriile de conținut și/sau categoriile de tipuri de date selectate. În schimb, aplicația controlează numai accesul la adresele de resurse Web și/sau adresele de grupuri de resurse Web specificate.

- **Filtrare după numele utilizatorilor sau ale grupurilor de utilizatori**. Poți specifica numele utilizatorilor și/sau grupurilor de utilizatori pentru care accesul la resurse Web este controlat după această regulă.

- **Planificare regulă**. Poți specifica planificarea regulii. Planificarea regulii determină intervalul de timp pentru care aplicația Kaspersky Endpoint Security monitorizează accesul la resursele Web la care se aplică regula.

După instalarea Kaspersky Endpoint Security, lista de reguli a componentei Control Web nu este goală. Opțiunea *Regulă implicită* este presetată. Această regulă se aplică oricăror resurse Web care nu sunt acoperite de alte reguli și permite sau blochează accesul la aceste resurse Web pentru toți utilizatorii.

Fiecare regulă are o prioritate. Cu cât o regulă este mai sus în listă, cu atât prioritatea sa este mai mare. Dacă un site web a fost adăugat mai multor reguli, componenta Control Web reglementează accesul la site-ul web pe baza regulii cu cea mai mare prioritate. De exemplu, Kaspersky Endpoint Security poate identifica un portal corporativ ca o rețea socială. Pentru a restricționa accesul la rețelele sociale și a oferi acces la portalul web corporativ, creați două reguli: o regulă de blocare pentru categoria site-urilor web *Rețele de socializare* și una de permitere pentru portalul web corporativ. Regula de acces pentru portalul web corporativ trebuie să aibă o prioritate mai mare decât regula de acces pentru rețelele sociale.

Cum se adaugă o regulă de acces la resurse web în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Security Controls → Control Web**.
4. Bifați caseta de selectare **Control Web**.
5. În blocul **Setări Control Web**, fă clic pe butonul **Adaugă**.
   Se deschide fereastra **Regulă de acces la resurse Web**.
6. Configurează regula de acces la resursele web (consultă tabelul de mai jos).
7. Dacă dorești ca, imediat după aplicarea politicii, componenta Control Web să încheie conexiunea cu resursa web interzisă, bifează caseta de selectare **Termină sesiunile browserului utilizatorului activ după aplicarea regulii**.

   > Controlul web permite deconectarea imediată a resurselor web numai în browserele web. Pentru alte aplicații, Web Control restricționează doar conexiunile noi.

   În cazul în care caseta de selectare este debifată, componenta Control Web restricționează numai conexiunile noi la resursele web interzise. Componenta Control Web nu oprește conexiunile active.
8. Salvați-vă modificările.

Cum se adaugă o regulă de acces la resurse web în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management → Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.
   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.

4. Accesați **Security Controls** → **Web Control**.

5. Duceți comutatorul **Web Control ENABLED** la poziția activat.

6. În blocul **Rules list**, fă clic pe butonul **Add**.

7. Configurează regula de acces la resursele web (consultă tabelul de mai jos).

8. Dacă dorești ca, imediat după aplicarea politicii, componenta Control Web să încheie conexiunea cu resursa web interzisă, bifează caseta de selectare **Terminate active user browser sessions after the rule is applied**.

   > Controlul web permite deconectarea imediată a resurselor web numai în browserele web. Pentru alte aplicații, Web Control restricționează doar conexiunile noi.

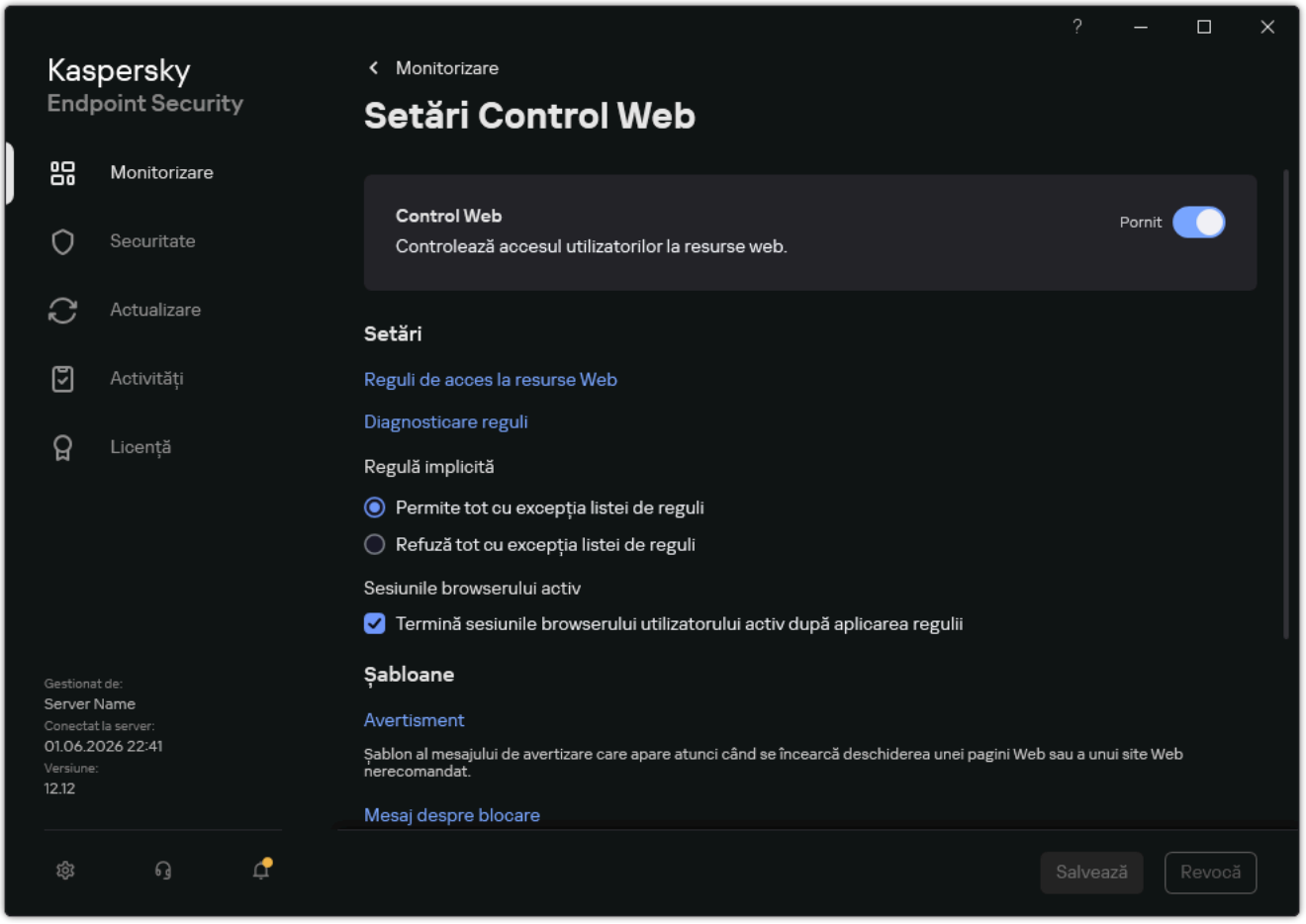
   În cazul în care caseta de selectare este debifată, componenta Control Web restricționează numai conexiunile noi la resursele web interzise. Componenta Control Web nu oprește conexiunile active.

9. Salvați-vă modificările.

Cum se adaugă o regulă de acces la resurse web în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Security Controls** → **Control Web**.



Setări Control Web

3. Duceți comutatorul **Control Web** la poziția activat.

4. În blocul **Setări**, fă clic pe butonul **Reguli de acces la resurse Web**.

5. În fereastra care se deschide, faceți clic pe butonul **Adaugă**.

   Se deschide fereastra **Regulă de acces la resurse Web**.

6. Configurează regula de acces la resursele web (consultă tabelul de mai jos).

7. Dacă dorești ca, imediat după aplicarea politicii, componenta Control Web să încheie conexiunea cu resursa web interzisă, bifează caseta de selectare **Termină sesiunile browserului utilizatorului activ după aplicarea regulii**.

   Controlul web permite deconectarea imediată a resurselor web numai în browserele web. Pentru alte aplicații, Web Control restricționează doar conexiunile noi.

   În cazul în care caseta de selectare este debifată, componenta Control Web restricționează numai conexiunile noi la resursele web interzise. Componenta Control Web nu oprește conexiunile active.

8. Salvați-vă modificările.

Ca urmare, noua regulă Control Web este adăugată în listă. Dacă este necesar, modifică prioritatea regulii Control Web. De asemenea, poți utiliza comutatorul pentru a dezactiva regula de acces la resursele web în orice moment, fără a o elimina din listă.

Parametrii regulii Control Web

Parametru	Descriere
Nume regulă	Numele regulii Control Web.
Condiție	• **Pornită**. • **Oprită**. Poți utiliza comutatorul pentru a dezactiva regula de acces la resursele web în orice moment.
Acțiune	• **Permite**. Componenta Control Web permite accesul la resurse web care corespund parametrilor regulii. • **Blochează**. Componenta Control Web blochează accesul la resursele web care corespund parametrilor regulii și afișează un mesaj de acces refuzat la site-ul web. • **Avertizează**. Atunci când utilizatorul încearcă să obțină acces la o resursă web care corespunde regulii, componenta Control Web afișează un avertisment care indică faptul că vizitarea resursei web este nerecomandată. Utilizând linkuri din mesajul de avertizare, utilizatorul poate obține acces la resursa Web solicitată.
Conținutul filtrului	• **După categorii de conținut**. Puteți controla accesul utilizatorilor la resursele web în funcție de categorie (de exemplu, categoria *Rețele de socializare*). • **După tipuri de date**. Puteți controla accesul utilizatorilor la resursele web pe baza tipului specific de date al datelor publicate (de exemplu, *Grafică*).
Adrese	• **Pentru toate adresele**. Control Web nu va filtra resursele web după adresă. • **Pentru adresele individuale**. Control Web va filtra numai adresele resurselor web din listă. Puteți introduce o adresă web sau puteți folosi măști. De asemenea, puteți exporta o listă de adrese de resurse web dintr-un fișier TXT. Poți selecta utilizatori în Active Directory, în lista de conturi din Kaspersky Security Center sau introducând manual un nume de utilizator local. Kaspersky recomandă utilizarea conturilor de utilizator locale numai în cazuri speciale, când nu este posibilă utilizarea conturilor de utilizator de domeniu. Dacă este dezactivată opțiunea Scanare conexiuni criptate, pentru protocolul HTTPS puteți filtra doar după numele de server.
Utilizatori	• **Pentru toți utilizatorii**. Control Web nu va filtra resursele web pentru anumiți utilizatori. • **Pentru utilizatori individuali și/sau grupuri individuale**. Control Web va filtra resursele web numai pentru anumiți utilizatori. Poți selecta utilizatori în Active Directory, în lista de conturi din Kaspersky Security Center sau introducând manual un nume de utilizator local. Kaspersky recomandă utilizarea conturilor de utilizator locale numai în cazuri speciale, când nu este posibilă utilizarea conturilor de utilizator de domeniu.
Planificare regulă	Planificarea regulii determină intervalul de timp pentru care aplicația Kaspersky Endpoint Security monitorizează accesul la resursele Web la care se aplică regula. De exemplu, puteți restricționa accesul la Internet printr-un browser doar în timpul programului de lucru.

Filtrare după adresele resurselor Web

Pentru a controla accesul la resurse web individuale, trebuie să creezi o regulă Control Web, o listă de adrese web și să selectezi o acțiune Control Web. Atunci când creezi o listă de adrese web, poți introduce adrese URL sau poți utiliza măști.

Regulile pot include o planificare a regulii și o listă de utilizatori cărora li se aplică regula. De exemplu, poți restricționa accesul la site-urile web numai în timpul orelor de lucru sau poți permite vizitarea site-urilor web de către utilizatorii din anumite grupuri.

Cum se activează un filtru de conținut al resurselor web în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Security Controls** → **Control Web**.
4. Bifați caseta de selectare **Control Web**.
5. În blocul **Setări Control Web**, fă clic pe butonul **Adaugă**.
   Se deschide fereastra **Regulă de acces la resurse Web**.
6. Configurează regula de acces la resursele web:
   a. În câmpul **Nume**, introduceți numele regulii.
   b. În lista verticală **Aplică adreselor**, selectează **Pentru adresele individuale**.
   c. Creează o listă de adrese de resurse web. Puteți introduce o adresă web sau puteți folosi măști. De asemenea, puteți exporta o listă de adrese de resurse web dintr-un fișier TXT.

      Dacă este dezactivată opțiunea Scanare conexiuni criptate, pentru protocolul HTTPS puteți filtra doar după numele de server.

   d. În lista verticală **Aplică utilizatorilor**, selectează filtrul relevant pentru utilizatori:

      - **Pentru toți utilizatorii**. Control Web nu va filtra resursele web după adresă.
      - **Pentru anumiți utilizatori sau pentru anumite grupuri**. Control Web va filtra numai adresele resurselor web din listă. Puteți introduce o adresă web sau puteți folosi măști. De asemenea, puteți exporta o listă de adrese de resurse web dintr-un fișier TXT. Poți selecta utilizatori în Active Directory, în lista de conturi din Kaspersky Security Center sau introducând manual un nume de utilizator local. Kaspersky recomandă utilizarea conturilor de utilizator locale numai în cazuri speciale, când nu este posibilă utilizarea conturilor de utilizator de domeniu.

e. În lista verticală **Acțiune**, selectează opțiunea:

- **Permite**. Componenta Control Web permite accesul la resurse web care corespund parametrilor regulii.
- **Blochează**. Componenta Control Web blochează accesul la resursele web care corespund parametrilor regulii și afișează un mesaj de acces refuzat la site-ul web.
- **Avertizează**. Atunci când utilizatorul încearcă să obțină acces la o resursă web care corespunde regulii, componenta Control Web afișează un avertisment care indică faptul că vizitarea resursei web este nerecomandată. Utilizând linkuri din mesajul de avertizare, utilizatorul poate obține acces la resursa Web solicitată.

f. În lista verticală **Planificare regulă**, selectează o planificare sau creează una nouă.

7. Dacă dorești ca, imediat după aplicarea politicii, componenta Control Web să încheie conexiunea cu resursa web interzisă, bifează caseta de selectare **Termină sesiunile browserului utilizatorului activ după aplicarea regulii**.

   Controlul web permite deconectarea imediată a resurselor web numai în browserele web. Pentru alte aplicații, Web Control restricționează doar conexiunile noi.

   În cazul în care caseta de selectare este debifată, componenta Control Web restricționează numai conexiunile noi la resursele web interzise. Componenta Control Web nu oprește conexiunile active.

8. Salvați-vă modificările.

Cum se activează un filtru de adrese al resurselor web în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Security Controls** → **Web Control**.
5. Duceți comutatorul **Web Control ENABLED** la poziția activat.
6. În blocul **Rules list**, fă clic pe butonul **Add**.
7. Configurează regula de acces la resursele web:

   a. În câmpul **Rule name**, introduceți numele regulii.

   b. Selectați starea **Enabled** pentru regula de acces la resursele web.

   Poți utiliza comutatorul pentru a dezactiva regula de acces la resursele web în orice moment, fără a o elimina din listă.

c. În secțiunea **Action**, selectați opțiunea relevantă:

- **Allow**. Componenta Control Web permite accesul la resurse web care corespund parametrilor regulii.
- **Block**. Componenta Control Web blochează accesul la resursele web care corespund parametrilor regulii și afișează un mesaj de acces refuzat la site-ul web.
- **Inform**. Atunci când utilizatorul încearcă să obțină acces la o resursă web care corespunde regulii, componenta Control Web afișează un avertisment care indică faptul că vizitarea resursei web este nerecomandată. Utilizând linkuri din mesajul de avertizare, utilizatorul poate obține acces la resursa Web solicitată.

d. În **Scope**, selectează **Individual websites**.

e. Configurează filtrul de conținut:

- **Individual address**. Creează o listă de adrese de resurse web. Puteți introduce o adresă web sau puteți folosi măști. De asemenea, puteți exporta o listă de adrese de resurse web dintr-un fișier TXT.

  > Dacă este dezactivată opțiunea Scanare conexiuni criptate, pentru protocolul HTTPS puteți filtra doar după numele de server.

- **Data type**. Puteți controla accesul utilizatorilor la resursele web pe baza tipului specific de date al datelor publicate (de exemplu, *Grafică*).

f. În **User or group**, selectează utilizatorii cărora dorești ca Control Web să le aplice regula.

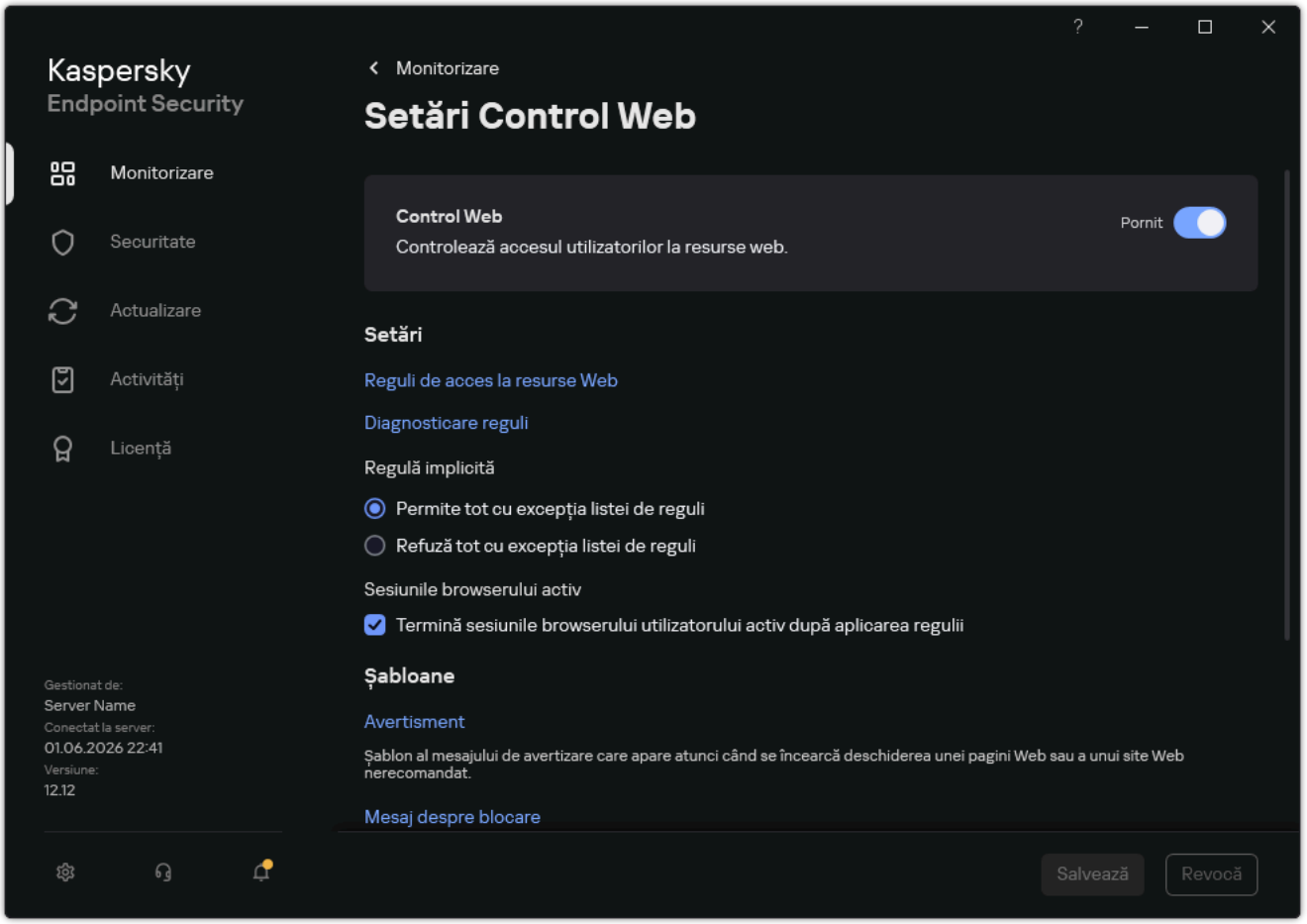
Control Web va filtra numai adresele resurselor web din listă. Puteți introduce o adresă web sau puteți folosi măști. De asemenea, puteți exporta o listă de adrese de resurse web dintr-un fișier TXT. Poți selecta utilizatori în Active Directory, în lista de conturi din Kaspersky Security Center sau introducând manual un nume de utilizator local. Kaspersky recomandă utilizarea conturilor de utilizator locale numai în cazuri speciale, când nu este posibilă utilizarea conturilor de utilizator de domeniu.

g. În blocul **Access schedule**, selectează o planificare sau creează una nouă.

8. Salvați-vă modificările.

Cum se activează un filtru de adrese al resursei web în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Security Controls** → **Control Web**.



Setări Control Web

3. În blocul **Setări**, fă clic pe butonul **Reguli de acces la resurse Web**.
4. În fereastra care se deschide, faceți clic pe butonul **Adaugă**.

   Se deschide fereastra **Regulă de acces la resurse Web**.
5. În câmpul **Nume regulă**, introduceți numele regulii.
6. Selectați starea **Pornită** pentru regula de acces la resursele web.

   Poți utiliza comutatorul pentru a dezactiva regula de acces la resursele web în orice moment.
7. În secțiunea **Acțiune**, selectați opțiunea relevantă:

   - **Permite**. Componenta Control Web permite accesul la resurse web care corespund parametrilor regulii.
   - **Blochează**. Componenta Control Web blochează accesul la resursele web care corespund parametrilor regulii și afișează un mesaj de acces refuzat la site-ul web.
   - **Avertizează**. Atunci când utilizatorul încearcă să obțină acces la o resursă web care corespunde regulii, componenta Control Web afișează un avertisment care indică faptul că vizitarea resursei web este nerecomandată. Utilizând linkuri din mesajul de avertizare, utilizatorul poate obține acces la resursa Web solicitată.

8. În **Adrese**, selectează **Pentru adresele individuale**.

   Creează o listă de adrese de resurse web. Puteți introduce o adresă web sau puteți folosi măști. De asemenea, puteți exporta o listă de adrese de resurse web dintr-un fișier TXT.

   > Dacă este dezactivată opțiunea Scanare conexiuni criptate, pentru protocolul HTTPS puteți filtra doar după numele de server.

9. În blocul **Utilizatori**, selectați filtrul relevant pentru utilizatori:

   - **Pentru toți utilizatorii**. Control Web nu va filtra resursele web pentru anumiți utilizatori.
   - **Pentru utilizatori individuali și/sau grupuri individuale**. Control Web va filtra numai adresele resurselor web din listă. Puteți introduce o adresă web sau puteți folosi măști. De asemenea, puteți exporta o listă de adrese de resurse web dintr-un fișier TXT. Poți selecta utilizatori în Active Directory, în lista de conturi din Kaspersky Security Center sau introducând manual un nume de utilizator local. Kaspersky recomandă utilizarea conturilor de utilizator locale numai în cazuri speciale, când nu este posibilă utilizarea conturilor de utilizator de domeniu.

10. În lista verticală **Planificare regulă**, selectează o planificare sau creează una nouă.

11. Dacă dorești ca, imediat după aplicarea politicii, componenta Control Web să încheie conexiunea cu resursa web interzisă, bifează caseta de selectare **Termină sesiunile browserului utilizatorului activ după aplicarea regulii**.

    > Controlul web permite deconectarea imediată a resurselor web numai în browserele web. Pentru alte aplicații, Web Control restricționează doar conexiunile noi.

    În cazul în care caseta de selectare este debifată, componenta Control Web restricționează numai conexiunile noi la resursele web interzise. Componenta Control Web nu oprește conexiunile active.

12. Salvați-vă modificările.

Ca urmare, noua regulă Control Web este adăugată în listă. Dacă este necesar, modifică prioritatea regulii Control Web. De asemenea, poți utiliza comutatorul pentru a dezactiva regula de acces la resursele web în orice moment, fără a o elimina din listă.

Filtrare după conținutul resurselor Web

Pentru a controla accesul în funcție de conținutul resurselor web, componenta Control Web oferă un filtru în funcție de categorie și un filtru în funcție de tipul datelor.

Site-urile web sunt clasificate în funcție de serviciul cloud Kaspersky Security Network, analiza euristică și baza de date a site-urilor web cunoscute (incluse în bazele de date ale aplicațiilor). De exemplu, puteți restricționa accesul utilizatorului la categoria *Rețele de socializare* sau la alte categorii.

Poți restricționa accesul utilizatorilor la un site web în funcție de tipul de date, de exemplu, pentru a ascunde imaginile. Kaspersky Endpoint Security determină tipul de date pe baza formatului fișierului și nu pe baza extensiei sale. Componenta Control Web distinge următoarele tipuri de date:

- Videoclipuri
- Sunet
- Fișiere ale aplicațiilor Office
- Fișiere executabile
- Arhive
- Grafică
- Scripturi

Kaspersky Endpoint Security nu scanează fișierele din arhive. De exemplu, dacă fișierele imagine au fost plasate într-o arhivă, Kaspersky Endpoint Security identifică tipul de date *Arhive* și nu *Grafică*.

Regulile pot include o planificare a regulii și o listă de utilizatori cărora li se aplică regula. De exemplu, poți restricționa accesul la site-urile web numai în timpul orelor de lucru sau poți permite vizitarea site-urilor web de către utilizatorii din anumite grupuri.

Cum se activează un filtru de conținut al resursei web în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Security Controls** → **Control Web**.
4. Bifați caseta de selectare **Control Web**.
5. În blocul **Setări Control Web**, fă clic pe butonul **Adaugă**.
   Se deschide fereastra **Regulă de acces la resurse Web**.
6. Configurează regula de acces la resursele web:
   a. În câmpul **Nume**, introduceți numele regulii.
   b. În lista verticală **Filtrează conținutul**, selectează conținutul relevant:
      - **După categorii de conținut**. Puteți controla accesul utilizatorilor la resursele web în funcție de categorie (de exemplu, categoria *Rețele de socializare*).
      - **După tipuri de date**. Puteți controla accesul utilizatorilor la resursele web pe baza tipului specific de date al datelor publicate (de exemplu, *Grafică*).
      - **După categorii de conținut și tipuri de date**. Sunt activate filtrele după categoriile de conținut și după tipurile de date.

   După selectarea filtrelor, configurează parametrii filtrelor.

c. În lista verticală **Aplică utilizatorilor**, selectează filtrul relevant pentru utilizatori:

- **Pentru toți utilizatorii**. Control Web nu va filtra resursele web după adresă.
- **Pentru anumiți utilizatori sau pentru anumite grupuri**. Control Web va filtra numai adresele resurselor web din listă. Puteți introduce o adresă web sau puteți folosi măști. De asemenea, puteți exporta o listă de adrese de resurse web dintr-un fișier TXT. Poți selecta utilizatori în Active Directory, în lista de conturi din Kaspersky Security Center sau introducând manual un nume de utilizator local. Kaspersky recomandă utilizarea conturilor de utilizator locale numai în cazuri speciale, când nu este posibilă utilizarea conturilor de utilizator de domeniu.

d. În lista verticală **Acțiune**, selectează opțiunea:

- **Permite**. Componenta Control Web permite accesul la resurse web care corespund parametrilor regulii.
- **Blochează**. Componenta Control Web blochează accesul la resursele web care corespund parametrilor regulii și afișează un mesaj de acces refuzat la site-ul web.
- **Avertizează**. Atunci când utilizatorul încearcă să obțină acces la o resursă web care corespunde regulii, componenta Control Web afișează un avertisment care indică faptul că vizitarea resursei web este nerecomandată. Utilizând linkuri din mesajul de avertizare, utilizatorul poate obține acces la resursa Web solicitată.

e. În lista verticală **Planificare regulă**, selectează o planificare sau creează una nouă.

7. Dacă dorești ca, imediat după aplicarea politicii, componenta Control Web să încheie conexiunea cu resursa web interzisă, bifează caseta de selectare **Termină sesiunile browserului utilizatorului activ după aplicarea regulii**.

   Controlul web permite deconectarea imediată a resurselor web numai în browserele web. Pentru alte aplicații, Web Control restricționează doar conexiunile noi.

   În cazul în care caseta de selectare este debifată, componenta Control Web restricționează numai conexiunile noi la resursele web interzise. Componenta Control Web nu oprește conexiunile active.

8. Salvați-vă modificările.

Cum se activează un filtru de conținut al resurselor web în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Security Controls** → **Web Control**.
5. Duceți comutatorul **Web Control ENABLED** la poziția activat.
6. În blocul **Rules list**, fă clic pe butonul **Add**.

7. Configurează regula de acces la resursele web:

   a. În câmpul **Rule name**, introduceți numele regulii.

   b. Selectați starea **Enabled** pentru regula de acces la resursele web.

      Poți utiliza comutatorul pentru a dezactiva regula de acces la resursele web în orice moment.

   c. În secțiunea **Action**, selectați opțiunea relevantă:

      - **Allow**. Componenta Control Web permite accesul la resurse web care corespund parametrilor regulii.
      - **Block**. Componenta Control Web blochează accesul la resursele web care corespund parametrilor regulii și afișează un mesaj de acces refuzat la site-ul web.
      - **Inform**. Atunci când utilizatorul încearcă să obțină acces la o resursă web care corespunde regulii, componenta Control Web afișează un avertisment care indică faptul că vizitarea resursei web este nerecomandată. Utilizând linkuri din mesajul de avertizare, utilizatorul poate obține acces la resursa Web solicitată.

   d. În **Scope**, selectează **Content category**.

   e. Configurează filtrul de conținut:

      - **Content category**. Puteți controla accesul utilizatorilor la resursele web în funcție de categorie (de exemplu, categoria *Rețele de socializare*).
      - **Data type**. Puteți controla accesul utilizatorilor la resursele web pe baza tipului specific de date al datelor publicate (de exemplu, *Grafică*).

   f. În **User or group**, selectează utilizatorii cărora dorești ca Control Web să le aplice regula.

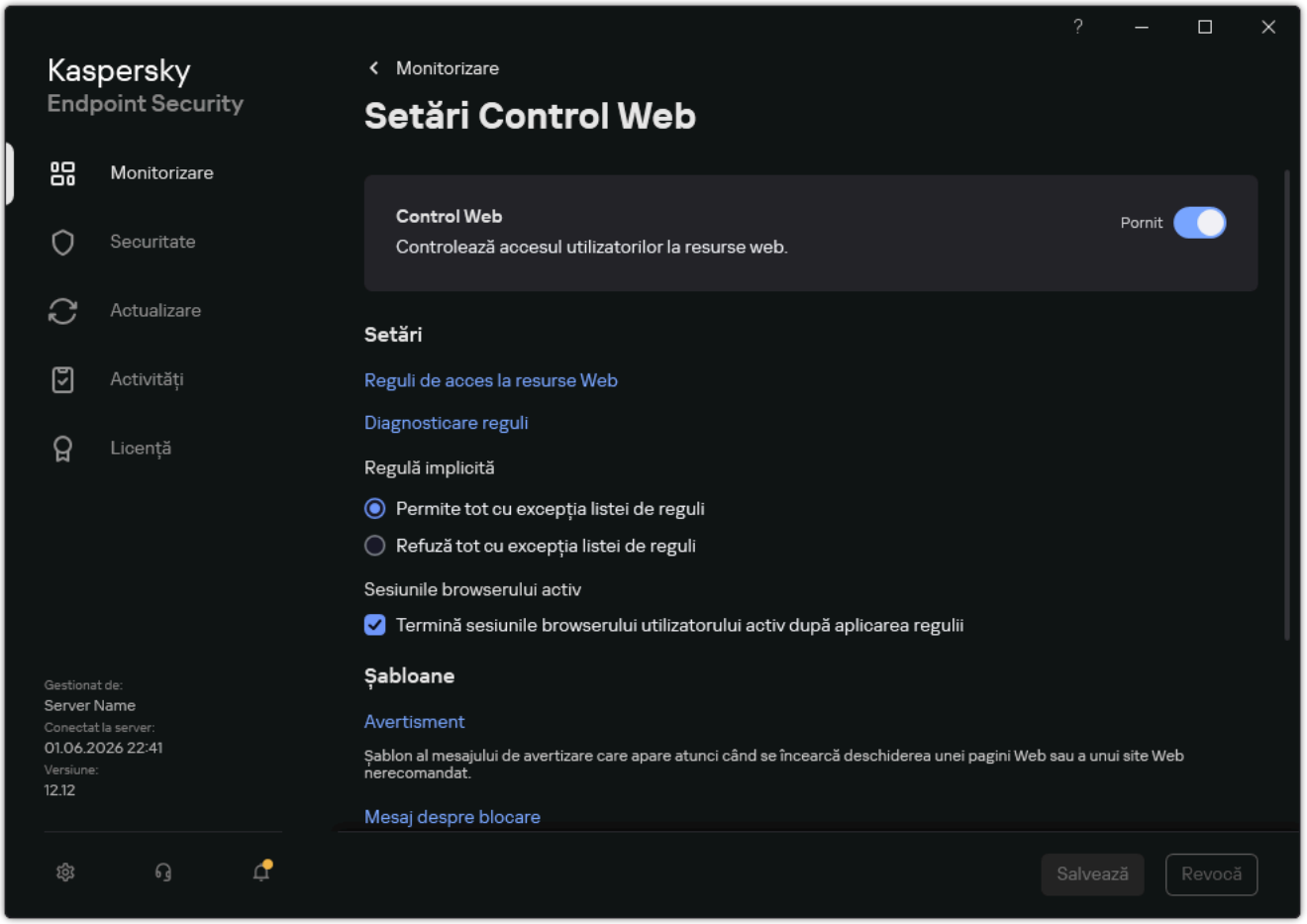
      Control Web va filtra numai adresele resurselor web din listă. Puteți introduce o adresă web sau puteți folosi măști. De asemenea, puteți exporta o listă de adrese de resurse web dintr-un fișier TXT. Poți selecta utilizatori în Active Directory, în lista de conturi din Kaspersky Security Center sau introducând manual un nume de utilizator local. Kaspersky recomandă utilizarea conturilor de utilizator locale numai în cazuri speciale, când nu este posibilă utilizarea conturilor de utilizator de domeniu.

   g. În blocul **Access schedule**, selectează o planificare sau creează una nouă.

8. Salvați-vă modificările.

Cum se activează un filtru de conținut al resursei web în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Security Controls** → **Control Web**.



Setări Control Web

3. În blocul **Setări**, fă clic pe butonul **Reguli de acces la resurse Web**.
4. În fereastra care se deschide, faceți clic pe butonul **Adaugă**.

   Se deschide fereastra **Regulă de acces la resurse Web**.
5. În câmpul **Nume regulă**, introduceți numele regulii.
6. Selectați starea **Pornită** pentru regula de acces la resursele web.

   Poți utiliza comutatorul pentru a dezactiva regula de acces la resursele web în orice moment.
7. În secțiunea **Acțiune**, selectați opțiunea relevantă:

   - **Permite**. Componenta Control Web permite accesul la resurse web care corespund parametrilor regulii.
   - **Blochează**. Componenta Control Web blochează accesul la resursele web care corespund parametrilor regulii și afișează un mesaj de acces refuzat la site-ul web.
   - **Avertizează**. Atunci când utilizatorul încearcă să obțină acces la o resursă web care corespunde regulii, componenta Control Web afișează un avertisment care indică faptul că vizitarea resursei web este nerecomandată. Utilizând linkuri din mesajul de avertizare, utilizatorul poate obține acces la resursa Web solicitată.

8. În blocul **Conținutul filtrului**, selectați filtrul de conținut relevant:

   - **După categorii de conținut**. Puteți controla accesul utilizatorilor la resursele web în funcție de categorie (de exemplu, categoria *Rețele de socializare*).
   - **După tipuri de date**. Puteți controla accesul utilizatorilor la resursele web pe baza tipului specific de date al datelor publicate (de exemplu, *Grafică*).

   Pentru a configura filtrul de conținut:

   a. Faceți clic pe linkul **Setări**.

   b. Bifați casetele de selectare de lângă numele categoriilor de conținut și/sau ale tipurilor de date necesare.

   Dacă bifezi caseta de selectare de lângă numele unei categorii de conținut și/sau de tip de date, aplicația Kaspersky Endpoint Security aplică regula de control al accesului resurselor Web care aparțin categoriilor de conținut și/sau tipurilor de date selectate.

   c. Reveniți la fereastră pentru configurarea regulii de acces la resursele web.

9. În blocul **Utilizatori**, selectați filtrul relevant pentru utilizatori:

   - **Pentru toți utilizatorii**. Control Web nu va filtra resursele web după adresă.
   - **Pentru utilizatori individuali și/sau grupuri individuale**. Control Web va filtra numai adresele resurselor web din listă. Puteți introduce o adresă web sau puteți folosi măști. De asemenea, puteți exporta o listă de adrese de resurse web dintr-un fișier TXT. Poți selecta utilizatori în Active Directory, în lista de conturi din Kaspersky Security Center sau introducând manual un nume de utilizator local. Kaspersky recomandă utilizarea conturilor de utilizator locale numai în cazuri speciale, când nu este posibilă utilizarea conturilor de utilizator de domeniu. Pentru a crea o listă de utilizatori cărora doriți să le aplicați regula:

     a. Fă clic pe **Adaugă**.

     b. În fereastra care se deschide, selectează utilizatorii sau grupurile de utilizatori cărora dorești să le aplici regula de acces la resursele web.

     c. Reveniți la fereastră pentru configurarea regulii de acces la resursele web.

10. În lista verticală **Planificare regulă**, selectați numele planificării necesare sau generează o planificare nouă bazată pe planificarea de regulă selectată. Pentru aceasta:

    a. Fă clic pe **Editează sau adaugă una nouă**.

    b. În fereastra care se deschide, faceți clic pe butonul **Adaugă**.

    c. În fereastra care se deschide, introduceți numele planificării regulii.

    d. Configurați programul de acces la resurse web pentru utilizatori.

    e. Reveniți la fereastră pentru configurarea regulii de acces la resursele web.

11. Dacă dorești ca, imediat după aplicarea politicii, componenta Control Web să încheie conexiunea cu resursa web interzisă, bifează caseta de selectare **Termină sesiunile browserului utilizatorului activ după aplicarea regulii**.

Controlul web permite deconectarea imediată a resurselor web numai în browserele web. Pentru alte aplicații, Web Control restricționează doar conexiunile noi.

În cazul în care caseta de selectare este debifată, componenta Control Web restricționează numai conexiunile noi la resursele web interzise. Componenta Control Web nu oprește conexiunile active.

12. Salvați-vă modificările.

Ca urmare, noua regulă Control Web este adăugată în listă. Dacă este necesar, modifică prioritatea regulii Control Web. De asemenea, poți utiliza comutatorul pentru a dezactiva regula de acces la resursele web în orice moment, fără a o elimina din listă.

Testarea regulilor de acces la resurse Web

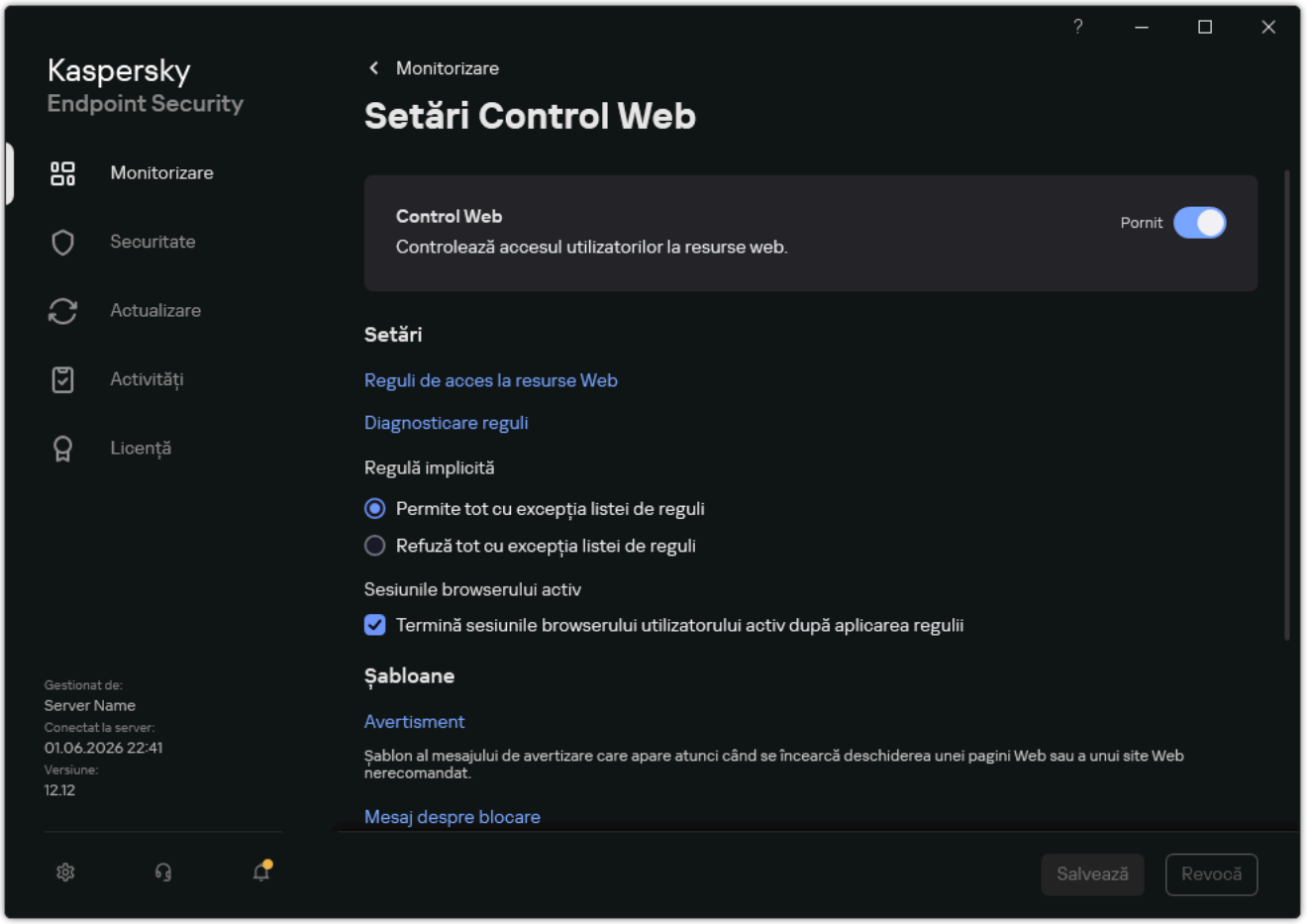
Atunci când configurezi Componenta Control Web, este posibil să blocați din greșeală accesul la resursele web de care utilizatorii au nevoie pentru activitatea lor. Pentru a afla care regulă Control Web blochează accesul la resursele web, poți utiliza instrumentul de *diagnosticare a Regulilor Control Web*. Diagnosticarea Regulilor Control Web este disponibilă numai în interfața Kaspersky Endpoint Security. În consola Kaspersky Security Center, nu poți afla ce regulă Control Web include o anumită resursă.

Dacă utilizatorul consideră că resursa Web este blocată în mod eronat, el poate face clic pe linkul din mesajul de notificare cu privire la blocarea resursei Web pentru a trimite un mesaj prestabilit către administratorul rețelei locale a companiei.

Pentru a testa regulile de acces la resurse Web:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Security Controls** → **Control Web**.



Setări Control Web

3. În blocul **Setări**, faceți clic pe linkul **Diagnosticare reguli**.

   Se deschide fereastra **Diagnosticare reguli**.

4. Dacă vrei să testezi regulile pe care Kaspersky Endpoint Security le folosește pentru a controla accesul la o anumită resursă web, bifează caseta de selectare **Specifică adresa**. Introdu adresa resursei web în câmpul de mai jos.

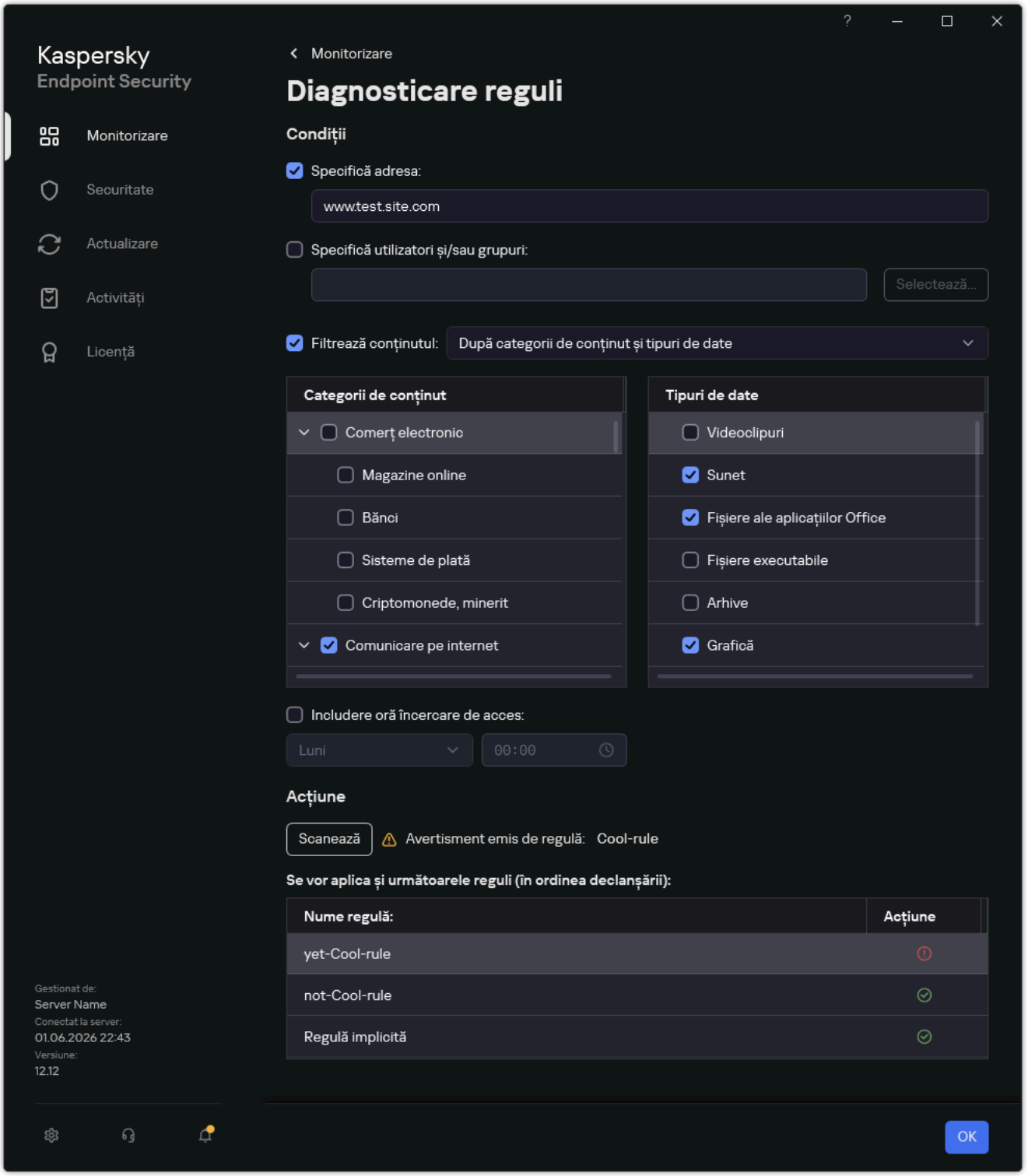
5. Dacă dorești să testezi regulile pe care aplicația Kaspersky Endpoint Security le utilizează pentru a controla accesul la resurse Web pentru anumiți utilizatori și/sau anumite grupuri de utilizatori, specifică o listă de utilizatori și/sau de grupuri de utilizatori.

6. Dacă doriți să testați regulile pe care aplicația Kaspersky Endpoint Security le utilizează pentru a controla accesul la resursele web cu anumite categorii de conținut și/sau categorii de tipuri de date, bifați caseta de selectare **Filtrează conținutul** și selectați opțiunea relevantă din lista verticală (**După categorii de conținut**, **După tipuri de date** sau **După categorii de conținut și tipuri de date**).

7. Dacă dorești să testezi regulile luând în considerare ora și ziua din săptămâna în care este efectuată o încercare de accesare a resurselor Web specificate în condițiile pentru diagnostice regulă, bifați caseta de selectare **Includere oră încercare de acces**. Apoi specifică ziua din săptămână și ora.

8. Fă clic pe **Scanează**.

După finalizarea testării se afișează un mesaj informativ cu privire la acțiunea efectuată de Kaspersky Endpoint Security, în funcție de prima regulă care se declanșează la încercarea de accesare a resurselor Web specificate (permitere, blocare sau avertizare). Prima regulă care se declanșează este cea a cărei poziție în lista de reguli a componentei Control Web este superioară pozițiilor celorlalte reguli care îndeplinesc condițiile de diagnosticare. Mesajul se afișează în dreapta butonului **Scanează**. Tabloul de mai jos prezintă regulile de declanșare rămase, specificând acțiunea luată de Kaspersky Endpoint Security. Regulile sunt listate în ordine descrescătoare a priorității.



Rezultatul testului de acces la resurse web

Exportul și importul regulilor Control Web

Poți exporta lista de reguli Control Web într-un fișier XML sau JSON. Apoi puteți modifica fișierul pentru a adăuga, de exemplu, un număr mare de adrese de același tip. Puteți utiliza funcția de export/import pentru a face o copie de rezervă a listei de reguli Control Web sau pentru a migra lista pe un alt server.

Cum se exportă și se importă o listă de reguli Control Web în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Security Controls → Control Web**.
4. Pentru a exporta lista de reguli Control Web:
   a. Selectați regulile pe care doriți să le exportați. Pentru a selecta mai multe porturi, utilizați tastele **CTRL** sau **SHIFT**.
      Dacă nu ați selectat nicio regulă, Kaspersky Endpoint Security va exporta toate regulile.
   b. Faceți clic pe linkul **Exportă**.
   c. În fereastra care se deschide, specificați numele fișierului XML în care doriți să exporți lista de reguli și selectați directorul în care doriți să salvați acest fișier.
   d. Salvați fișierul.
      Kaspersky Endpoint Security exportă lista de reguli în fișierul XML.
5. Pentru a importa lista de reguli Control Web:
   a. Faceți clic pe linkul **Importă**.
      În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de reguli.
   b. Deschideți fișierul.
      În cazul în care computerul are deja o listă de reguli, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul XML.
6. Salvați-vă modificările.

Cum se exportă și se importă o listă de reguli Control Web în Consola Web și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management → Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.
   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Security Controls → Web Control**.

5. Pentru a exporta lista de reguli, în blocul **Rules list**:

   a. Selectați regulile pe care doriți să le exportați.

   b. Fă clic pe butonul → **Export**.

      Kaspersky Endpoint Security exportă lista de reguli într-un fișier JSON în directorul de descărcări implicit.

6. Pentru a importa lista de reguli, în blocul **Rules list**:

   a. Fă clic pe butonul → **Import**.

      În fereastra care se deschide, selectați fișierul JSON din care doriți să importați lista de reguli.

   b. Deschideți fișierul.

      În cazul în care computerul are deja o listă de reguli, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul JSON.

7. Salvați-vă modificările.

Exportul și importul adreselor resurselor web ale regulii Control Web

Dacă ai creat o listă de adrese de resurse Web într-o regulă de acces la resurse Web, poți exporta această listă într-un fișier:

- În format TXT în Consola de administrare (MMC)
- În format CSV în interfața aplicației

Ulterior, poți importa lista din acest fișier pentru a evita crearea manuală a unei liste noi de adrese de resurse Web la configurarea unei reguli de acces. Opțiunea de a exporta și, ulterior, de a importa lista de adrese de resurse Web poate fi utilă dacă, de exemplu, creezi reguli de acces cu parametri similari.

De asemenea, poți exporta/importa toate regulile Control Web și nu doar adresele de resurse web ale unei reguli individuale.

> Nu poți exporta/importa adresele de resurse web ale unei reguli Control Web în Web Console sau Cloud Console.

Cum se exportă/importă adresele resurselor web ale regulii Control Web în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Security Controls** → **Control Web**.
4. În blocul **Setări Control Web**, selectează regula a cărei listă de adrese de resurse web dorești să o exporți sau să o importi.

   Sunt afișate proprietățile regulilor Control Web.

5. Pentru a exporta lista de resurse web, efectuează următoarele acțiuni în lista de adrese:

   a. Selectați adresele pe care doriți să le exportați.

      Dacă nu ați selectat nicio adresă, Kaspersky Endpoint Security va exporta toate adresele.

   b. Fă clic pe butonul .

   c. În fereastra care se deschide, introdu numele fișierului TXT în care dorești să exporți lista cu adresele resurselor web și selectează directorul în care dorești să salvezi acest fișier.

   d. Salvați fișierul.

      Kaspersky Endpoint Security exportă lista de adrese de resurse web într-un fișier TXT.

6. Pentru a importa lista de resurse web, efectuează următoarele acțiuni în lista de adrese:

   a. Fă clic pe butonul .

      În fereastra care se deschide, selectați fișierul TXT din care doriți să importați lista de resurse web.

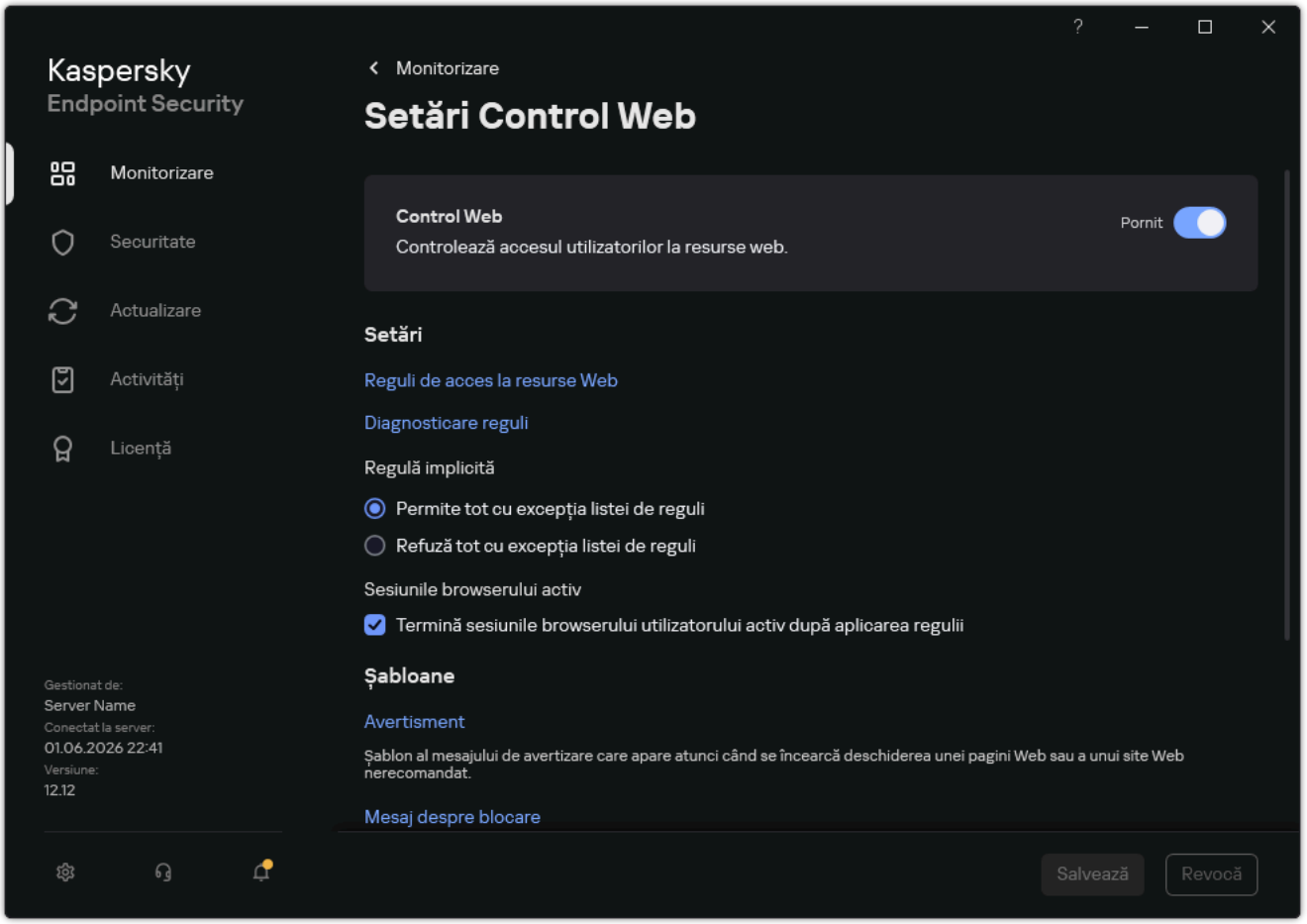
   b. Deschideți fișierul.

      În cazul în care computerul are deja o listă de adrese, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul TXT.

7. Salvați-vă modificările.

Cum se exportă/importă adresele resurselor web ale regulii Control Web în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Security Controls** → **Control Web**.



Setări Control Web

3. În blocul **Setări**, fă clic pe butonul **Reguli de acces la resurse Web**.
4. Selectați regula a cărei listă de adrese de resurse web doriți să o exportați sau importați.
5. Pentru a exporta lista de adrese web de încredere, efectuați următoarele în blocul **Adrese**:
   a. Selectați adresele pe care doriți să le exportați.
      Dacă nu ați selectat nicio adresă, Kaspersky Endpoint Security va exporta toate adresele.
   b. Fă clic pe **Exportă**.
   c. În fereastra care se deschide, introdu numele fișierului CSV în care dorești să exporți lista cu adresele resurselor web și selectează directorul în care dorești să salvezi acest fișier.
   d. Salvați fișierul.
      Kaspersky Endpoint Security exportă lista de adrese de resurse web într-un fișier CSV.
6. Pentru a importa lista resurselor web, efectuați următoarele în blocul **Adrese**:
   a. Fă clic pe **Importă**.
      În fereastra care se deschide, selectați fișierul CSV din care doriți să importați lista de resurse web.

b. Deschideți fișierul.

În cazul în care computerul are deja o listă de adrese, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul CSV.

7. Salvați-vă modificările.

Monitorizarea activității pe Internet a utilizatorilor

Kaspersky Endpoint Security vă permite să înregistrați în jurnal datele privind vizitele utilizatorilor pe toate site-urile web, inclusiv pe site-urile permise. Acest lucru vă permite să obțineți istoricul complet al vizualizărilor browserului. Kaspersky Endpoint Security trimite evenimentele de activitate a utilizatorului către Kaspersky Security Center, în jurnalul local al Kaspersky Endpoint Security și în Jurnalul de evenimente Windows. Pentru a primi evenimente în Kaspersky Security Center, trebuie să configurați setările evenimentelor într-o politică din Consola de administrare sau Consola Web. Puteți configura, de asemenea, transmiterea evenimentelor componentei Control Web prin e-mail și afișarea notificărilor pe ecran pe computerul utilizatorului.

Browsere care acceptă funcția de monitorizare: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Yandex Browser, Mozilla Firefox. Monitorizarea activității utilizatorului nu funcționează în alte browsere.

Kaspersky Endpoint Security creează următoarele evenimente de activitate pe Internet a utilizatorilor:

- Blocare site web (starea *Critical*).
- Vizitarea unui site web nerecomandat (stare *Warning*).
- Vizită pe un site web permis (stare *Info*).

Înainte de a activa monitorizarea activității pe Internet a utilizatorului, trebuie să faceți următoarele:

- Injectați un script de interacțiune a paginii web în traficul web (consultați instrucțiunile de mai jos). Scriptul permite înregistrarea evenimentelor Control Web.
- Pentru monitorizarea traficului HTTPS, trebuie să activați scanarea conexiunilor securizate.

Injectarea unui script de interacțiune a paginii web

Cum se injectează un script de interacțiune a paginii web în traficul web în Consola de administrare (MMC)

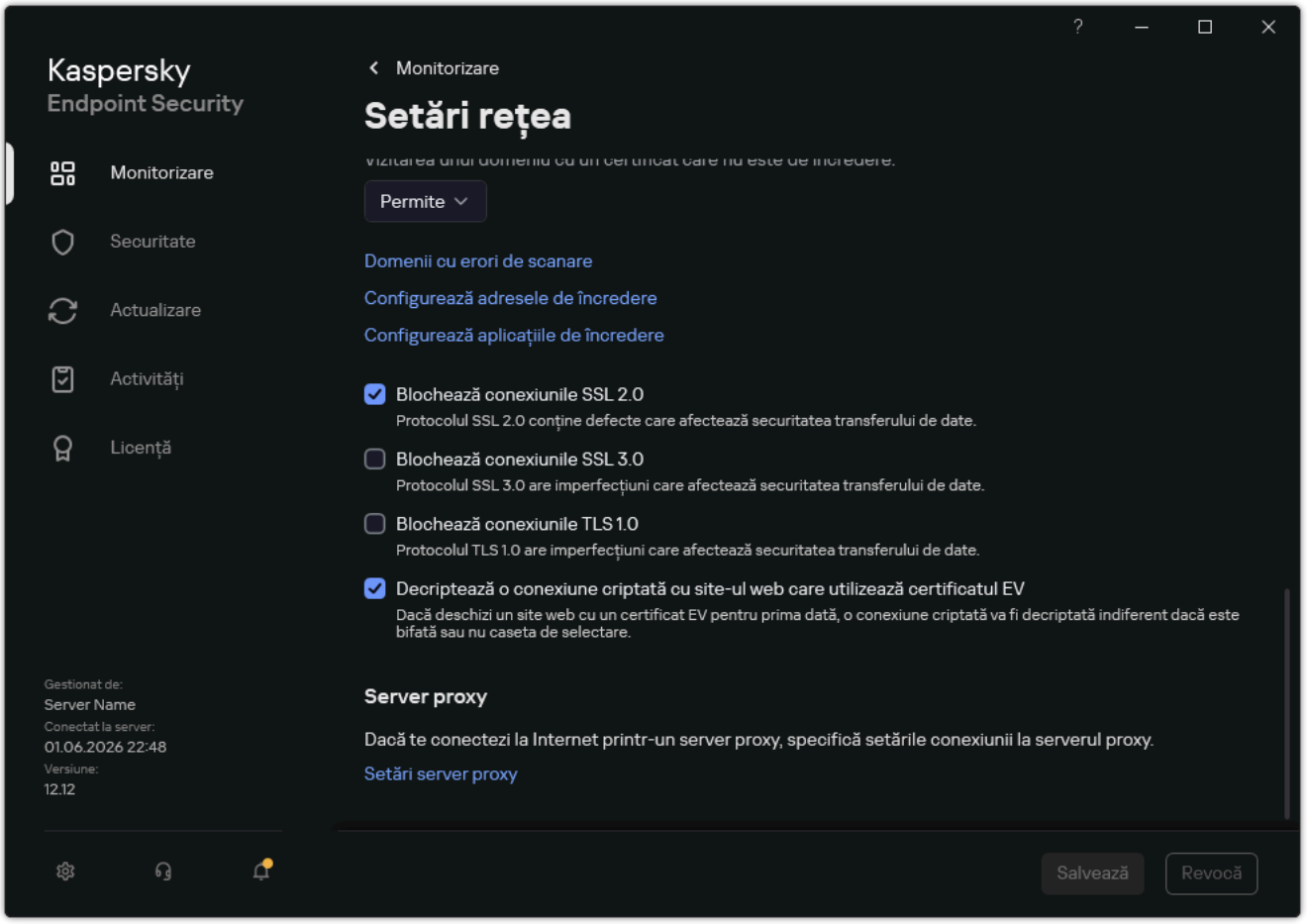
1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Setări generale** → **Setări rețea**.
4. În blocul **Scanare conexiuni criptate**, bifați caseta de selectare **Injectează segmente de script în traficul web pentru a interacționa cu paginile web**.
5. Salvați-vă modificările.

Cum se injectează un script de interacțiune a paginii web în traficul web în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.
   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. În fereastra politicii, selectați **General Settings** → **Network Settings**.
5. În **Monitoring of internet connections**, activează comutatorul **Monitoring of internet connections ENABLED**.
6. Salvați-vă modificările.

Cum se injectează un script de interacțiune a paginii web în traficul web în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Setări generale** → **Setări rețea**.



Setări de rețea pentru aplicație

3. În blocul **Procesare trafic**, bifați caseta de selectare **Injectează segmente de script în traficul web pentru a interacționa cu paginile web**.
4. Salvați-vă modificările.

Drept urmare, Kaspersky Endpoint Security va injecta un script de interacțiune a paginii web în traficul web. Acest script permite înregistrarea evenimentelor Control Web pentru jurnalul de evenimente al aplicației, jurnalul de evenimente al sistemului de operare și rapoarte.

Configurarea înregistrării în jurnal a evenimentelor componentei Control Web

Pentru a configura înregistrarea în jurnal a evenimentelor componentei Control Web pe computerul utilizatorului:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Setări generale** → **Interfață**.
3. În blocul **Notificări**, fă clic pe butonul **Configurează notificările**.
4. În fereastra care se deschide, selectați secțiunea **Control Web**.

   Aceasta deschide tabelul evenimentelor componentei Control Web și a metodelor de notificare.
5. Configurați metoda de notificare pentru fiecare eveniment: **Salvează în raportul local** sau **Salvează în Jurnal evenimente Windows**.

   Pentru a înregistra în jurnal evenimentele permise de vizitare a site-ului web, trebuie să configurați și componenta Control Web (consultați instrucțiunile de mai jos).

   În tabelul de evenimente, puteți activa, de asemenea, o notificare pe ecran și o notificare prin e-mail. Pentru a trimite notificări prin e-mail, trebuie să configurați setările serverului SMTP. Pentru mai multe detalii despre trimiterea notificărilor prin e-mail, consultați Ajutor pentru Kaspersky Security Center.
6. Salvați-vă modificările.

Drept urmare, Kaspersky Endpoint Security începe să înregistreze în jurnal evenimente de activitate pe Internet a utilizatorului.

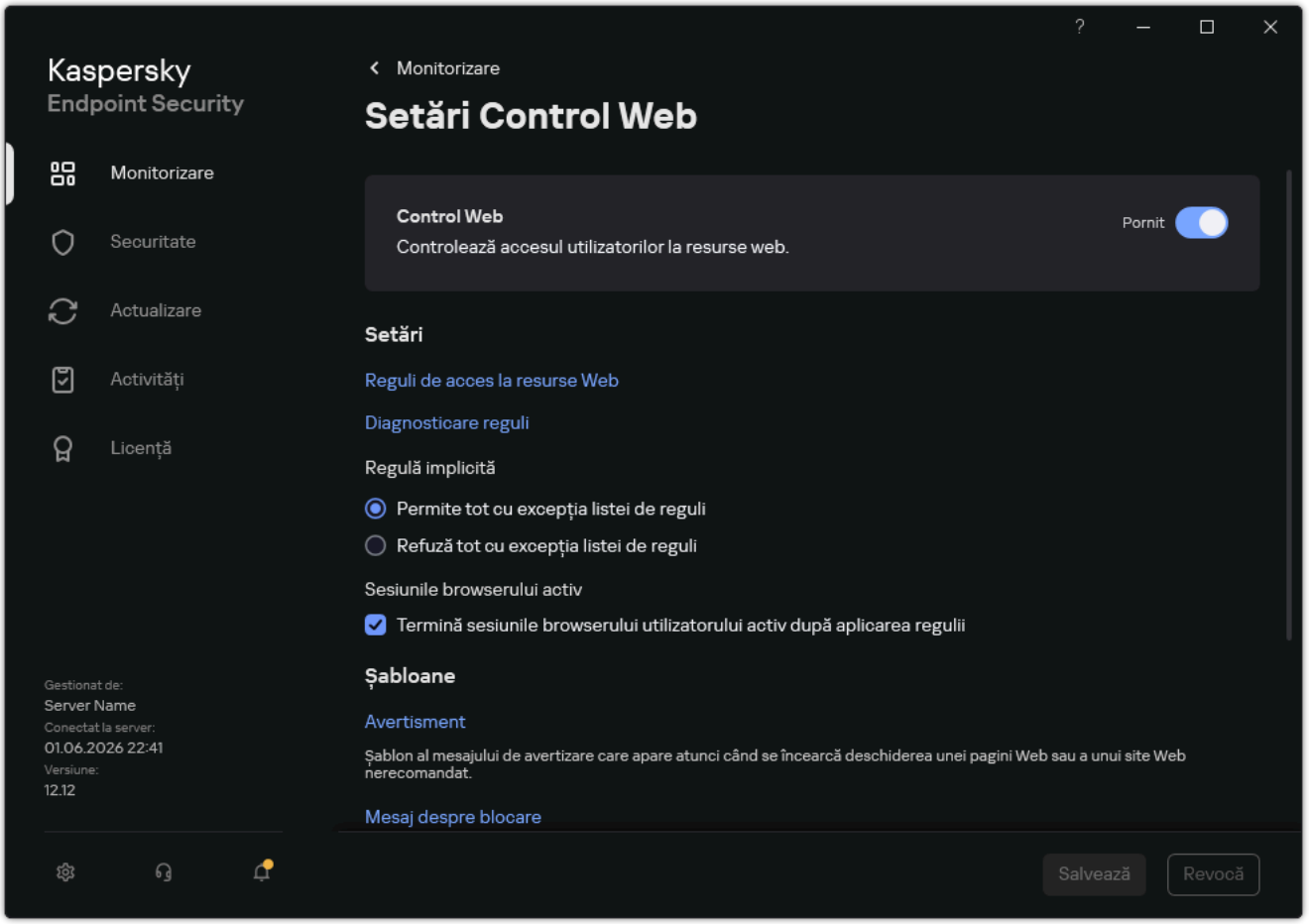
Web Control trimite evenimentele de activitate ale utilizatorului către Kaspersky Security Center după cum urmează:

- Dacă utilizați Kaspersky Security Center, Web Control trimite evenimentele pentru toate obiectele care alcătuiesc pagina web. Din acest motiv, mai multe evenimente pot fi create atunci când o pagină web este blocată. De exemplu, atunci când se blochează pagina web http://www.example.com, Kaspersky Endpoint Security poate transmite evenimente pentru următoarele obiecte: http://www.example.com, http://www.example.com/icon.ico, http://www.example.com/file.js, etc.
- Dacă utilizați Kaspersky Security Center Cloud Console, Web Console grupează evenimentele și trimite doar protocolul și domeniul site-ului web. De exemplu, dacă un utilizator vizitează paginile web nerecomandate http://www.example.com/main, http://www.example.com/contact, http://www.example.com/gallery, Kaspersky Endpoint Security va trimite un singur eveniment cu obiectul http://www.example.com.

Înregistrarea în jurnal a evenimentelor la vizitarea site-urilor web permise

Pentru a activa înregistrarea în jurnal a evenimentelor la vizitarea site-urilor web permise:

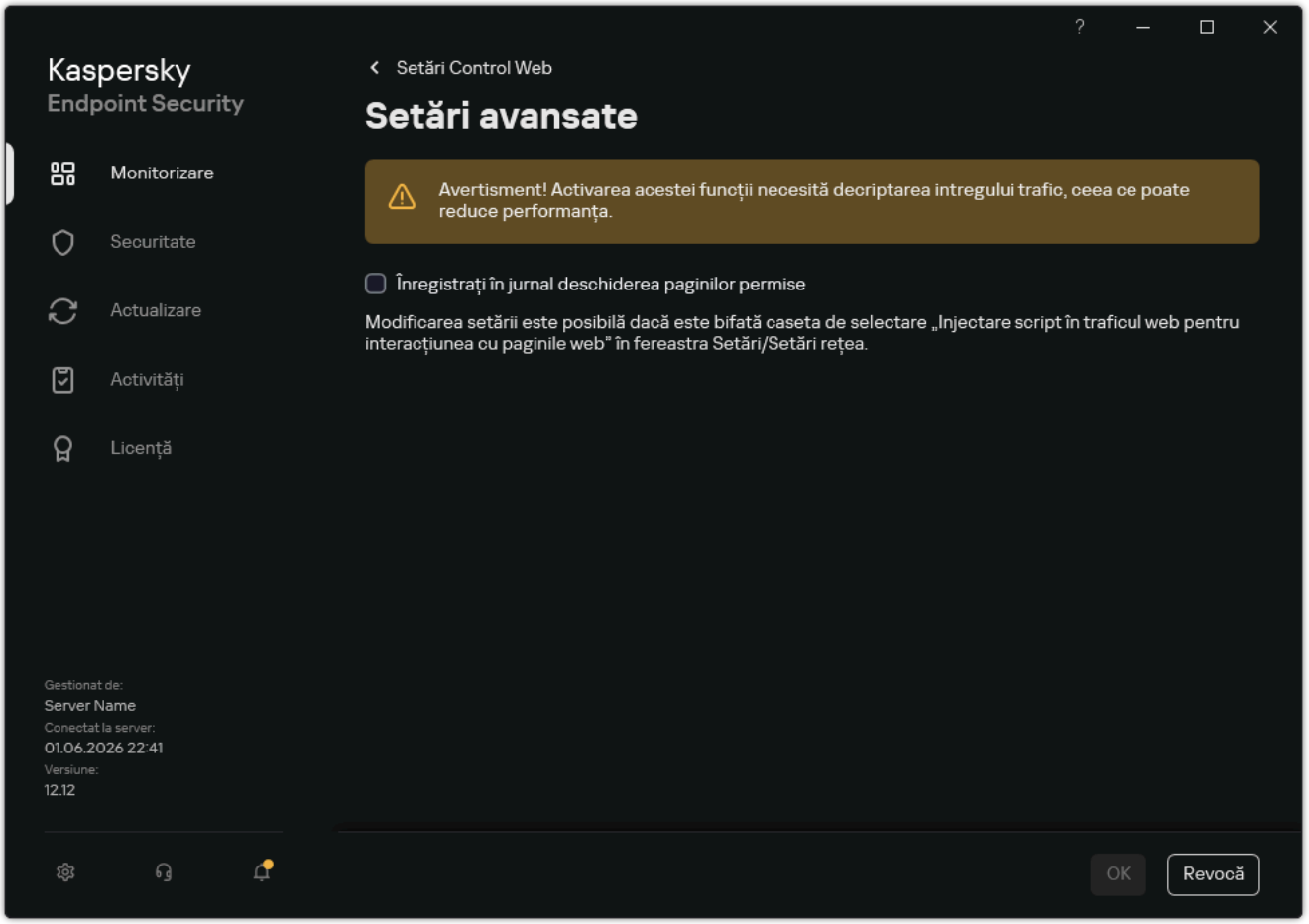
1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Security Controls** → **Control Web**.



Setări Control Web

3. În blocul **Suplimentar**, fă clic pe butonul **Setări avansate**.

4. În fereastra care se deschide, bifați caseta de selectare **Înregistrați în jurnal deschiderea paginilor permise**.



Setări avansate Control Web.

5. Salvați-vă modificările.

Drept urmare, veți putea vizualiza istoricul complet al browserului.

Editarea șabloanelor de mesaje ale componentei Control Web

În funcție de tipul de acțiune specificată în proprietățile regulilor pentru componenta Control Web, Kaspersky Endpoint Security afișează unul dintre următoarele tipuri de mesaje atunci când utilizatorii încearcă să acceseze resurse de pe Internet (aplicația înlocuiește o pagină HTML cu un mesaj pentru răspunsul din partea serverului HTTP):

- Mesaj de avertizare. Acest mesaj îl avertizează pe utilizator că vizitarea resursei Web nu se recomandă și/sau violează politica de securitate a companiei. Kaspersky Endpoint Security afișează un mesaj de avertizare dacă opțiunea **Avertizează** este selectată în setările regulii care descrie această resursă web.

  Dacă utilizatorul consideră că avertizarea este eronată, el poate face clic pe linkul din avertizare pentru a trimite un mesaj prestabilit către administratorul rețelei locale a companiei.

- Mesaj informativ cu privire la blocarea unei resurse Web. Kaspersky Endpoint Security afișează un mesaj informativ cu privire la blocarea unei resurse web (consultă figura de mai jos) dacă opțiunea **Blochează** este selectată în setările regulii care descrie această resursă web.

Dacă utilizatorul consideră că resursa Web este blocată în mod eronat, el poate face clic pe linkul din mesajul de notificare cu privire la blocarea resursei Web pentru a trimite un mesaj prestabilit către administratorul rețelei locale a companiei.



Mesaj despre blocarea resurselor web

Pentru mesajul de avertizare, pentru mesajul informativ cu privire la blocarea unei resurse Web și pentru mesajul trimis către administratorul rețelei LAN sunt furnizate șabloane speciale. Sunt furnizate variabile speciale pentru gestionarea șabloanelor pentru mesaje (de exemplu, `%USER_NAME%`). Variabilele permit utilizarea unui singur șablon de mesaj pentru computere diferite. La generarea unui mesaj, Kaspersky Endpoint Security preia valoarea variabilei din setările sistemului de operare și o inserează în mesajul corespunzător computerului, utilizatorului și evenimentului specific.

Cum se schimbă șablonul de mesaj al componentei Control web în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Security Controls** → **Control Web**.
4. În blocul **Setări șablon de mesaje**, fă clic pe butonul **Șabloane**.

5. Configurați șabloanele de mesaje pentru Control web:

   - **Avertisment**. Câmpul de intrare conține șablonul mesajului care se afișează dacă se declanșează o regulă sau o avertizare despre încercări de accesare a unei resurse Web nedorite.

   - **Mesaj despre blocare**. Câmpul de introducere conține șablonul mesajului care apare dacă se declanșează o regulă care blochează accesul la o resursă web.

   - **Mesaj către administrator**. Șablonul mesajului care va fi trimis administratorului rețelei LAN în cazul în care utilizatorul consideră că blocarea s-a făcut din greșeală. După ce utilizatorul solicită accesul, Kaspersky Endpoint Security trimite un eveniment către Kaspersky Security Center: **Mesaj către administrator privind blocarea accesului la paginile Web**. Descrierea evenimentului conține un mesaj către administrator cu variabile înlocuite. Puteți vizualiza aceste evenimente în consola Kaspersky Security Center, utilizând selecția de evenimente predefinită **User requests**. Dacă organizația dvs. nu are instalat Kaspersky Security Center sau nu există nicio conexiune la serverul de administrare, aplicația va trimite un mesaj administratorului la adresa de e-mail specificată.

   Pentru a adăuga o variabilă la textul șablonului, plasează cursorul în poziția dorită, fă clic pe **Variabilă** și selectează variabila necesară din lista de opțiuni disponibile.

   De asemenea, poți restaura textul șablonului implicit utilizând butonul **În mod implicit**.

6. Salvați-vă modificările.

Cum se schimbă șablonul de mesaj al componentei Control web în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **Security Controls** → **Web Control**.

5. În blocul **Message templates**, fă clic pe linkul **Message about website blocking** și configurează șabloanele pentru mesajele componentei Control Web:

   - **Warning**. Câmpul de intrare conține șablonul mesajului care se afișează dacă se declanșează o regulă sau o avertizare despre încercări de accesare a unei resurse Web nedorite.

   - **Message about blocking**. Câmpul de introducere conține șablonul mesajului care apare dacă se declanșează o regulă care blochează accesul la o resursă web.

   - **Message to administrator**. Șablonul mesajului care va fi trimis administratorului rețelei LAN în cazul în care utilizatorul consideră că blocarea s-a făcut din greșeală. După ce utilizatorul solicită accesul, Kaspersky Endpoint Security trimite un eveniment către Kaspersky Security Center: **Mesaj către administrator privind blocarea accesului la paginile Web**. Descrierea evenimentului conține un mesaj către administrator cu variabile înlocuite. Puteți vizualiza aceste evenimente în consola Kaspersky Security Center, utilizând selecția de evenimente predefinită **User requests**. Dacă organizația dvs. nu are instalat Kaspersky Security Center sau nu există nicio conexiune la serverul de administrare, aplicația va trimite un mesaj administratorului la adresa de e-mail specificată.

   Pentru a adăuga o variabilă la textul șablonului, plasează cursorul în poziția dorită, fă clic pe **Add variable** și selectează variabila necesară din lista de opțiuni disponibile.

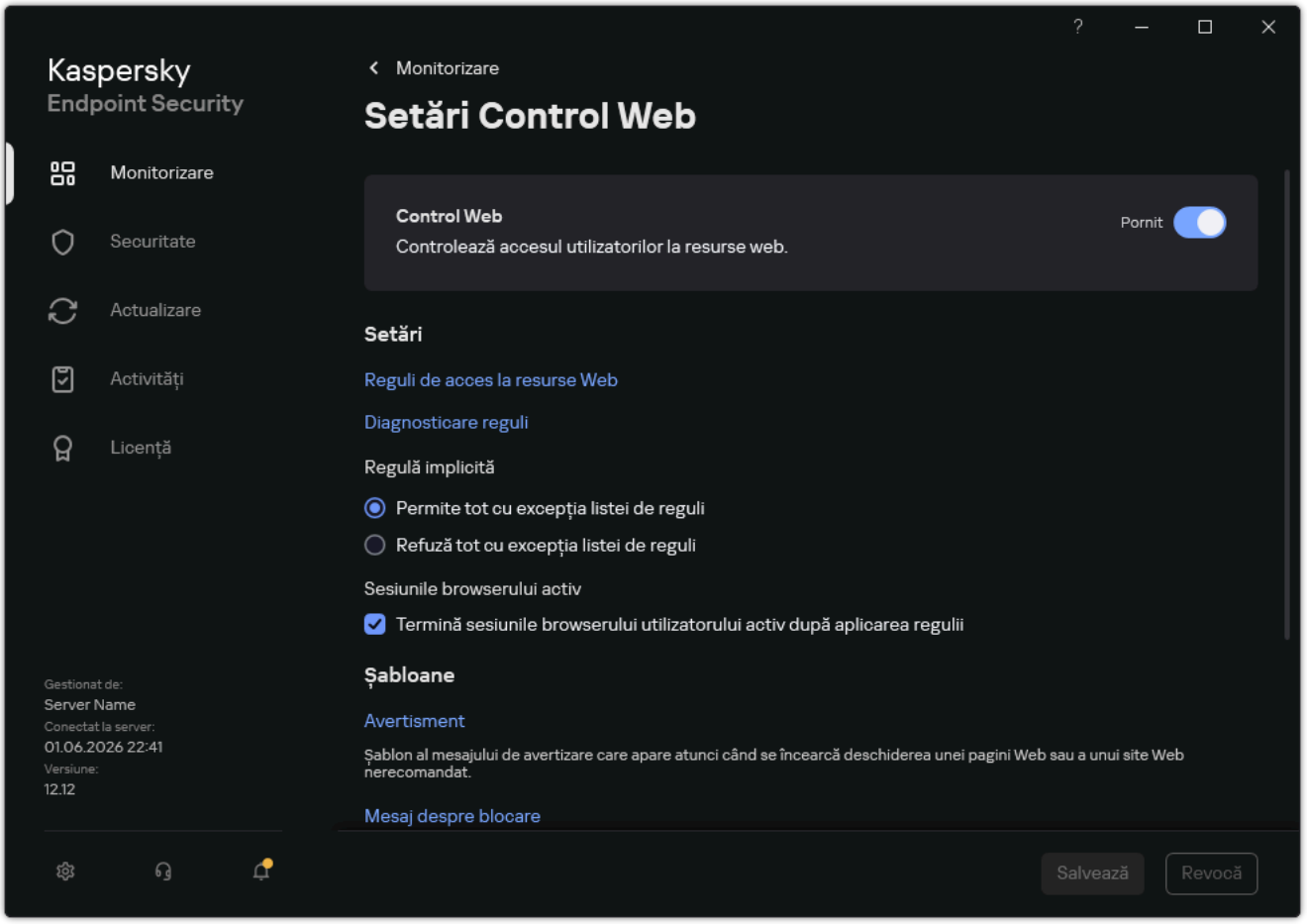
De asemenea, poți restaura textul șablonului implicit utilizând butonul **Reset to default**.

6. Salvați-vă modificările.

Cum se schimbă șablonul de mesaj al componentei Control web în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Security Controls** → **Control Web**.



Setări Control Web

3. În blocul **Șabloane**, configurați șabloanele pentru mesajele Control Web:

- **Avertisment**. Câmpul de intrare conține șablonul mesajului care se afișează dacă se declanșează o regulă sau o avertizare despre încercări de accesare a unei resurse Web nedorite.
- **Mesaj despre blocare**. Câmpul de introducere conține șablonul mesajului care apare dacă se declanșează o regulă care blochează accesul la o resursă web.
- **Mesaj către administrator**. Șablonul mesajului care va fi trimis administratorului rețelei LAN în cazul în care utilizatorul consideră că blocarea s-a făcut din greșeală. După ce utilizatorul solicită accesul, Kaspersky Endpoint Security trimite un eveniment către Kaspersky Security Center: **Mesaj către administrator privind blocarea accesului la paginile Web**. Descrierea evenimentului conține un mesaj către administrator cu variabile înlocuite. Puteți vizualiza aceste evenimente în consola Kaspersky Security Center, utilizând selecția de evenimente predefinită **User requests**. Dacă organizația dvs. nu are instalat Kaspersky Security Center sau nu există nicio conexiune la serverul de administrare, aplicația va trimite un mesaj administratorului la adresa de e-mail specificată.

Pentru a adăuga o variabilă la textul șablonului, plasează cursorul în poziția dorită, fă clic pe **Adaugă variabilă** și selectează variabila necesară din lista de opțiuni disponibile.

De asemenea, poți restaura textul șablonului implicit utilizând butonul **Resetează**.

4. Salvați-vă modificările.

Editarea măștilor pentru adrese de resurse Web

Utilizarea unei *măști pentru adrese de resurse Web* (denumită și „mască de adresă") poate fi utilă dacă ai nevoie să introduci multe adrese de resurse Web similare la crearea unei reguli de accesare a resurselor Web. Dacă este bine construită, o mască de adresă poate înlocui un număr mare de adrese de resurse Web.

Atunci când creați o mască de adresă, respectați aceste reguli:

1. Caracterul `*` înlocuiește orice secvență care conține zero sau mai multe caractere.

   De exemplu, dacă introduceți masca de adrese `*abc*`, regula de acces este aplicată tuturor resurselor Web care conțin secvența `abc`. Exemplu: `http://www.example.com/page_0-9abcdef.html`.

2. O secvență de caractere `*.` (cunoscută și ca *mască de domeniu*) vă permite să selectați toate domeniile unei adrese. Masca de domeniu `*.` reprezintă orice nume de domeniu, subdomeniu sau o linie goală.

   Exemplu: masca `*.example.com` reprezintă următoarele adrese:

   - `http://pictures.example.com`. Masca de domeniu `*.` reprezintă `pictures.`.
   - `http://user.pictures.example.com`. Masca de domeniu `*.` reprezintă `pictures.` și `user.`.
   - `http://example.com`. Masca de domeniu `*.` este interpretată ca o linie goală.

3. Secvența de caractere `www.` de la începutul unei măști de adrese este interpretată ca o secvență `*.`.

   Exemplu: masca de adresă `www.example.com` este tratată ca `*.example.com`. Această mască acoperă adresele `www2.example.com` și `www.pictures.example.com`.

4. Dacă o mască de adrese nu are la început caracterul `*`, conținutul măștii de adrese este echivalent cu același conținut cu prefixul `*.`

5. Dacă o mască de adresă se termină cu alt caracter decât `/` sau `*`, conținutul măștii de adresă este echivalent cu același conținut cu postfixul `/*`.

   Exemplu: masca de adresă `http://www.example.com` acoperă adrese precum `http://www.example.com/abc`, unde `a`, `b` și `c` sunt orice caractere.

6. Dacă o mască de adresă are la sfârșit caracterul `/`, conținutul măștii de adresă este echivalent cu același conținut cu postfixul `/*`.

7. Secvența de caractere `/*` la sfârșitul unei măști de adrese este interpretată ca `/*` sau ca un șir necompletat.

8. Adresele de resurse Web sunt comparate cu o mască de adrese, luându-se în considerare protocolul (http sau https):

   - Dacă masca de adrese nu conține niciun protocol de rețea, această mască de adrese acoperă adresele fără niciun protocol de rețea.

     Exemplu: masca de adresă `example.com` acoperă adresele `http://example.com` și `https://example.com`.

- Dacă masca de adrese conține un protocol de rețea, această mască de adrese acoperă numai adresele cu același protocol de rețea ca și masca de adrese.

  Exemplu: masca de adresă `http://*.example.com` acoperă adresa `http://www.example.com`, însă nu acoperă `https://www.example.com`.

9. O mască de adresă încadrată între ghilimele este tratată fără a se lua în considerare alte înlocuiri suplimentare, cu excepția caracterului `*` în cazul în care a fost inclus inițial în masca de adresă. Regulile 5 și 7 nu se aplică pentru măștile de adresă încadrate între ghilimele duble (vezi exemplele 14 – 18 din tabelul de mai jos).

10. Numele de utilizator și parola, portul de conectare și tipul majusculă/minusculă al caracterului nu sunt luate în considerare la compararea cu masca de adrese a unei resurse Web.

Exemple de moduri de utilizare a regulilor pentru crearea măștilor de adrese

Nr.	Mască de adresă	Adresă resursă Web de verificat	Este adresa acoperită de masca de adrese	Comentariu
1	*.example.com	http://www.123example.com	Nu	Vezi regula 1.
2	*.example.com	http://www.123.example.com	Da	Vezi regula 2.
3	*example.com	http://www.123example.com	Da	Vezi regula 1.
4	*example.com	http://www.123.example.com	Da	Vezi regula 1.
5	http://www.*.example.com	http://www.123example.com	Nu	Vezi regula 1.
6	www.example.com	http://www.example.com	Da	Vezi regulile 3, 2, 1.
7	www.example.com	https://www.example.com	Da	Vezi regulile 3, 2, 1.
8	http://www.*.example.com	http://123.example.com	Da	Vezi regulile 3, 4, 1.
9	www.example.com	http://www.example.com/abc	Da	Vezi regulile 3, 5, 1.
10	example.com	http://www.example.com	Da	Vezi regulile 3, 1.
11	http://example.com/	http://example.com/abc	Da	Vezi regula 6.
12	http://example.com/*	http://example.com	Da	Vezi regula 7.
13	http://example.com	https://example.com	Nu	Vezi regula 8.
14	"example.com"	http://www.example.com	Nu	Vezi regula 9.
15	"http://www.example.com"	http://www.example.com/abc	Nu	Vezi regula 9.
16	"*.example.com"	http://www.example.com	Da	Vezi regulile 1, 9.
17	"http://www.example.com/*"	http://www.example.com/abc	Da	Vezi regulile 1, 9.
18	"www.example.com"	http://www.example.com; https://www.example.com	Da	Vezi regulile 9, 8.
19	www.example.com/abc/123	http://www.example.com/abc	Nu	O mască de adrese conține mai multe informații decât adresa unei resurse Web.

Control web pentru mașini virtuale

Componenta Control web controlează traficul pe computer, precum și pe o mașină virtuală care este implementată local pe computer. Acest lucru funcționează fără a fi nevoie să instalați aplicația Kaspersky Endpoint Security pe mașina virtuală locală. Aceasta înseamnă că, dacă utilizatorul încearcă să deschidă un site web care este blocat de o regulă Control web într-un browser de pe *mașina virtuală*, aplicația instalată pe sistemul de operare gazdă al *computerului* interzice accesul la acel site web.

Componenta Control web funcționează diferit pe diferite mașini virtuale.

Oracle VM VirtualBox

Kaspersky Endpoint Security acceptă regulile Control web pe mașinile virtuale Oracle VM VirtualBox fără limitări. Aplicația poate controla tot traficul mașinii virtuale. Dacă este configurat un filtru de utilizator în regulile Control web, aplicația funcționează corect deoarece toate procesele mașinilor virtuale sunt pornite de utilizatorul local.

VMware Workstation

Kaspersky Endpoint Security acceptă regulile Control web pe mașinile virtuale VMware Workstation fără limitări. Aplicația nu acceptă reguli cu un filtru configurat de utilizator. Procesele mașinii virtuale se execută sub utilizatorul sistemului (SYSTEM). Acest lucru face imposibilă identificarea utilizatorului care încearcă să deschidă site-ul web pe mașina virtuală.

Microsoft Hyper-V

Kaspersky Endpoint Security nu acceptă regulile Control web pe mașinile virtuale Microsoft Hyper-V.

Variabile în șabloanele de mesaje pentru Control Web

Poți utiliza următoarele variabile în șabloanele de mesaje pentru utilizatori sau în șabloanele de mesaje pentru administratori:

- **User** – `%USER_NAME%`.

  Numele contului de utilizator curent de pe computerul pe care a fost generat mesajul, în formatul `<device name>\<user alias>` (de exemplu, `DESKTOP-123\John.Smith`).

- **Web resource address** – `%CANONIC_REQUEST_URL%`.

  Adresa resursei web blocate.

- **Rule name** – `%RULE%`.

  Numele regulii care a blocat resursa web.

- **Email for sending a message** – `%COMPLAIN_EMAIL%`.

  Adresa de e-mail pentru feedback despre blocurile de resurse web. Făcând clic pe adresa de e-mail, se deschide o fereastră în care utilizatorul poate scrie un mesaj către administrator.

- **Name of content category** – `%CONTENT_CATEGORY_LIST%`.

  Categoria de site web căreia îi aparține resursa blocată (de exemplu, *Payment systems*).

- **Name of data type category** – `%TYPE_CATEGORY_LIST%`.

  Categoria tipului de date din resursa web blocată (de exemplu, *Graphic files*).

- **Link to requested web resource** – `%CONTINUE_PAGE%`.

  Linkul către pagina web solicitată (de exemplu, `http://www.example.com/pagename.html`).

- **Link to website** – `%CONTINUE_SITE%`.

  Linkul către site-ul web care conține pagina web solicitată (de exemplu, `http://www.example.com/`).

- **Link for access to domains** – `%CONTINUE_DOMAIN%`.

  Linkul pe care se poate da clic pentru a accesa toate paginile web existente ale numelui de domeniu. De exemplu, dacă adresa paginii web blocate este `http://www.example.com`, variabila `%CONTINUE_DOMAIN%` este înlocuită cu linkul `http://*.example.com`. Făcând clic pe acest link, vei avea acces la toate adresele web ale numelui de domeniu de bază `http://www.example.com/`, inclusiv la subdomenii, de exemplu, `http://start.example.com/*` sau `http://domain.domain.example.com/*`, unde caracterul `*` reprezintă orice secvență de caractere (inclusiv un șir gol).

Control dispozitive

Componenta Control dispozitive gestionează accesul utilizatorilor la dispozitivele instalate pe sau conectate la un computer (de exemplu, hard diskuri, camere video sau module Wi-Fi). Acest lucru îți permite să protejezi computerul împotriva infectării atunci când sunt conectate astfel de dispozitive și să împiedici pierderea sau scurgerea datelor.

Dacă Control dispozitive este activată, aplicația transmite informații despre dispozitivele conectate la Kaspersky Security Center. Puteți vizualiza lista dispozitivelor conectate în Kaspersky Security Center în directorul **Advanced** → **Repositories** → **Hardware**.

Nivelurile de acces ale dispozitivului

Componenta Control dispozitive controlează accesul la următoarele niveluri:

- **Device type**. De exemplu, imprimante, unități amovibile și unități CD/DVD.

  Poți configura accesul la dispozitive după cum urmează:

  - Permite – .
  - Blochează – .
  - Conform regulilor (numai imprimante și dispozitive portabile) – .
  - În funcție de magistrala de conectare (cu excepția Wi-Fi) – .
  - Blochează cu excepții (doar Wi-Fi) – .

- **Magistrală de conectare**. O *magistrală de conectare* este o interfață utilizată pentru conectarea dispozitivelor la computer (de exemplu, USB sau FireWire). Dacă modul **În funcție de magistrala de conectare** este selectat pentru tipul de dispozitiv, aplicația permite sau interzice accesul la dispozitiv în funcție de interfața de conectare (ex. USB).

Poți configura accesul la dispozitive după cum urmează:

- Permite – ✓.
- Blochează – ⊘.

- **Dispozitive de încredere**. *Dispozitivele de încredere* sunt dispozitivele la care utilizatorii specificați în setările pentru dispozitive de încredere au acces complet în orice moment.

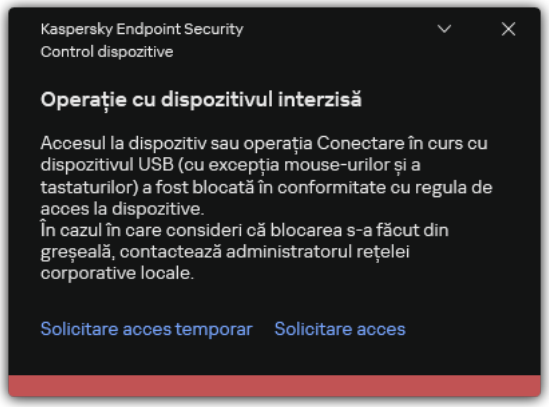
  Poți adăuga dispozitive de încredere pe baza următoarelor date:

  - **Dispozitive după ID**. Fiecare dispozitiv are un identificator unic (ID-ul hardware sau HWID). Poți vedea ID-ul în proprietățile dispozitivului utilizând instrumentele sistemului de operare. Exemplu de ID dispozitiv: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Adăugarea dispozitivelor după ID este convenabilă dacă doriți să adăugați mai multe dispozitive specifice.
  - **Dispozitive după model**. Fiecare dispozitiv are un ID de vânzător (VID) și un ID de produs (PID). Poți vedea ID-urile în proprietățile dispozitivului utilizând instrumentele sistemului de operare. Șablon pentru introducerea VID și PID: `VID_1234&PID_5678`. Adăugarea dispozitivelor după model este convenabilă dacă utilizați dispozitive ale unui anumit model în organizația dvs. În acest fel, puteți adăuga toate dispozitivele acestui model.
  - **Dispozitive după masca de ID**. Dacă utilizați mai multe dispozitive cu ID-uri similare, puteți adăuga dispozitive la lista de încredere folosind măști. Caracterul `*` înlocuiește orice set de caractere. Kaspersky Endpoint Security nu acceptă caracterul `?` atunci când introduceți o mască. De exemplu, `WDC_C*`.
  - **Dispozitive după masca modelului**. Dacă utilizați mai multe dispozitive cu VID sau PID similare (de exemplu, dispozitive de la același producător), puteți adăuga dispozitive la lista de încredere folosind măști. Caracterul `*` înlocuiește orice set de caractere. Kaspersky Endpoint Security nu acceptă caracterul `?` atunci când introduceți o mască. De exemplu, `VID_05AC&PID_*`.

Componenta Control dispozitive reglementează accesul utilizatorilor la dispozitive utilizând *reguli de acces*. Componenta Control dispozitive îți permite, de asemenea, să salvezi evenimente de conectare/deconectare a dispozitivelor. Pentru a salva evenimente, trebuie să configurezi înregistrarea evenimentelor într-o politică.

Dacă accesul la un dispozitiv depinde de magistrala de conectare (starea ◔), Kaspersky Endpoint Security nu salvează evenimente de conectare/deconectare a dispozitivului. Pentru a permite Kaspersky Endpoint Security să salveze evenimente de conectare/deconectare a dispozitivului, permite accesul la tipul corespunzător de dispozitiv (starea ✓) sau adaugă dispozitivul la lista de încredere.

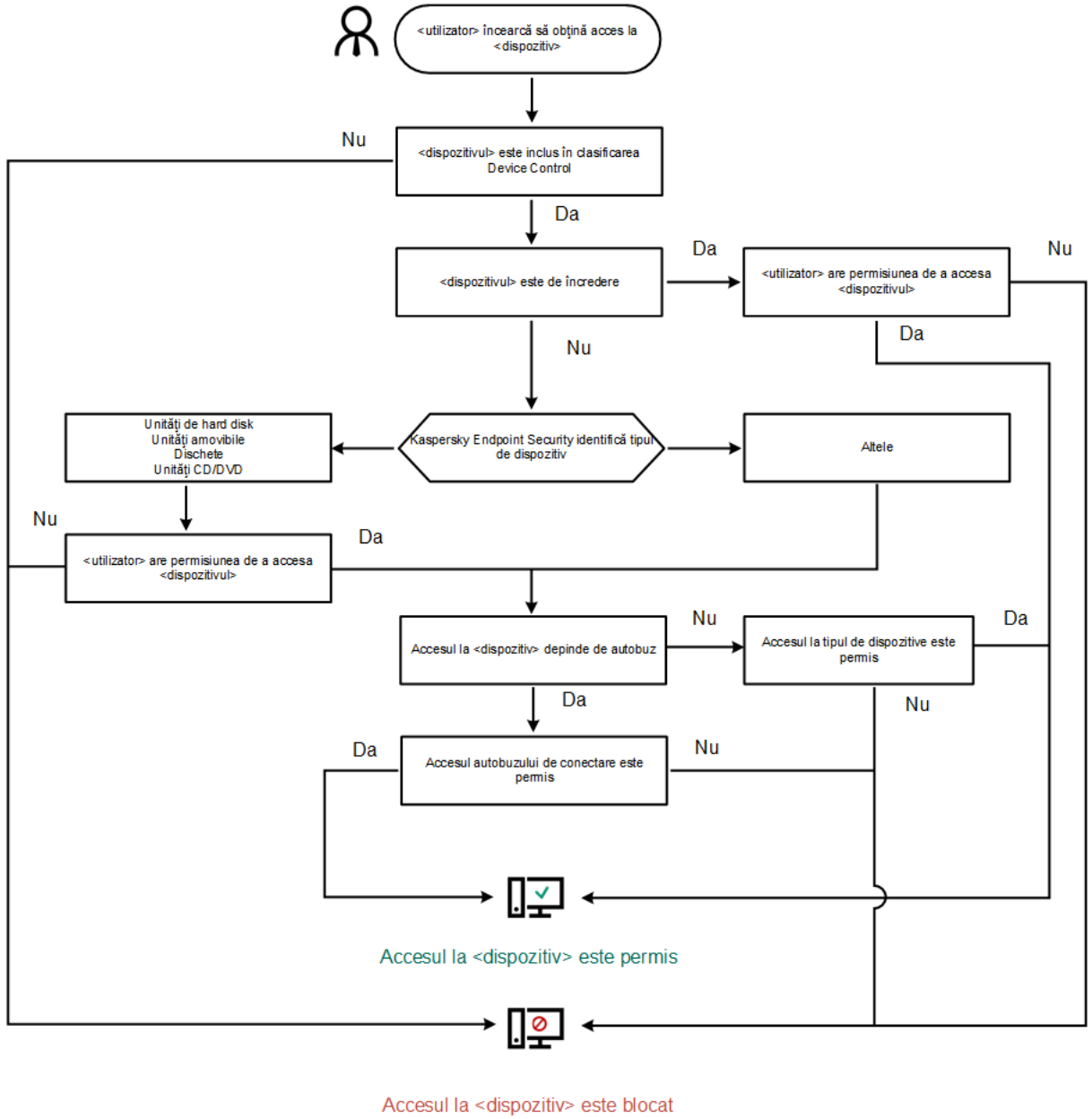
Atunci când un dispozitiv blocat de componenta Control dispozitive este conectat la computer, Kaspersky Endpoint Security va bloca accesul și va afișa o notificare (vezi figura de mai jos).



Notificări ale componentei Control dispozitive

Algoritmul de funcționare a componentei Control dispozitive

După ce utilizatorul conectează un dispozitiv la computer, Kaspersky Endpoint Security decide dacă permite accesul la dispozitivul respectiv (consultați figura de mai jos).



Algoritmul de funcționare a componentei Control dispozitive

Dacă un dispozitiv este conectat și accesul este permis, puteți edita regula de acces și bloca accesul. În acest caz, data următoare când cineva încearcă să acceseze dispozitivul (cum ar fi să vizualizeze arborele directorului sau să efectueze operațiuni de citire sau scriere), Kaspersky Endpoint Security blochează accesul. Un dispozitiv fără sistem de fișiere este blocat numai după următoarea conectare a dispozitivului.

Dacă un utilizator al computerului pe care este instalat Kaspersky Endpoint Security trebuie să solicite accesul la un dispozitiv care a fost blocat din greșeală, trimite utilizatorului instrucțiunile de solicitare acces.

Despre regulile de acces

O *regulă de acces al dispozitivului* este un grup de setări care determină modul în care utilizatorii pot accesa dispozitive instalate sau conectate la computer. Aceste setări includ accesul la un anumit dispozitiv, un program de acces și permisiuni de citire sau scriere. Nu poți adăuga un dispozitiv care este în afara clasificării componentei Control dispozitive. Accesul la astfel de dispozitive este permis pentru toți utilizatorii.

Reguli de acces la dispozitive

Grupul de setări pentru o regulă de acces diferă în funcție de tipul de dispozitiv (vezi tabelul de mai jos).

Setări pentru reguli de acces

Dispozitive	Controlul accesului	Planificare pentru acces la un dispozitiv	Atribuire a unor utilizatori și/sau a unui grup de utilizatori	Prioritate	Permisiune de citire/scriere
Unități de hard disk	✓	✓	✓	✓	✓
Unități amovibile (inclusiv unități flash USB)	✓	✓	✓	✓	✓
Dischete	✓	✓	✓	✓	✓
Unități CD/DVD	✓	✓	✓	✓	✓
Dispozitive portabile (MTP)	✓	✓	✓	✓	✓
Imprimante locale	✓	–	✓	✓	–
Imprimante în rețea	✓	–	✓	✓	–
Modemuri	✓	–	–	–	–
Dispozitive cu bandă	✓	–	–	–	–
Dispozitive multifuncționale	✓	–	–	–	–
Cititoare de carduri inteligente	✓	–	–	–	–
Dispozitive Windows CE USB ActiveSync	✓	–	–	–	–
Plăci de rețea externe	✓	–	–	–	–
Bluetooth	✓	–	–	–	–
Camere și scanere	✓	–	–	–	–

Reguli de acces pentru rețele Wi-Fi

O regulă de acces la rețele Wi-Fi determină dacă utilizarea rețelelor Wi-Fi este permisă (starea ✓) sau interzisă (starea ⊘). Poți adăuga o *rețea Wi-Fi de încredere* (starea) la o regulă. Utilizarea unei rețele Wi-Fi de încredere este permisă fără limitări. În mod implicit, o regulă de acces la rețele Wi-Fi permite accesul la orice rețea Wi-Fi.

Reguli de acces la magistrale de conectare

Dacă valoarea **În funcție de magistrala de conectare** este selectată pentru regula de acces în funcție de tipul de dispozitiv, aplicația permite sau refuză accesul la dispozitiv în funcție de interfața de conectare. În mod implicit, se creează reguli care permit accesul la magistrale pentru toate magistralele de conectare prezente în clasificarea componentei Control dispozitive.

Regulile de acces la magistrale de conectare determină dacă conectarea dispozitivelor este permisă (starea ✓) sau interzisă (starea ⊘). Prioritatea regulilor de acces la tipul de dispozitiv este mai mare decât prioritatea regulilor de acces la magistrala de conexiune.

Tastatura și mouse-ul nu pot fi blocate utilizând Control dispozitive. Dacă interziceți accesul la magistrala de conexiune USB, utilizatorul va continua să lucreze cu o tastatură și un mouse conectate prin USB. Componenta BadUSB Attack Prevention este concepută să împiedice dispozitivele USB infectate care emulează o tastatură să se conecteze la computer.

Gestionarea accesului la dispozitive în funcție de tip

Componenta Control dispozitive permite gestionarea accesului la dispozitive în funcție de tip. Tipul dispozitivului este determinat de sistemul de operare la conectarea acestuia. Poți căuta tipul dispozitivului utilizând instrumentul Device Manager încorporat în sistemul de operare. Pentru a gestiona accesul la dispozitive, trebuie să configurezi regulile. O *regulă de acces al dispozitivului* este un grup de setări care determină modul în care utilizatorii pot accesa dispozitive instalate sau conectate la computer. Aceste setări includ accesul la un anumit dispozitiv, un program de acces și permisiuni de citire sau scriere. Nu poți adăuga un dispozitiv care este în afara clasificării componentei Control dispozitive. Accesul la astfel de dispozitive este permis pentru toți utilizatorii.

În mod implicit, componenta Control dispozitive permite accesul la toate dispozitivele pentru toți utilizatorii.

Poți configura accesul la dispozitive după cum urmează:

- **Permite**.

  Kaspersky Endpoint Security oferă tuturor utilizatorilor acces complet la dispozitive.

- **Blochează**.

  Kaspersky Endpoint Security blochează conectarea dispozitivelor. Aplicația permite doar conectarea dispozitivelor de încredere.

- **În funcție de magistrala de conectare**.

  Kaspersky Endpoint Security determină interfața de conectare a dispozitivelor și restricționează accesul la acestea în funcție de starea conexiunii lor la magistrală. Aplicația permite, de asemenea, conectarea dispozitivelor de încredere.

- **Conform regulilor**.

  Pentru anumite tipuri de dispozitive, poți desemna utilizatori individuali sau un grup de utilizatori cărora li se permite să utilizeze dispozitivele, poți configura un program pentru accesul la dispozitive și poți configura permisiuni de citire și scriere. Aplicația permite, de asemenea, conectarea dispozitivelor de încredere.

Fii atent când configurezi accesul la dispozitivele de tip **Unități de hard disk**. Dacă blochezi accesul la discul de sistem, aplicația poate cauza o eroare (BSOD) la pornirea sistemului de operare.

Dacă un dispozitiv nu se încadrează în schema de clasificare a componentei Control dispozitive, accesul la acesta nu poate fi restricționat.

Cum se gestionează accesul la dispozitive după tip în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați **Policies**.
3. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
4. În fereastra politicii, selectați **Security Controls** → **Control dispozitive**.
5. În **Setări Control dispozitive**, selectează fila **Tipuri de dispozitive**.

   Fereastra **Tipuri de dispozitive** afișează regulile de acces pentru toate dispozitivele care sunt incluse în clasificarea componentei Control dispozitive.
6. Configurează regulile de acces pentru dispozitive:

   a. Selectează modul de acces: **Permite**, **Blochează**, **În funcție de magistrala de conectare**, **Conform regulilor**.

   Pentru a selecta modul de acces Conform regulilor, fă dublu clic pentru a deschide proprietățile regulii de acces.

   b. Dacă selectați modul de acces **În funcție de magistrala de conectare**, trebuie să configurați regulile de acces pentru interfețele de conexiune în fila **Magistrale de conectare**.

   c. În cazul dispozitivelor de stocare (de exemplu, suporturi de stocare amovibile), poți configura permisiuni de acces pentru utilizatori individuali. De asemenea, poți configura un program pentru accesul la dispozitive și permisiuni de citire și scriere.

   Poți adăuga dispozitive la lista de încredere. *Dispozitivele de încredere* sunt dispozitivele la care utilizatorii specificați în setările pentru dispozitive de încredere au acces complet în orice moment.

   d. Dacă este necesar, configurează regulile de imprimare.

   e. Dacă este necesar, configurează regulile de acces la dispozitivele Bluetooth.

   f. Dacă este necesar, configurează regulile de conectare a computerului la rețeaua Wi-Fi.
7. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se gestionează accesul la dispozitive în funcție de tip în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați fila **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Security Controls** → **Device Control**.
5. În **Device access rules**, selectează fila **Devices and Wi-Fi networks**.

   Tabelul listează regulile de acces pentru toate dispozitivele care sunt prezente în clasificarea componentei Control dispozitive.
6. Configurează regulile de acces pentru dispozitive:

   a. Selectează modul de acces: **Allow**, **Block**, **Depends on bus**, **Custom**.

   Dacă modul de acces lipsește din meniul vertical, deschide proprietățile regulii de acces făcând dublu clic pe tipul de dispozitiv.

   b. Dacă selectați modul de acces **Depends on bus**, trebuie să configurați regulile de acces pentru interfețele de conexiune în fila **Connection buses**.

   c. În cazul dispozitivelor de stocare (de exemplu, suporturi de stocare amovibile), poți configura permisiuni de acces pentru utilizatori individuali. De asemenea, poți configura un program pentru accesul la dispozitive și permisiuni de citire și scriere.

   Poți adăuga dispozitive la lista de încredere. *Dispozitivele de încredere* sunt dispozitivele la care utilizatorii specificați în setările pentru dispozitive de încredere au acces complet în orice moment.

   d. Dacă este necesar, configurează regulile de imprimare.

   e. Dacă este necesar, configurează regulile de acces la dispozitivele Bluetooth.

   f. Dacă este necesar, configurează regulile de conectare a computerului la rețeaua Wi-Fi.
7. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se gestionează accesul la dispozitive în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Security Controls** → **Control dispozitive**.
3. În blocul **Setări de acces**, faceți clic pe linkul **Dispozitive și rețele Wi-Fi**.

   Tabelul listează regulile de acces pentru toate dispozitivele care sunt prezente în clasificarea componentei Control dispozitive.
4. Configurează regulile de acces pentru dispozitive:

   a. Selectează modul de acces: **Permite**, **Blochează**, **În funcție de magistrala de conectare**, **Conform regulilor**.

   Dacă modul de acces lipsește din meniul vertical, deschide proprietățile regulii de acces făcând dublu clic pe tipul de dispozitiv.

b. Dacă selectați modul de acces **În funcție de magistrala de conectare**, trebuie să configurați regulile de acces pentru interfețele de conexiune în fila **Magistrale de conectare**.

c. În cazul dispozitivelor de stocare (de exemplu, suporturi de stocare amovibile), poți configura permisiuni de acces pentru utilizatori individuali. De asemenea, poți configura un program pentru accesul la dispozitive și permisiuni de citire și scriere.

Poți adăuga dispozitive la lista de încredere. *Dispozitivele de încredere* sunt dispozitivele la care utilizatorii specificați în setările pentru dispozitive de încredere au acces complet în orice moment.

d. Dacă este necesar, configurează regulile de imprimare.

e. Dacă este necesar, configurează regulile de acces la dispozitivele Bluetooth.

f. Dacă este necesar, configurează regulile de conectare a computerului la rețeaua Wi-Fi.

5. Salvați-vă modificările.

Prin urmare, atunci când un utilizator încearcă să acceseze un dispozitiv, aplicația blochează accesul conform regulilor. Kaspersky Endpoint Security înregistrează și un eveniment corespunzător. Dacă dorești să acorzi acces unor dispozitive individuale, poți adăuga aceste dispozitive la lista de dispozitive de încredere.

Gestionarea accesului la dispozitive prin magistrala de conectare

Pentru a edita o regulă de acces la magistrale de conectare:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Security Controls** → **Control dispozitive**.
3. În blocul **Setări de acces**, fă clic pe butonul **Magistrale de conectare**.

   Fereastra deschisă afișează regulile de acces pentru toate magistralele de conectare care sunt incluse în clasificarea componentelor Control dispozitive.
4. Selectați regula de acces pe care dorești să o editezi.
5. În coloana **Acces**, selectați dacă permiteți sau nu accesul la magistrala de conectare: **Permite** sau **Blochează**.

   Dacă ați schimbat accesul la **Port serial** (COM) sau **Port paralel** (LPT) al magistralei de conectare, trebuie să reporniți computerul pentru a activa regula de acces.
6. Salvați-vă modificările.

Diferențierea drepturilor de acces ale utilizatorilor la dispozitive

Puteți configura drepturile de acces ale utilizatorilor în funcție de tipul de dispozitiv sau pentru dispozitive de încredere.

Diferențierea drepturilor de acces ale utilizatorilor în funcție de tipul de dispozitiv

Funcția Control dispozitive permite configurarea drepturilor de acces ale utilizatorilor la datele de pe *dispozitivele de stocare*. Pentru astfel de dispozitive, puteți configura permisiuni de scriere și citire. Funcția Control dispozitive acceptă următoarele tipuri de *dispozitive de stocare*:

- Unități de hard disk.
- Unități amovibile (inclusiv unități flash USB).
- Dischete.
- Unități CD/DVD.
- Dispozitive portabile (MTP). Dispozitivele portabile (MTP) includ, de exemplu, dispozitive mobile, camere foto, playere media și așa mai departe.

Astfel, puteți, de exemplu, să permiteți utilizarea suporturilor amovibile doar grupului de administratori. Pentru alte tipuri de dispozitive, puteți refuza sau permite accesul tuturor utilizatorilor. De asemenea, puteți configura drepturile de acces ale utilizatorilor pentru utilizarea imprimantelor.

Cum se configurează drepturile de acces ale utilizatorilor la datele de pe dispozitivele de stocare în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați **Policies**.
3. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
4. În fereastra politicii, selectați **Security Controls → Control dispozitive**.
5. În **Setări Control dispozitive**, selectează fila **Tipuri de dispozitive**.

   Fereastra **Tipuri de dispozitive** afișează regulile de acces pentru toate dispozitivele care sunt incluse în clasificarea componentei Control dispozitive.
6. Pentru a configura regulile de acces la dispozitivele de stocare, fă dublu clic pentru a deschide lista de reguli.
7. Configurarea regulilor de acces la dispozitivele de stocare:

   a. În blocul **Reguli de acces**, fă clic pe butonul **Adaugă**.

      Această acțiune deschide o fereastră pentru adăugarea unei noi reguli de acces la dispozitivele de stocare.

   b. În câmpul **Prioritatea regulii**, setează prioritatea de *scriere a regulii*. O regulă include următoarele atribute: cont de utilizator, programul, permisiuni (citire/scriere) și prioritate.

      O regulă are o prioritate specifică. Dacă un utilizator a fost adăugat la mai multe grupuri, Kaspersky Endpoint Security reglementează accesul la dispozitiv pe baza regulii cu cea mai mare prioritate. Kaspersky Endpoint Security îți permite alocarea unei priorități de la 0 la 10.000. Cu cât valoarea este mai mare, cu atât prioritatea este mai mare. Cu alte cuvinte, o intrare cu valoarea 0 are cea mai scăzută prioritate.

      De exemplu, puteți acorda permisiuni numai de citire grupului Oricine și acorda permisiuni de citire/scriere grupului de administratori. Pentru aceasta, atribuiți o prioritate 1 pentru grupul de administratori și atribuiți o prioritate de 0 pentru grupul Oricine.

Prioritatea pentru o regulă de blocare este mai mare decât prioritatea pentru o regulă de permitere. Cu alte cuvinte, dacă un utilizator a fost adăugat la mai multe grupuri și prioritatea tuturor regulilor este aceeași, Kaspersky Endpoint Security reglementează accesul dispozitivului pe baza oricărei reguli de blocare existente.

c. În **Regulă pentru utilizatori și grupuri**, selectați utilizatori sau grupuri de utilizatori. Poți selecta utilizatori în Active Directory, în lista de conturi din Kaspersky Security Center sau introducând manual un nume de utilizator local. Kaspersky recomandă utilizarea conturilor de utilizator locale numai în cazuri speciale, când nu este posibilă utilizarea conturilor de utilizator de domeniu.

d. Fă clic pe **OK**.

8. În **Planificări pentru regula de acces selectată**, configurează un program de acces la dispozitivul de stocare pentru utilizatori.

   De exemplu, poți permite utilizatorilor să utilizeze dispozitivele de stocare numai în timpul orelor de program.

9. Configurează permisiunile de acces ale utilizatorilor la dispozitivele de stocare în managerul de fișiere (**Citește** / **Scrie**).

10. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se configurează drepturile de acces ale utilizatorilor la datele de pe dispozitivele de stocare în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați fila **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **Security Controls** → **Device Control**.

5. În blocul **Device access rules**, în tabelul cu regulile de acces, deschide proprietățile regulilor de acces pentru dispozitivele de stocare.

6. În secțiunea **Device access rules**, selectați **Custom**.

7. Configurarea regulilor de acces la dispozitivele de stocare:

   a. În blocul **Users and their rights**, fă clic pe butonul **Add**.

   Această acțiune deschide o fereastră pentru adăugarea unei noi reguli de acces la dispozitivele de stocare.

   b. În câmpul **Priority**, setează prioritatea de *scriere a regulii*. O regulă include următoarele atribute: cont de utilizator, programul, permisiuni (citire/scriere) și prioritate.

   O regulă are o prioritate specifică. Dacă un utilizator a fost adăugat la mai multe grupuri, Kaspersky Endpoint Security reglementează accesul la dispozitiv pe baza regulii cu cea mai mare prioritate. Kaspersky Endpoint Security îți permite alocarea unei priorități de la 0 la 10.000. Cu cât valoarea este mai mare, cu atât prioritatea este mai mare. Cu alte cuvinte, o intrare cu valoarea 0 are cea mai scăzută prioritate.

   De exemplu, puteți acorda permisiuni numai de citire grupului Oricine și acorda permisiuni de citire/scriere grupului de administratori. Pentru aceasta, atribuiți o prioritate 1 pentru grupul de administratori și atribuiți o prioritate de 0 pentru grupul Oricine.

Prioritatea pentru o regulă de blocare este mai mare decât prioritatea pentru o regulă de permitere. Cu alte cuvinte, dacă un utilizator a fost adăugat la mai multe grupuri și prioritatea tuturor regulilor este aceeași, Kaspersky Endpoint Security reglementează accesul dispozitivului pe baza oricărei reguli de blocare existente.

c. În **User or group**, selectați utilizatori sau grupuri de utilizatori. Poți selecta utilizatori în Active Directory, în lista de conturi din Kaspersky Security Center sau introducând manual un nume de utilizator local. Kaspersky recomandă utilizarea conturilor de utilizator locale numai în cazuri speciale, când nu este posibilă utilizarea conturilor de utilizator de domeniu.

d. În **Access schedule**, configurează un program de acces la dispozitivul de stocare pentru utilizatori.

De exemplu, poți permite utilizatorilor să utilizeze dispozitivele de stocare numai în timpul orelor de program.

e. Configurează permisiunile de acces ale utilizatorilor la dispozitivele de stocare în managerul de fișiere (**Read** / **Write**).

f. Fă clic pe **Save**.

8. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se configurează drepturile de acces ale utilizatorilor la datele de pe dispozitivele de stocare în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Security Controls** → **Control dispozitive**.

3. În blocul **Setări de acces**, faceți clic pe linkul **Dispozitive și rețele Wi-Fi**.

Tabelul listează regulile de acces pentru toate dispozitivele care sunt prezente în clasificarea componentei Control dispozitive.

4. Pentru a configura regulile de acces la dispozitivele de stocare, fă dublu clic pentru a deschide lista de reguli.

5. Configurarea regulilor de acces la dispozitivele de stocare:

a. În blocul **Drepturile utilizatorilor**, fă clic pe butonul **Adaugă**.

Această acțiune deschide o fereastră pentru adăugarea unei noi reguli de acces la dispozitivele de stocare.

b. În câmpul **Prioritate**, setează prioritatea de *scriere a regulii*. O regulă include următoarele atribute: cont de utilizator, programul, permisiuni (citire/scriere) și prioritate.

O regulă are o prioritate specifică. Dacă un utilizator a fost adăugat la mai multe grupuri, Kaspersky Endpoint Security reglementează accesul la dispozitiv pe baza regulii cu cea mai mare prioritate. Kaspersky Endpoint Security îți permite alocarea unei priorități de la 0 la 10.000. Cu cât valoarea este mai mare, cu atât prioritatea este mai mare. Cu alte cuvinte, o intrare cu valoarea 0 are cea mai scăzută prioritate.

De exemplu, puteți acorda permisiuni numai de citire grupului Oricine și acorda permisiuni de citire/scriere grupului de administratori. Pentru aceasta, atribuiți o prioritate 1 pentru grupul de administratori și atribuiți o prioritate de 0 pentru grupul Oricine.

Prioritatea pentru o regulă de blocare este mai mare decât prioritatea pentru o regulă de permitere. Cu alte cuvinte, dacă un utilizator a fost adăugat la mai multe grupuri și prioritatea tuturor regulilor este aceeași, Kaspersky Endpoint Security reglementează accesul dispozitivului pe baza oricărei reguli de blocare existente.

c. În **Utilizatori**, selectați utilizatori sau grupuri de utilizatori. Poți selecta utilizatori în Active Directory sau poți introduce manual un nume de utilizator local. Kaspersky recomandă utilizarea conturilor de utilizator locale numai în cazuri speciale, când nu este posibilă utilizarea conturilor de utilizator de domeniu.

d. Fă clic pe **OK**.

6. În **Planificare pentru acces la dispozitive**, configurează un program de acces la dispozitivul de stocare pentru utilizatori.

   De exemplu, poți permite utilizatorilor să utilizeze dispozitivele de stocare numai în timpul orelor de program.

7. Configurează permisiunile de acces ale utilizatorilor la dispozitivele de stocare în managerul de fișiere (**Citește** / **Scrie**).

8. Salvați-vă modificările.

Diferențierea drepturilor de acces ale utilizatorilor la dispozitivele de încredere

Dispozitivele de încredere sunt dispozitivele la care utilizatorii specificați în setările pentru dispozitive de încredere au acces complet în orice moment. Pentru a lucra cu dispozitive de încredere, puteți acorda acces unui utilizator individual, unui grup de utilizatori sau tuturor utilizatorilor organizației. Poți configura drepturile de acces ale utilizatorilor în proprietățile dispozitivului de încredere.

Gestionarea accesului la dispozitivele mobile

Kaspersky Endpoint Security vă permite să controlați accesul la date de pe dispozitivele mobile pe care rulează Android și iOS. Dispozitivele mobile aparțin categoriei de dispozitive portabile (MTP). Prin urmare, pentru a configura accesul la dispozitivele mobile, trebuie să editați setările de acces pentru dispozitivele portabile (MTP).

Când un dispozitiv mobil este conectat la computer, sistemul de operare determină tipul dispozitivului. Dacă Android Debug Bridge (ADB), iTunes sau aplicațiile lor echivalente sunt instalate pe computer, sistemul de operare identifică dispozitivele mobile ca dispozitive ADB sau iTunes. În toate celelalte cazuri, sistemul de operare poate identifica tipul dispozitivului mobil ca un dispozitiv portabil (MTP) pentru transfer de fișiere, un dispozitiv PTP (cameră) pentru transfer de imagini sau un alt dispozitiv. Tipul dispozitivului depinde de modelul dispozitivului mobil și de modul de conectare USB selectat. Kaspersky Endpoint Security vă permite să configurați permisiuni de acces individuale pentru datele de pe dispozitivele mobile din aplicațiile ADB, iTunes sau managerul de fișiere. În toate celelalte cazuri, componenta Control dispozitive permite accesul la dispozitivele mobile în conformitate cu regulile de acces la dispozitivele portabile (MTP).

Accesul la dispozitivele mobile

Dispozitivele mobile aparțin categoriei de dispozitive portabile (MTP), prin urmare setările pentru acestea sunt aceleași. Poți selecta unul dintre următoarele moduri de acces la dispozitivele mobile:

- **Permite**. Kaspersky Endpoint Security permite accesul complet la dispozitivele mobile. Puteți deschide, crea, modifica, copia sau șterge fișiere de pe dispozitivele mobile folosind managerul de fișiere sau aplicațiile ADB și iTunes. De asemenea, puteți încărca bateria dispozitivului conectând dispozitivul mobil la un port USB al computerului.
- **Blochează**. Kaspersky Endpoint Security restricționează accesul la dispozitivele mobile din managerul de fișiere și aplicațiile ADB și iTunes. Aplicația permite accesul numai la dispozitive mobile de încredere. De asemenea, puteți încărca bateria dispozitivului conectând dispozitivul mobil la un port USB al computerului.
- **În funcție de magistrala de conectare**. Kaspersky Endpoint Security permite conectarea la dispozitive mobile, în conformitate cu starea conexiunii USB (**Permite** sau **Blochează**).
- **Conform regulilor**. Kaspersky Endpoint Security restricționează accesul la dispozitivele mobile în conformitate cu regulile. În reguli, puteți configura drepturile de acces (citire/scriere), selectați utilizatori sau un grup de utilizatori care pot avea acces la dispozitive mobile și configurați un program de acces pentru dispozitivele mobile. De asemenea, puteți restricționa accesul la dispozitivele mobile folosind aplicațiile ADB și iTunes.

Configurarea regulilor de acces la dispozitivele mobile

Regulile de acces pentru dispozitivele portabile (MTP), dispozitivele ADB și dispozitivele iTunes sunt configurate diferit. Pentru dispozitivele portabile (MTP) și dispozitivele ADB, puteți configura reguli pentru utilizatori individuali sau grupuri de utilizatori și puteți crea un program pentru când se vor aplica regulile. Pentru dispozitivele iTunes, nu puteți face acest lucru. Puteți permite sau refuza accesul la date doar prin intermediul aplicației iTunes pentru toți utilizatorii.

Cum să configurați regulile de acces la dispozitivele mobile în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Security Controls** → **Control dispozitive**.
4. În **Setări Control dispozitive**, selectează fila **Tipuri de dispozitive**.

   Tabelul listează regulile de acces pentru toate dispozitivele care sunt prezente în clasificarea componentei Control dispozitive.
5. În meniul contextual pentru tipul de dispozitiv **Dispozitive portabile (MTP)**, configurați modul de acces al dispozitivului mobil: **Permite**, **Blochează** saur **În funcție de magistrala de conectare**.
6. Pentru a configura regulile de acces la dispozitivele mobile, faceți dublu clic pentru a deschide lista de reguli.

7. Configurarea regulilor de acces la dispozitivele mobile:

   a. În blocul **Reguli de acces**, fă clic pe butonul **Adaugă**.

      Aceasta deschide o fereastră pentru adăugarea unei noi reguli de acces la dispozitivul mobil.

   b. În câmpul **Prioritate**, setați prioritatea de scriere a regulii. O regulă include următoarele atribute: cont de utilizator, program, permisiuni (citire/scriere/acces ADB) și prioritate.

      O regulă are o prioritate specifică. Dacă un utilizator a fost adăugat la mai multe grupuri, Kaspersky Endpoint Security reglementează accesul la dispozitiv pe baza regulii cu cea mai mare prioritate. Kaspersky Endpoint Security îți permite alocarea unei priorități de la 0 la 10.000. Cu cât valoarea este mai mare, cu atât prioritatea este mai mare. Cu alte cuvinte, o intrare cu valoarea 0 are cea mai scăzută prioritate.

      De exemplu, puteți acorda permisiuni numai de citire grupului Oricine și acorda permisiuni de citire/scriere grupului de administratori. Pentru aceasta, atribuiți o prioritate 1 pentru grupul de administratori și atribuiți o prioritate de 0 pentru grupul Oricine.

      Prioritatea pentru o regulă de blocare este mai mare decât prioritatea pentru o regulă de permitere. Cu alte cuvinte, dacă un utilizator a fost adăugat la mai multe grupuri și prioritatea tuturor regulilor este aceeași, Kaspersky Endpoint Security reglementează accesul dispozitivului pe baza oricărei reguli de blocare existente.

   c. În **Regulă pentru utilizatori și grupuri**, selectați utilizatori sau grupuri de utilizatori. Poți selecta utilizatori în Active Directory, în lista de conturi din Kaspersky Security Center sau introducând manual un nume de utilizator local. Kaspersky recomandă utilizarea conturilor de utilizator locale numai în cazuri speciale, când nu este posibilă utilizarea conturilor de utilizator de domeniu.

   d. Fă clic pe **OK**.

8. În **Planificări pentru regula de acces selectată**, configurați un program de acces la dispozitivul mobil pentru utilizatori.

   Configurarea unui program de acces separat pentru dispozitivele ADB nu este posibilă. Puteți configura un program de acces comun pentru dispozitivele ADB și dispozitivele portabile (MTP).

9. Configurați permisiunile de acces ale utilizatorilor la dispozitivele mobile în managerul de fișiere (**Citește** / **Scrie**).

10. Configurați accesul la date de pe un dispozitiv mobil prin aplicația ADB, folosind caseta de selectare **Acces prin ADB**.

    În cazul în care caseta de selectare este debifată, atunci când dispozitivul mobil este conectat, aplicația ADB este împiedicată să detecteze dispozitivul.

11. În **Acces prin iTunes**, configurați accesul la datele de pe dispozitivul mobil prin aplicația iTunes.

    Kaspersky Endpoint Security aplică setările pentru accesul la dispozitivele mobile prin aplicația iTunes pentru toți utilizatorii. Configurarea unui program de acces separat pentru dispozitivele iTunes nu este posibilă.

12. Salvați-vă modificările.

Cum să configurați regulile de acces la dispozitivele mobile în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Security Controls** → **Device Control**.
5. În blocul **Device access rules**, faceți clic pe linkul **Devices and Wi-Fi networks**.

   Tabelul listează regulile de acces pentru toate dispozitivele care sunt prezente în clasificarea componentei Control dispozitive.
6. Selectați tipul de dispozitiv **Portable devices (MTP)**.

   Această acțiune deschide drepturile de acces la dispozitivele portabile (MTP).
7. Configurează modul de acces la dispozitivele mobile: **Allow**, **Block**, **Depends on bus** sau **Custom**.
8. Utilizând comutatorul **Access via iTunes for all users ENABLED**, configurează accesul la datele de pe dispozitivul mobil prin aplicația iTunes.

   Kaspersky Endpoint Security aplică setările pentru accesul la dispozitivele mobile prin aplicația iTunes pentru toți utilizatorii. Configurarea unui program de acces separat pentru dispozitivele iTunes nu este posibilă.
9. Dacă selectați modul **Custom**, trebuie să adăugați reguli de acces pentru dispozitive. Pentru aceasta, în **Users and their rights**, faceți clic pe butonul **Add** butonul și configurați regula de acces la dispozitivul mobil:

   a. În câmpul **Priority**, setați prioritatea de scriere a regulii. O regulă include următoarele atribute: cont de utilizator, program, permisiuni (citire/scriere/acces ADB) și prioritate.

   O regulă are o prioritate specifică. Dacă un utilizator a fost adăugat la mai multe grupuri, Kaspersky Endpoint Security reglementează accesul la dispozitiv pe baza regulii cu cea mai mare prioritate. Kaspersky Endpoint Security îți permite alocarea unei priorități de la 0 la 10.000. Cu cât valoarea este mai mare, cu atât prioritatea este mai mare. Cu alte cuvinte, o intrare cu valoarea 0 are cea mai scăzută prioritate.

   De exemplu, puteți acorda permisiuni numai de citire grupului Oricine și acorda permisiuni de citire/scriere grupului de administratori. Pentru aceasta, atribuiți o prioritate 1 pentru grupul de administratori și atribuiți o prioritate de 0 pentru grupul Oricine.

   Prioritatea pentru o regulă de blocare este mai mare decât prioritatea pentru o regulă de permitere. Cu alte cuvinte, dacă un utilizator a fost adăugat la mai multe grupuri și prioritatea tuturor regulilor este aceeași, Kaspersky Endpoint Security reglementează accesul dispozitivului pe baza oricărei reguli de blocare existente.

   b. În **User or group**, selectați utilizatorii sau grupurile de utilizatori pentru acces la dispozitivele mobile. Poți selecta utilizatori în Active Directory, în lista de conturi din Kaspersky Security Center sau introducând manual un nume de utilizator local. Kaspersky recomandă utilizarea conturilor de utilizator locale numai în cazuri speciale, când nu este posibilă utilizarea conturilor de utilizator de domeniu.

c. În **Access schedule**, configurați un program de acces la dispozitivul mobil pentru utilizatori.

> Configurarea unui program de acces separat pentru dispozitivele ADB nu este posibilă. Puteți configura un program de acces comun pentru dispozitivele ADB și dispozitivele portabile (MTP).

d. Configurați permisiunile de acces ale utilizatorilor la dispozitivele mobile în managerul de fișiere (**Read** / **Write**).

e. Configurați accesul la date de pe un dispozitiv mobil prin aplicația ADB, folosind caseta de selectare **Access via ADB**.

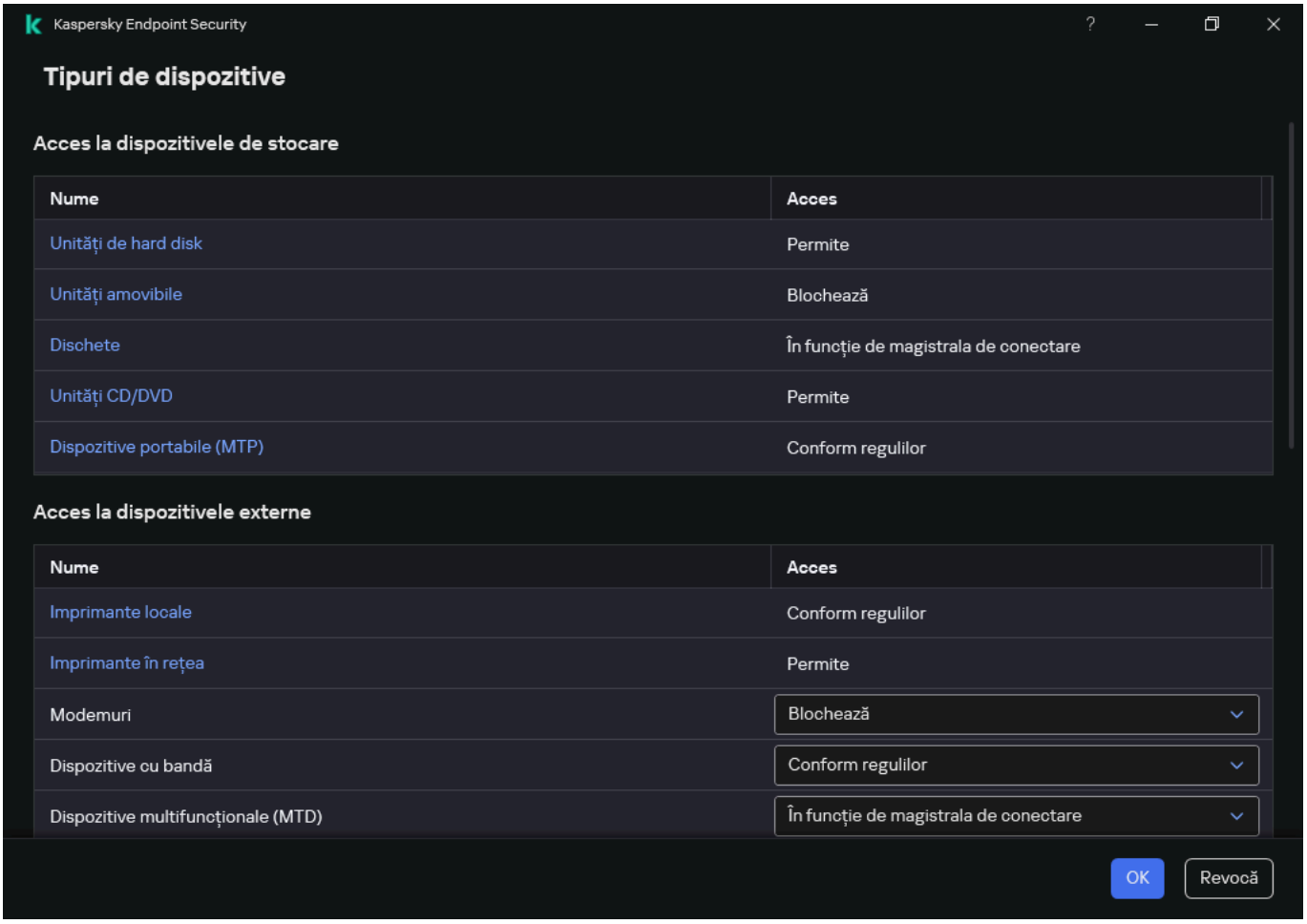
În cazul în care caseta de selectare este debifată, atunci când dispozitivul mobil este conectat, aplicația ADB este împiedicată să detecteze dispozitivul.

10. Salvați-vă modificările.

Cum se configurează regulile de acces la dispozitivele mobile în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Security Controls → Control dispozitive**.
3. În blocul **Setări de acces**, fă clic pe butonul **Dispozitive și rețele Wi-Fi**.

   Fereastra deschisă afișează regulile de acces pentru toate dispozitivele care sunt incluse în clasificarea componentelor Control dispozitive.



Tipuri de dispozitive din componenta Control dispozitive

4. În blocul **Acces la dispozitivele de stocare**, faceți clic pe linkul **Dispozitive portabile (MTP)**.

   Această acțiune deschide o fereastră care conține regulile de acces la dispozitivele portabile (MTP).

5. În **Acces**, configurați modul de acces la dispozitivele mobile: **Permite**, **Blochează**, **În funcție de magistrala de conectare** sau **Conform regulilor**.

6. Dacă selectați modul **Conform regulilor**, trebuie să adăugați reguli de acces pentru dispozitive:

   a. În blocul **Drepturile utilizatorilor**, fă clic pe butonul **Adaugă**.

      Aceasta deschide o fereastră pentru adăugarea unei noi reguli de acces la dispozitivul mobil.

   b. În câmpul **Prioritate**, setați prioritatea de scriere a regulii. O regulă include următoarele atribute: cont de utilizator, program, permisiuni (citire/scriere/acces ADB) și prioritate.

      O regulă are o prioritate specifică. Dacă un utilizator a fost adăugat la mai multe grupuri, Kaspersky Endpoint Security reglementează accesul la dispozitiv pe baza regulii cu cea mai mare prioritate. Kaspersky Endpoint Security îți permite alocarea unei priorități de la 0 la 10.000. Cu cât valoarea este mai mare, cu atât prioritatea este mai mare. Cu alte cuvinte, o intrare cu valoarea 0 are cea mai scăzută prioritate.

      De exemplu, puteți acorda permisiuni numai de citire grupului Oricine și acorda permisiuni de citire/scriere grupului de administratori. Pentru aceasta, atribuiți o prioritate 1 pentru grupul de administratori și atribuiți o prioritate de 0 pentru grupul Oricine.

      Prioritatea pentru o regulă de blocare este mai mare decât prioritatea pentru o regulă de permitere. Cu alte cuvinte, dacă un utilizator a fost adăugat la mai multe grupuri și prioritatea tuturor regulilor este aceeași, Kaspersky Endpoint Security reglementează accesul dispozitivului pe baza oricărei reguli de blocare existente.

   c. În **Condiție**, activați modul de acces la dispozitivele mobile.

   d. În **Reguli de acces**, configurați permisiunile de acces la dispozitivele mobile pentru utilizatori.

      - Configurați permisiunile de acces ale utilizatorilor la dispozitivele mobile în managerul de fișiere (**Citește** / **Scrie**).

      - Configurați accesul la date de pe un dispozitiv mobil prin aplicația ADB, folosind caseta de selectare **Acces prin ADB**.

        În cazul în care caseta de selectare este debifată, atunci când dispozitivul mobil este conectat, aplicația ADB este împiedicată să detecteze dispozitivul.

   e. În **Utilizatori**, selectați utilizatorii sau grupurile de utilizatori pentru acces la dispozitivele mobile. Poți selecta utilizatori în Active Directory, în lista de conturi din Kaspersky Security Center sau introducând manual un nume de utilizator local. Kaspersky recomandă utilizarea conturilor de utilizator locale numai în cazuri speciale, când nu este posibilă utilizarea conturilor de utilizator de domeniu.

   f. În **Planificare pentru acces la dispozitive**, configurați un program de acces la dispozitivele mobile pentru utilizatori.

      Configurarea unui program de acces separat pentru dispozitivele ADB nu este posibilă. Puteți configura un program de acces comun pentru dispozitivele ADB și dispozitivele portabile (MTP).

g. În **Acces prin iTunes**, configurați accesul la datele de pe dispozitivul mobil prin aplicația iTunes.

Kaspersky Endpoint Security aplică setările pentru accesul la dispozitivele mobile prin aplicația iTunes pentru toți utilizatorii. Configurarea unui program de acces separat pentru dispozitivele iTunes nu este posibilă.

7. Salvați-vă modificările.

Drept urmare, accesul utilizatorului la dispozitivele mobile este restricționat în conformitate cu regulile. Dacă ați interzis accesul la dispozitive mobile în aplicațiile ADB și iTunes, atunci când conectați un dispozitiv mobil, aplicațiile ADB și iTunes sunt împiedicate să detecteze dispozitivul mobil.

Dispozitive mobile de încredere

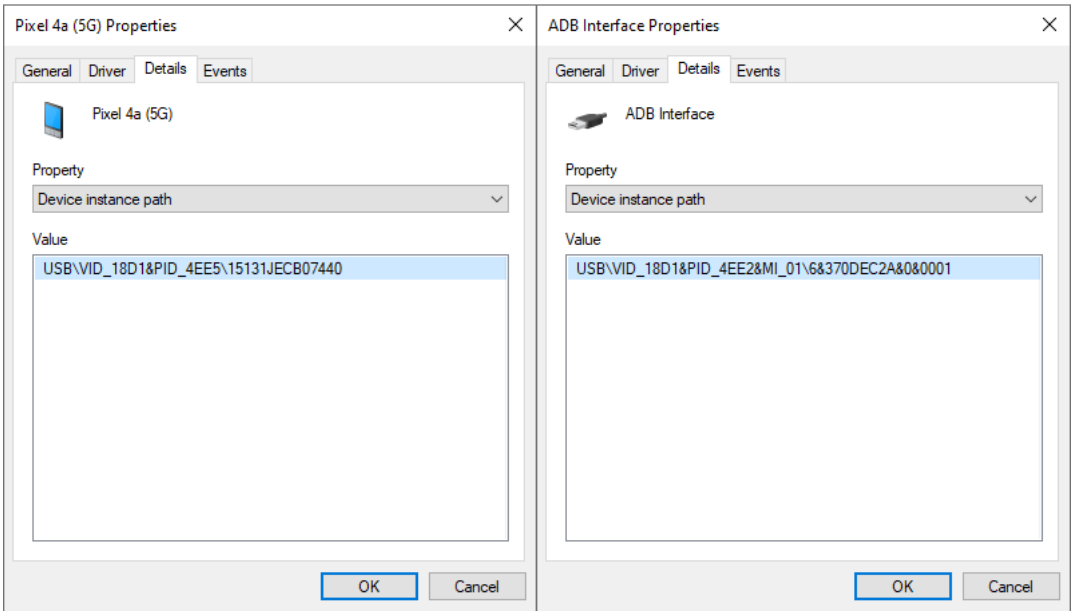
Dispozitivele de încredere sunt dispozitivele la care utilizatorii specificați în setările pentru dispozitive de încredere au acces complet în orice moment.

Procedura pentru adăugarea unui dispozitiv mobil de încredere este exact la fel ca pentru alte tipuri de dispozitive de încredere. Puteți adăuga un dispozitiv mobil după ID sau modelul dispozitivului.

Pentru a adăuga un dispozitiv mobil de încredere după ID, veți avea nevoie de un ID unic (Hardware ID – HWID). Puteți găsi ID-ul în proprietățile dispozitivului, utilizând instrumentele sistemului de operare (vezi figura de mai jos). Instrumentul Manager dispozitive vă permite să faceți acest lucru. ID-urile dispozitivelor portabile (MTP) și ale dispozitivelor ADB și iTunes sunt diferite chiar și pentru același dispozitiv mobil. ID-ul unui dispozitiv portabil (MTP) poate arăta astfel: `15131JECB07440`. ID-ul unui dispozitiv ADB poate arăta astfel: `6&370DEC2A&0&0001`. Adăugarea dispozitivelor după ID este convenabilă dacă doriți să adăugați mai multe dispozitive specifice. Puteți folosi și măști.

Dacă ați instalat aplicațiile ADB sau iTunes după conectarea unui dispozitiv la computer, ID-ul unic al dispozitivului poate fi resetat. Aceasta înseamnă că Kaspersky Endpoint Security va identifica acest dispozitiv ca un dispozitiv nou. Dacă un dispozitiv este de încredere, adăugați-l din nou în lista de încredere.

Pentru a adăuga un dispozitiv mobil de încredere după modelul dispozitivului, veți avea nevoie de Vendor ID (VID) și Product ID (PID). Puteți găsi ID-urile în proprietățile dispozitivului, utilizând instrumentele sistemului de operare (vezi figura de mai jos). Șablon pentru introducerea VID și PID: `VID_18D1&PID_4EE5`. Adăugarea dispozitivelor după model este convenabilă dacă utilizați dispozitive ale unui anumit model în organizația dvs. În acest fel, puteți adăuga toate dispozitivele acestui model.



ID dispozitiv în Manager dispozitive

Gestionarea accesului la dispozitivele Bluetooth

Kaspersky Endpoint Security permite gestionarea accesului la dispozitivele Bluetooth. Dispozitivele Bluetooth includ tastaturi fără fir, mouse-uri, căști, imprimante etc. Puteți utiliza Bluetooth-ul și pentru comunicare, de ex. cu un dispozitiv mobil.

Când dispozitivele Bluetooth sunt conectate sau deconectate, aplicația poate crea mai multe evenimente despre dispozitiv. Motivul este că sistemul de operare poate detecta un dispozitiv Bluetooth ca mai multe dispozitive de diferite tipuri. Kaspersky Endpoint Security gestionează și adaptorul Bluetooth prin care dispozitivul este conectat ca dispozitiv separat. De aceea, aplicația creează un eveniment pentru fiecare dintre dispozitivele detectate.

Poți selecta unul dintre următoarele moduri de acces la dispozitivele Bluetooth:

- **Permite și nu înregistra în jurnal** . Kaspersky Endpoint Security permite conectarea oricăror dispozitive Bluetooth și nu salvează informații despre conexiune în jurnalul de evenimente. Puteți conecta dispozitive de intrare Bluetooth (tastaturi, mouse-uri etc.), puteți trimite date prin Bluetooth, puteți gestiona alte dispozitive Bluetooth (căști, căști cu microfon încorporat etc.).

- **Permite** . Kaspersky Endpoint Security permite conectarea oricăror dispozitive Bluetooth. Puteți conecta dispozitive de intrare Bluetooth (tastaturi, mouse-uri etc.), puteți trimite date prin Bluetooth, puteți gestiona alte dispozitive Bluetooth (căști, căști cu microfon încorporat etc.).

- **Blochează** . Kaspersky Endpoint Security restricționează accesul la dispozitivele Bluetooth. Poți permite conectarea numai a dispozitivelor de intrare Bluetooth. (clasa Human Interface Devices). Aceste dispozitive includ tastaturi, mouse-uri, joystick-uri etc.

Nu este posibil să creezi o listă de dispozitive Bluetooth de încredere. Dacă ai acces restricționat la dispozitivele Bluetooth, poți conecta numai dispozitivele de intrare Bluetooth.

Cum se configurează regulile de acces la dispozitivele Bluetooth în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați **Policies**.
3. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
4. În fereastra politicii, selectați **Security Controls** → **Control dispozitive**.
5. În **Setări Control dispozitive**, selectează fila **Tipuri de dispozitive**.

   Tabelul listează regulile de acces pentru toate dispozitivele care sunt prezente în clasificarea componentei Control dispozitive.
6. În meniul contextual pentru tipul de dispozitiv **Bluetooth**, configurați modul de acces al dispozitivului Bluetooth: **Permite** , **Blochează** , **Permite și nu înregistra în jurnal** .
7. Dacă selectați modul **Blochează**, puteți permite conectarea doar a dispozitivelor de intrare Bluetooth (tastaturi, mouse-uri etc.). Pentru aceasta, în **Excluderi**, bifați caseta de selectare **Dispozitive de intrare (mouse-uri și tastaturi)**.
8. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se configurează regulile de acces la dispozitivele Bluetooth în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați fila **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Security Controls** → **Device Control**.

5. În blocul **Device access rules**, faceți clic pe linkul **Devices and Wi-Fi networks**.

   Tabelul listează regulile de acces pentru toate dispozitivele care sunt prezente în clasificarea componentei Control dispozitive.

6. Selectați tipul de dispozitiv **Bluetooth devices**.

   Aceasta deschide setările de acces la dispozitivul Bluetooth.

7. Configurați modul de acces la dispozitivul Bluetooth: **Allow**, **Block**, **Allow and do not log**.

8. Dacă selectați modul **Block**, puteți permite conectarea doar a dispozitivelor de intrare Bluetooth (tastaturi, mouse-uri etc.). Pentru aceasta, în **Exclusions**, bifați caseta de selectare **Input devices (mice and keyboards)**.

9. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

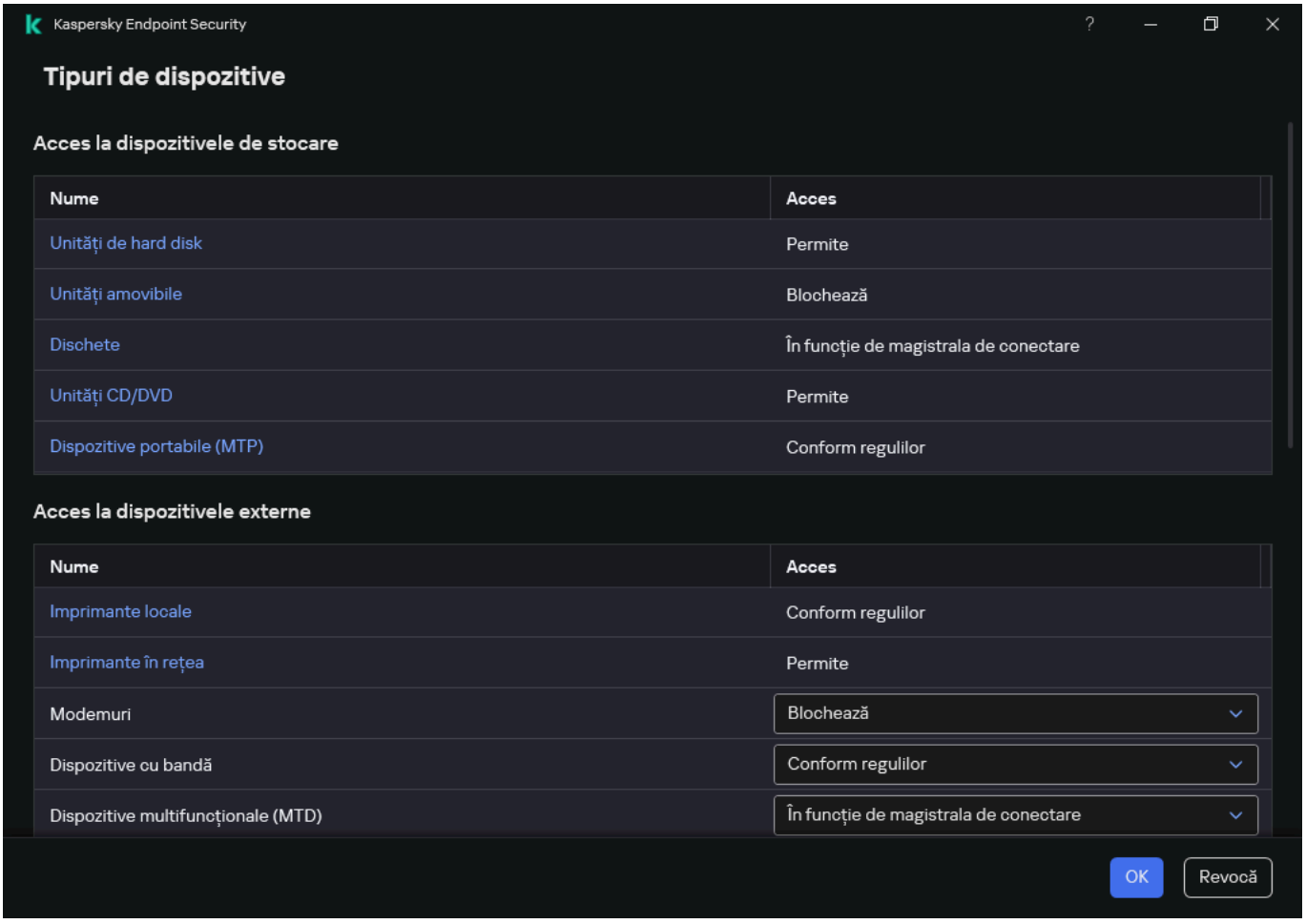
Cum se configurează regulile de acces la dispozitivele Bluetooth în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Security Controls → Control dispozitive**.

3. În blocul **Setări de acces**, fă clic pe butonul **Dispozitive și rețele Wi-Fi**.

   Fereastra deschisă afișează regulile de acces pentru toate dispozitivele care sunt incluse în clasificarea componentelor Control dispozitive.



Tipuri de dispozitive din componenta Control dispozitive

4. În blocul **Acces la dispozitivele externe**, faceți clic pe linkul **Bluetooth**.

   Aceasta deschide setările de acces la dispozitivul Bluetooth.

5. În **Acces**, configurați modul de acces la dispozitivele Bluetooth: **Permite**, **Blochează**, **Permite și nu înregistra în jurnal**.

6. Dacă selectați modul **Blochează**, puteți permite conectarea doar a dispozitivelor de intrare Bluetooth (tastaturi, mouse-uri etc.). Pentru aceasta, în **Excluderi**, bifați caseta de selectare **Dispozitive de intrare (mouse-uri și tastaturi)**.

7. Salvați-vă modificările.

Controlul imprimării

Controlul imprimării nu este acceptat pe computerele bazate pe arhitectura Arm.

Puteți utiliza opțiunea Controlul imprimării pentru a configura accesul utilizatorului la imprimantele locale și în rețea.

Controlul imprimantei locale

Kaspersky Endpoint Security permite configurarea accesului la imprimantele locale pe două niveluri: *conectare* și *imprimare*.

Kaspersky Endpoint Security controlează conectarea la imprimanta locală prin următoarele magistrale: USB, Port serial (COM), Port paralel (LPT).

Kaspersky Endpoint Security controlează conectarea imprimantelor locale la porturile COM și LPT numai la nivelul magistralei. Astfel, pentru a preveni conectările la imprimantă prin porturile COM și LPT, trebuie să selectezi modul de acces În funcție de magistrala de conectare pentru imprimantele locale și să interzici conectările la magistralele COM și LPT.

Pentru imprimantele conectate la USB, aplicația exercită controlul pe două niveluri: tip dispozitiv (imprimante locale) și magistrală de conectare (USB).

Puteți selecta unul dintre următoarele moduri de acces la imprimantele locale prin USB:

- **Permite** ✓. Kaspersky Endpoint Security oferă tuturor utilizatorilor acces deplin la imprimantele locale. Utilizatorii pot conecta imprimante și pot imprima documente folosind mijloacele oferite de sistemul de operare.

- **Blochează** ⊘. Kaspersky Endpoint Security blochează conectarea imprimantelor locale. Aplicația permite doar conectarea imprimantelor de încredere.

- **În funcție de magistrala de conectare**. Kaspersky Endpoint Security permite conectarea la imprimantele locale, în conformitate cu starea conexiunii magistralei USB (**Permite** sau **Blochează**).
- **Conform regulilor**. Pentru a controla imprimarea, trebuie să adăugați *reguli de imprimare*. În reguli, puteți selecta utilizatorii sau un grup de utilizatori pentru care doriți să permiteți sau să blocați accesul la imprimarea documentelor pe imprimantele locale.

Controlul imprimantei în rețea

Kaspersky Endpoint Security permite configurarea accesului la imprimare pe imprimantele în rețea. Poți selecta unul dintre următoarele moduri de acces la imprimantele în rețea:

- **Permite și nu înregistra în jurnal**. Kaspersky Endpoint Security nu controlează imprimarea pe imprimantele de rețea. Aplicația oferă acces la imprimare tuturor utilizatorilor și nu salvează informații despre imprimare în jurnalul de evenimente.
- **Permite**. Kaspersky Endpoint Security oferă acces tuturor utilizatorilor la imprimarea pe imprimantele în rețea.
- **Blochează**. Kaspersky Endpoint Security restricționează accesul la imprimantele în rețea pentru toți utilizatorii. Aplicația permite accesul numai la imprimantele de încredere.
- **Conform regulilor**. Kaspersky Endpoint Security oferă acces la imprimare în conformitate cu regulile de imprimare. În reguli, puteți selecta utilizatorii sau un grup de utilizatori cărora li se va permite sau li se va interzice imprimarea documentelor pe o imprimantă în rețea.

Adăugarea regulilor de imprimare pentru imprimante

Cum se adăugă reguli de imprimare în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Security Controls → Control dispozitive**.
4. În **Setări Control dispozitive**, selectează fila **Tipuri de dispozitive**.

   Tabelul listează regulile de acces pentru toate dispozitivele care sunt prezente în clasificarea componentei Control dispozitive.
5. În meniul contextual pentru tipurile de dispozitive **Imprimante locale** și **Imprimante în rețea**, configurați modul de acces pentru imprimantele relevante: **Permite**, **Blochează**, **Permite și nu înregistra în jurnal** (doar pentru imprimante de rețea) sau **În funcție de magistrala de conectare** (doar pentru imprimante locale).
6. Pentru a configura regulile de imprimare pe imprimantele locale și în rețea, faceți dublu clic pe listele de reguli pentru a le deschide.
7. Selectați **Conform regulilor** ca mod de acces la imprimantă.

8. Selectați utilizatorii sau grupurile de utilizatori cărora doriți să le aplicați regula de imprimare.

   a. Fă clic pe **Adaugă**.

      Aceasta deschide o fereastră pentru adăugarea unei noi reguli de imprimare.

   b. Atribuiți o prioritate regulii. Introducerea unei reguli include următoarele atribute: cont de utilizator, acțiune (permite/blochează) și prioritate.

      O regulă are o prioritate specifică. Dacă un utilizator a fost adăugat la mai multe grupuri, Kaspersky Endpoint Security reglementează accesul la dispozitiv pe baza regulii cu cea mai mare prioritate. Kaspersky Endpoint Security îți permite alocarea unei priorități de la 0 la 10.000. Cu cât valoarea este mai mare, cu atât prioritatea este mai mare. Cu alte cuvinte, o intrare cu valoarea 0 are cea mai scăzută prioritate.

      De exemplu, puteți acorda permisiuni numai de citire grupului Oricine și acorda permisiuni de citire/scriere grupului de administratori. Pentru aceasta, atribuiți o prioritate 1 pentru grupul de administratori și atribuiți o prioritate de 0 pentru grupul Oricine.

      Prioritatea pentru o regulă de blocare este mai mare decât prioritatea pentru o regulă de permitere. Cu alte cuvinte, dacă un utilizator a fost adăugat la mai multe grupuri și prioritatea tuturor regulilor este aceeași, Kaspersky Endpoint Security reglementează accesul dispozitivului pe baza oricărei reguli de blocare existente.

   c. În **Acțiune**, configurați accesul utilizatorului la imprimarea pe imprimantă.

   d. Faceți clic pe **Utilizatori și grupuri** și selectați utilizatorii sau grupurile de utilizatori pentru acces la imprimare. Poți selecta utilizatori în Active Directory, în lista de conturi din Kaspersky Security Center sau introducând manual un nume de utilizator local. Kaspersky recomandă utilizarea conturilor de utilizator locale numai în cazuri speciale, când nu este posibilă utilizarea conturilor de utilizator de domeniu.

   e. Fă clic pe **OK**.

9. Salvați-vă modificările.

Cum se adaugă reguli de imprimare în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Security Controls** → **Device Control**.
5. În blocul **Device access rules**, faceți clic pe linkul **Devices and Wi-Fi networks**.

   Tabelul listează regulile de acces pentru toate dispozitivele care sunt prezente în clasificarea componentei Control dispozitive.
6. Selectați tipul de dispozitiv **Local printers** sau **Network printers**.

   Aceasta deschide regulile de acces la imprimantă.
7. Configurați modul de acces pentru imprimantele relevante: **Allow**, **Block**, **Allow and do not log** (doar pentru imprimante de rețea), **Depends on bus** (doar pentru imprimante locale) sau **Custom**.
8. Dacă selectați modul **Custom**, trebuie să adăugați reguli de imprimare pentru imprimantele locale sau în rețea. Pentru aceasta, faceți clic pe butonul **Add** în tabelul cu regulile de imprimare:

   Aceasta deschide setările noii reguli de imprimare.

9. Atribuiți o prioritate regulii. Introducerea unei reguli include următoarele atribute: cont de utilizator, acțiune (permite/blochează) și prioritate.

   O regulă are o prioritate specifică. Dacă un utilizator a fost adăugat la mai multe grupuri, Kaspersky Endpoint Security reglementează accesul la dispozitiv pe baza regulii cu cea mai mare prioritate. Kaspersky Endpoint Security îți permite alocarea unei priorități de la 0 la 10.000. Cu cât valoarea este mai mare, cu atât prioritatea este mai mare. Cu alte cuvinte, o intrare cu valoarea 0 are cea mai scăzută prioritate.

   De exemplu, puteți acorda permisiuni numai de citire grupului Oricine și acorda permisiuni de citire/scriere grupului de administratori. Pentru aceasta, atribuiți o prioritate 1 pentru grupul de administratori și atribuiți o prioritate de 0 pentru grupul Oricine.

   Prioritatea pentru o regulă de blocare este mai mare decât prioritatea pentru o regulă de permitere. Cu alte cuvinte, dacă un utilizator a fost adăugat la mai multe grupuri și prioritatea tuturor regulilor este aceeași, Kaspersky Endpoint Security reglementează accesul dispozitivului pe baza oricărei reguli de blocare existente.

10. În **Action**, configurați accesul utilizatorului la imprimarea pe imprimantă.

11. În **User or group**, selectați utilizatorii sau grupurile de utilizatori pentru acces la imprimare. Poți selecta utilizatori în Active Directory, în lista de conturi din Kaspersky Security Center sau introducând manual un nume de utilizator local. Kaspersky recomandă utilizarea conturilor de utilizator locale numai în cazuri speciale, când nu este posibilă utilizarea conturilor de utilizator de domeniu.

12. Salvați-vă modificările.

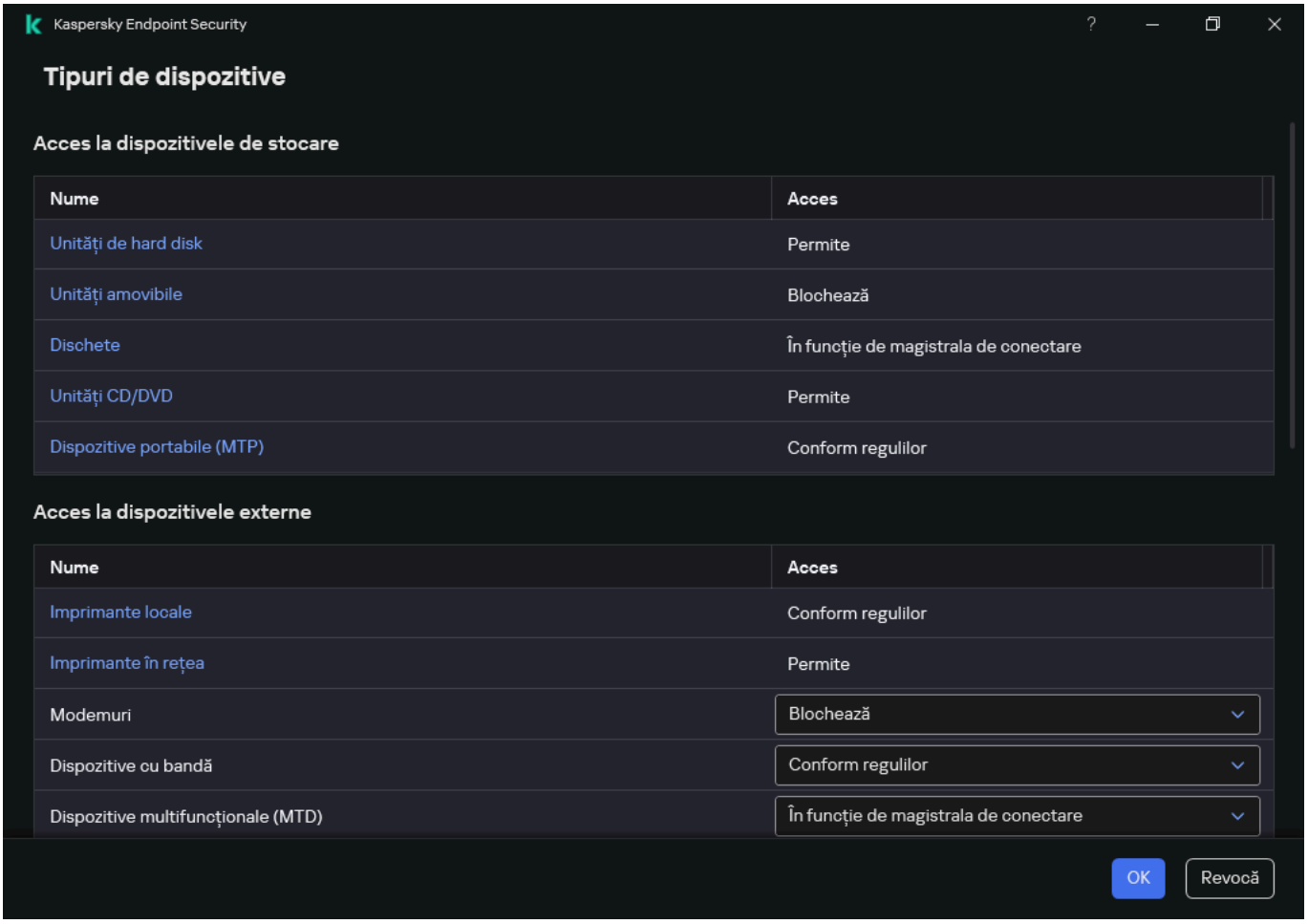
Cum se adaugă reguli de imprimare în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Security Controls** → **Control dispozitive**.

3. În blocul **Setări de acces**, fă clic pe butonul **Dispozitive și rețele Wi-Fi**.

Fereastra deschisă afișează regulile de acces pentru toate dispozitivele care sunt incluse în clasificarea componentelor Control dispozitive.



Tipuri de dispozitive din componenta Control dispozitive

4. În **Acces la dispozitivele externe**, faceți clic pe **Imprimante locale** sau **Imprimante în rețea**.

   Aceasta deschide o fereastră cu reguli de acces la imprimantă.

5. În **Acces la imprimantele locale** sau **Acces la imprimantele în rețea**, configurați modul de acces pentru imprimante: **Permite**, **Blochează**, **Permite și nu înregistra în jurnal** (doar pentru imprimante de rețea), **În funcție de magistrala de conectare** (doar pentru imprimante locale) sau **Conform regulilor**.

6. Dacă selectați modul **Conform regulilor**, trebuie să adăugați reguli de imprimare pentru imprimante. Selectați utilizatorii sau grupurile de utilizatori cărora doriți să le aplicați regula de imprimare.

   a. Fă clic pe **Adaugă**.

      Aceasta deschide o fereastră pentru adăugarea unei noi reguli de imprimare.

   b. Atribuiți o prioritate regulii. Introducerea unei reguli include următoarele atribute: cont de utilizator, permisiuni (permite/blochează) și prioritate.

      O regulă are o prioritate specifică. Dacă un utilizator a fost adăugat la mai multe grupuri, Kaspersky Endpoint Security reglementează accesul la dispozitiv pe baza regulii cu cea mai mare prioritate. Kaspersky Endpoint Security îți permite alocarea unei priorități de la 0 la 10.000. Cu cât valoarea este mai mare, cu atât prioritatea este mai mare. Cu alte cuvinte, o intrare cu valoarea 0 are cea mai scăzută prioritate.

      De exemplu, puteți acorda permisiuni numai de citire grupului Oricine și acorda permisiuni de citire/scriere grupului de administratori. Pentru aceasta, atribuiți o prioritate 1 pentru grupul de administratori și atribuiți o prioritate de 0 pentru grupul Oricine.

Prioritatea pentru o regulă de blocare este mai mare decât prioritatea pentru o regulă de permitere. Cu alte cuvinte, dacă un utilizator a fost adăugat la mai multe grupuri și prioritatea tuturor regulilor este aceeași, Kaspersky Endpoint Security reglementează accesul dispozitivului pe baza oricărei reguli de blocare existente.

c. În **Acțiune**, configurați permisiunile utilizatorului pentru accesul la imprimare.

d. În **Utilizatori și grupuri**, selectați utilizatorii sau grupurile de utilizatori pentru acces la imprimare. Poți selecta utilizatori în Active Directory, în lista de conturi din Kaspersky Security Center sau introducând manual un nume de utilizator local. Kaspersky recomandă utilizarea conturilor de utilizator locale numai în cazuri speciale, când nu este posibilă utilizarea conturilor de utilizator de domeniu.

7. Salvați-vă modificările.

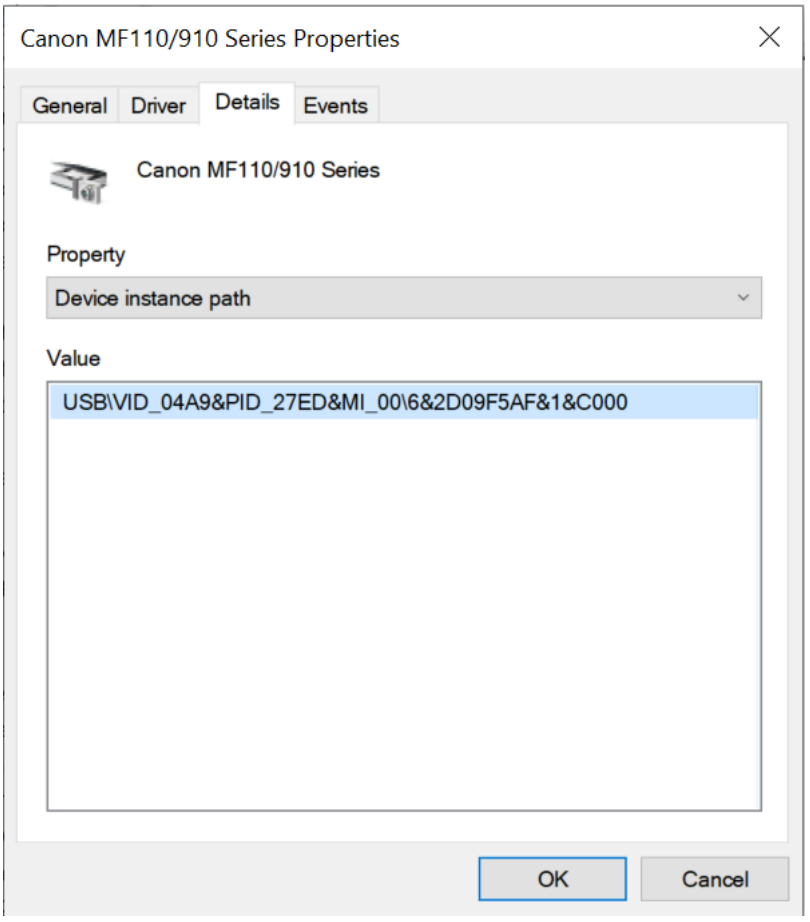
Imprimante de încredere

Dispozitivele de încredere sunt dispozitivele la care utilizatorii specificați în setările pentru dispozitive de încredere au acces complet în orice moment.

Procedura pentru adăugarea de imprimante de încredere este exact la fel ca pentru alte tipuri de dispozitive de încredere. Puteți adăuga imprimante locale după ID sau modelul dispozitivului. Puteți adăuga imprimante în rețea numai după ID-ul dispozitivului.

Pentru a adăuga o imprimantă locală de încredere după ID, veți avea nevoie de un ID unic (Hardware ID – HWID). Puteți găsi ID-ul în proprietățile dispozitivului, utilizând instrumentele sistemului de operare (vezi figura de mai jos). Instrumentul Device Manager vă permite să faceți acest lucru. ID-ul unei imprimante locale poate arăta astfel: `6&2D09F5AF&1&C000`. Adăugarea dispozitivelor după ID este convenabilă dacă doriți să adăugați mai multe dispozitive specifice. Puteți folosi și măști.

Pentru a adăuga o imprimantă locală de încredere după modelul dispozitivului, veți avea nevoie de Vendor ID (VID) și Product ID (PID). Puteți găsi ID-urile în proprietățile dispozitivului, utilizând instrumentele sistemului de operare (vezi figura de mai jos). Șablon pentru introducerea VID și PID: `VID_04A9&PID_27FD`. Adăugarea dispozitivelor după model este convenabilă dacă utilizați dispozitive ale unui anumit model în organizația dvs. În acest fel, puteți adăuga toate dispozitivele acestui model.



ID dispozitiv în Manager dispozitive

Pentru a adăuga o imprimantă în rețea de încredere, veți avea nevoie de ID-ul dispozitivului acesteia. Pentru imprimantele în rețea, ID-ul dispozitivului poate fi numele de rețea al imprimantei (numele imprimantei partajate), adresa IP a imprimantei sau adresa URL a imprimantei.

Controlul conexiunilor Wi-Fi

Componenta Control dispozitive permite gestionarea conexiunii Wi-Fi a computerului (laptopului). Rețelele Wi-Fi publice pot fi nesigure, iar utilizarea unor astfel de rețele poate duce la pierderea datelor. Componenta Control dispozitive vă permite să blocați un utilizator să se conecteze la Wi-Fi sau să permiteți conectarea numai la rețele de încredere. De exemplu, puteți permite conectarea numai la rețeaua Wi-Fi corporativă care este suficient de sigură. Component Control dispozitive va bloca accesul la toate rețelele Wi-Fi, cu excepția celor specificate în lista de încredere.

Pe computerele care rulează Windows 11, trebuie să activezi Serviciile de localizare pentru a controla conexiunile Wi-Fi. Pentru aceasta, trebuie să activezi comutatorul **Servicii de localizare** în setările sistemului de operare (**Setări** → **Confidențialitate și securitate** → **Locație**). Dacă serviciile de localizare sunt dezactivate, Kaspersky Endpoint Security nu controlează conexiunile la rețelele Wi-Fi.

Cum se restricționează conexiunile Wi-Fi în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Security Controls** → **Control dispozitive**.
4. În **Setări Control dispozitive**, selectează fila **Tipuri de dispozitive**.

   Tabelul listează regulile de acces pentru toate dispozitivele care sunt prezente în clasificarea componentei Control dispozitive.
5. În meniul contextual pentru tipul de dispozitiv **Wi-Fi**, selectați acțiunea Control dispozitive care este efectuată atunci când vă conectați la Wi-Fi: **Permite** (), **Blochează** () sau **Blochează cu excepții** ().
6. Dacă ați selectat opțiunea **Blochează cu excepții**, creați o listă cu rețelele Wi-Fi de încredere:

   a. Faceți dublu clic pentru a deschide lista de rețele Wi-Fi de încredere.

   b. În blocul **Rețele Wi-Fi de încredere**, fă clic pe butonul **Adaugă**.

   c. Aceasta deschide o fereastră; în acea fereastră, configurați rețeaua Wi-Fi de încredere (vezi figura de mai jos):

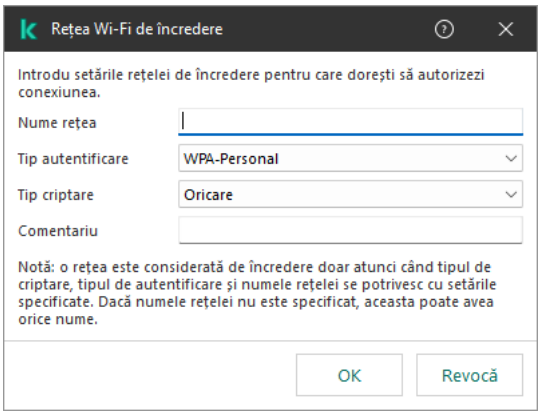
   - **Nume rețea**. Numele sau SSID-ul (Service Set Identifier) rețelei Wi-Fi.
   - **Tip autentificare**. Tipul de autentificare utilizat la conectarea la rețeaua Wi-Fi.

     Începând cu Kaspersky Endpoint Security for Windows versiunea 12.0, a fost adăugat la aplicație suport pentru protocolul WPA3. Dacă pe un computer este aplicată o politică Kaspersky Endpoint Security versiunea 12.2, protocolul WPA2 este selectat pe computerele cu Kaspersky Endpoint Security versiunea 11.11.0 și anterioară; WPA2 / WPA3 este selectat pentru versiunile de 12.0 până la 12.1; WPA3 este selectat pentru versiunile 12.2 și versiunile ulterioare.
   - **Tip criptare**. Tipul de criptare folosit pentru a proteja traficul Wi-Fi.
   - **Comentariu**. Mai multe informații despre rețeaua Wi-Fi adăugată.

   Puteți vizualiza setările rețelei Wi-Fi de încredere în setările routerului.

   O rețea Wi-Fi este considerată a fi de încredere dacă setările sale corespund tuturor setărilor specificate în regulă.

7. Salvați-vă modificările.



Setările rețelei Wi-Fi de încredere

Cum să restricționați conexiunile Wi-Fi în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Security Controls** → **Device Control**.
5. În **Device access rules**, selectează fila **Devices and Wi-Fi networks**.

   Tabelul listează regulile de acces pentru toate dispozitivele care sunt prezente în clasificarea componentei Control dispozitive.
6. În blocul **Wi-Fi networks**, faceți clic pe linkul **Wi-Fi**.
7. În fereastra care se deschide, selectează acțiunea de Control dispozitive efectuată la conectarea la o rețea Wi-Fi: **Allow**, **Block**, sau **Block with exclusions**.
8. Dacă ați selectat opțiunea **Block with exclusions**, creați o listă cu rețelele Wi-Fi de încredere:

   a. Faceți dublu clic pentru a deschide lista de rețele Wi-Fi de încredere.

   b. În blocul **Trusted Wi-Fi networks**, fă clic pe butonul **Add**.

   c. Aceasta deschide o fereastră; în acea fereastră, configurați rețeaua Wi-Fi de încredere (vezi figura de mai jos):

   - **Name**. Numele sau SSID-ul (Service Set Identifier) rețelei Wi-Fi.
   - **Authentication type**. Tipul de autentificare utilizat la conectarea la rețeaua Wi-Fi.

     Începând cu Kaspersky Endpoint Security for Windows versiunea 12.0, a fost adăugat la aplicație suport pentru protocolul WPA3. Dacă pe un computer este aplicată o politică Kaspersky Endpoint Security versiunea 12.2, protocolul WPA2 este selectat pe computerele cu Kaspersky Endpoint Security versiunea 11.11.0 și anterioară; WPA2 / WPA3 este selectat pentru versiunile de 12.0 până la 12.1; WPA3 este selectat pentru versiunile 12.2 și versiunile ulterioare.

- **Encryption type**. Tipul de criptare folosit pentru a proteja traficul Wi-Fi.
- **Comment**. Mai multe informații despre rețeaua Wi-Fi adăugată.

Puteți vizualiza setările rețelei Wi-Fi de încredere în setările routerului.

> O rețea Wi-Fi este considerată a fi de încredere dacă setările sale corespund tuturor setărilor specificate în regulă.

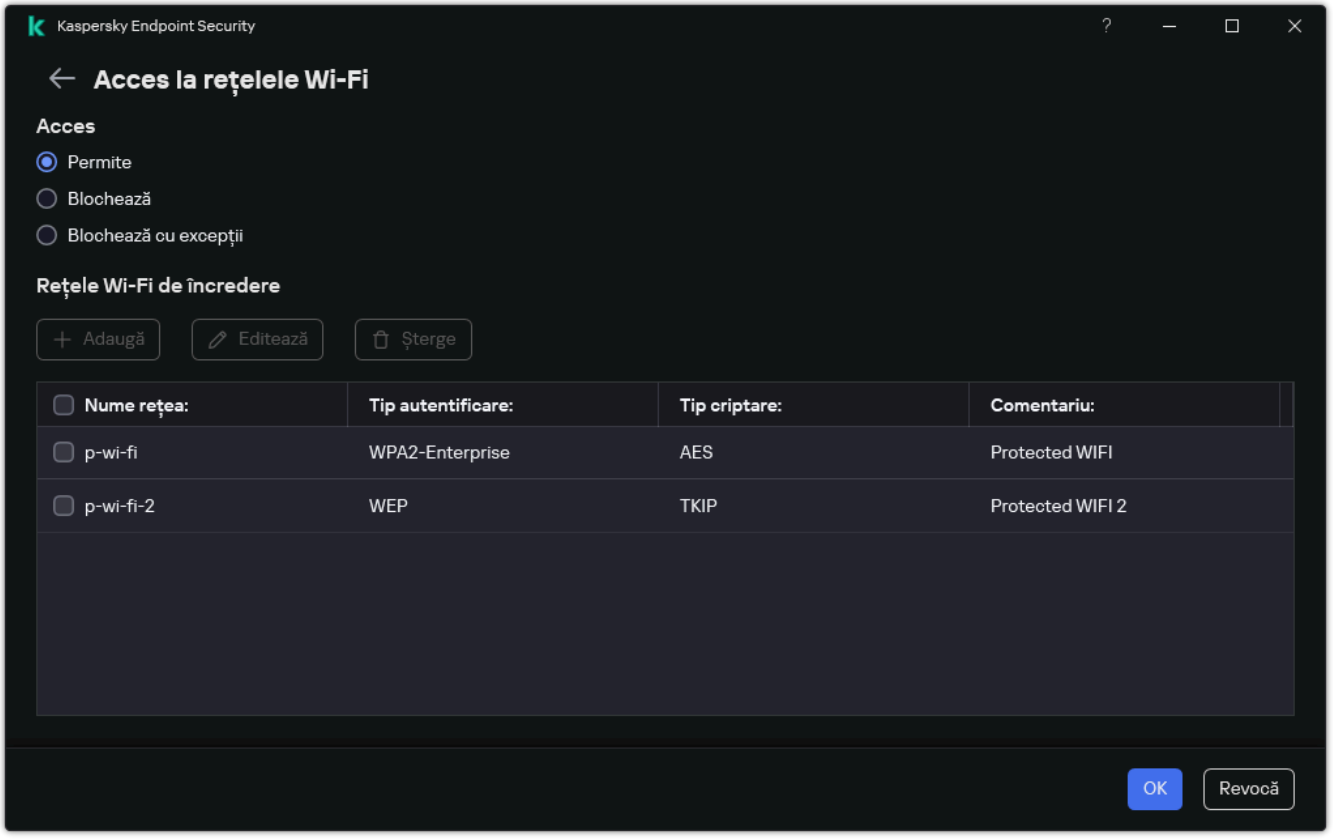
9. Salvați-vă modificările.

Cum se restricționează conexiunile Wi-Fi în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Security Controls → Control dispozitive**.
3. În blocul **Setări de acces**, fă clic pe butonul **Dispozitive și rețele Wi-Fi**.

   Fereastra deschisă afișează regulile de acces pentru toate dispozitivele care sunt incluse în clasificarea componentelor Control dispozitive.
4. În blocul **Acces la rețelele Wi-Fi**, faceți clic pe linkul **Wi-Fi**.

   Fereastra deschisă afișează regulile de acces la rețeaua Wi-Fi.



Setări de acces la rețeaua Wi-Fi

5. În opțiunea **Acces**, selectați acțiunea Control dispozitive efectuată atunci când vă conectați la Wi-Fi: **Permite**, **Blochează**, sau **Blochează cu excepții**.

6. Dacă ați selectat opțiunea **Blochează cu excepții**, creați o listă cu rețelele Wi-Fi de încredere:

   a. În blocul **Rețele Wi-Fi de încredere**, fă clic pe butonul **Adaugă**.

   b. Aceasta deschide o fereastră; în acea fereastră, configurați rețeaua Wi-Fi de încredere (vezi figura de mai jos):

   - **Nume rețea**. Numele sau SSID-ul (Service Set Identifier) rețelei Wi-Fi.
   - **Tip autentificare**. Tipul de autentificare utilizat la conectarea la rețeaua Wi-Fi.

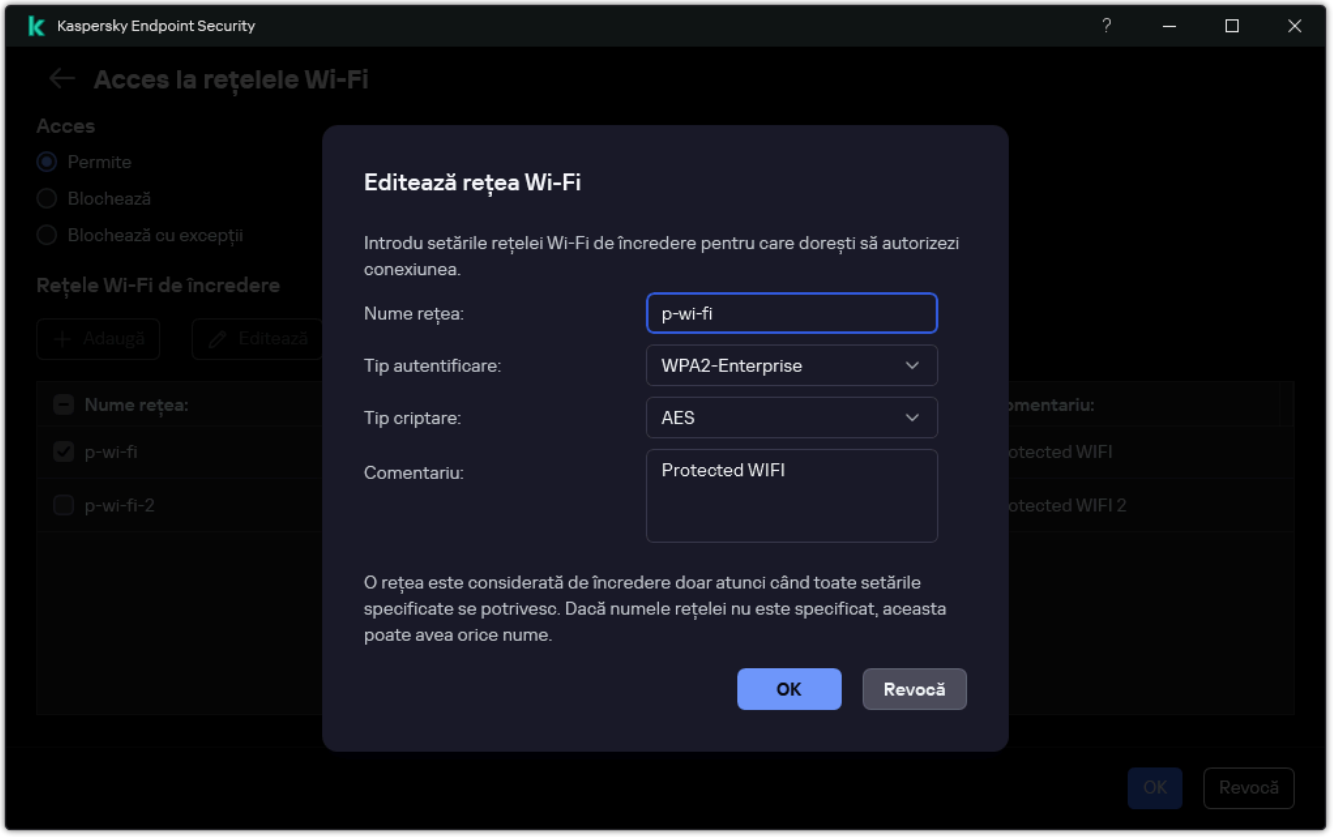
     Începând cu Kaspersky Endpoint Security for Windows versiunea 12.0, a fost adăugat la aplicație suport pentru protocolul WPA3. Dacă pe un computer este aplicată o politică Kaspersky Endpoint Security versiunea 12.2, protocolul WPA2 este selectat pe computerele cu Kaspersky Endpoint Security versiunea 11.11.0 și anterioară; WPA2 / WPA3 este selectat pentru versiunile de 12.0 până la 12.1; WPA3 este selectat pentru versiunile 12.2 și versiunile ulterioare.

   - **Tip criptare**. Tipul de criptare folosit pentru a proteja traficul Wi-Fi.
   - **Comentariu**. Mai multe informații despre rețeaua Wi-Fi adăugată.

   Puteți vizualiza setările rețelei Wi-Fi de încredere în setările routerului.

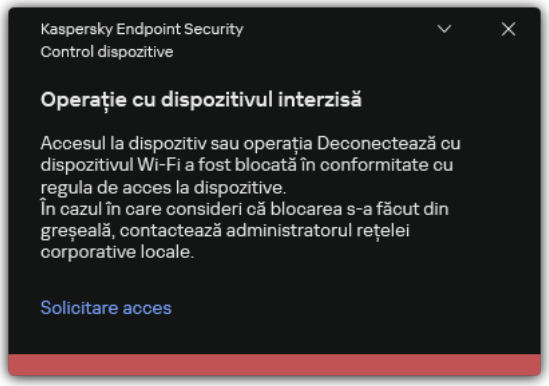
   O rețea Wi-Fi este considerată a fi de încredere dacă setările sale corespund tuturor setărilor specificate în regulă.

7. Salvați-vă modificările.



Setările rețelei Wi-Fi de încredere

Ca urmare, atunci când un utilizator încearcă să se conecteze la o rețea Wi-Fi care nu este listată ca fiind de încredere, aplicația blochează conexiunea și afișează o notificare (vezi figura de mai jos).



Notificări ale componentei Control dispozitive

Monitorizarea utilizării unităților amovibile

Monitorizarea utilizării unităților amovibile include:

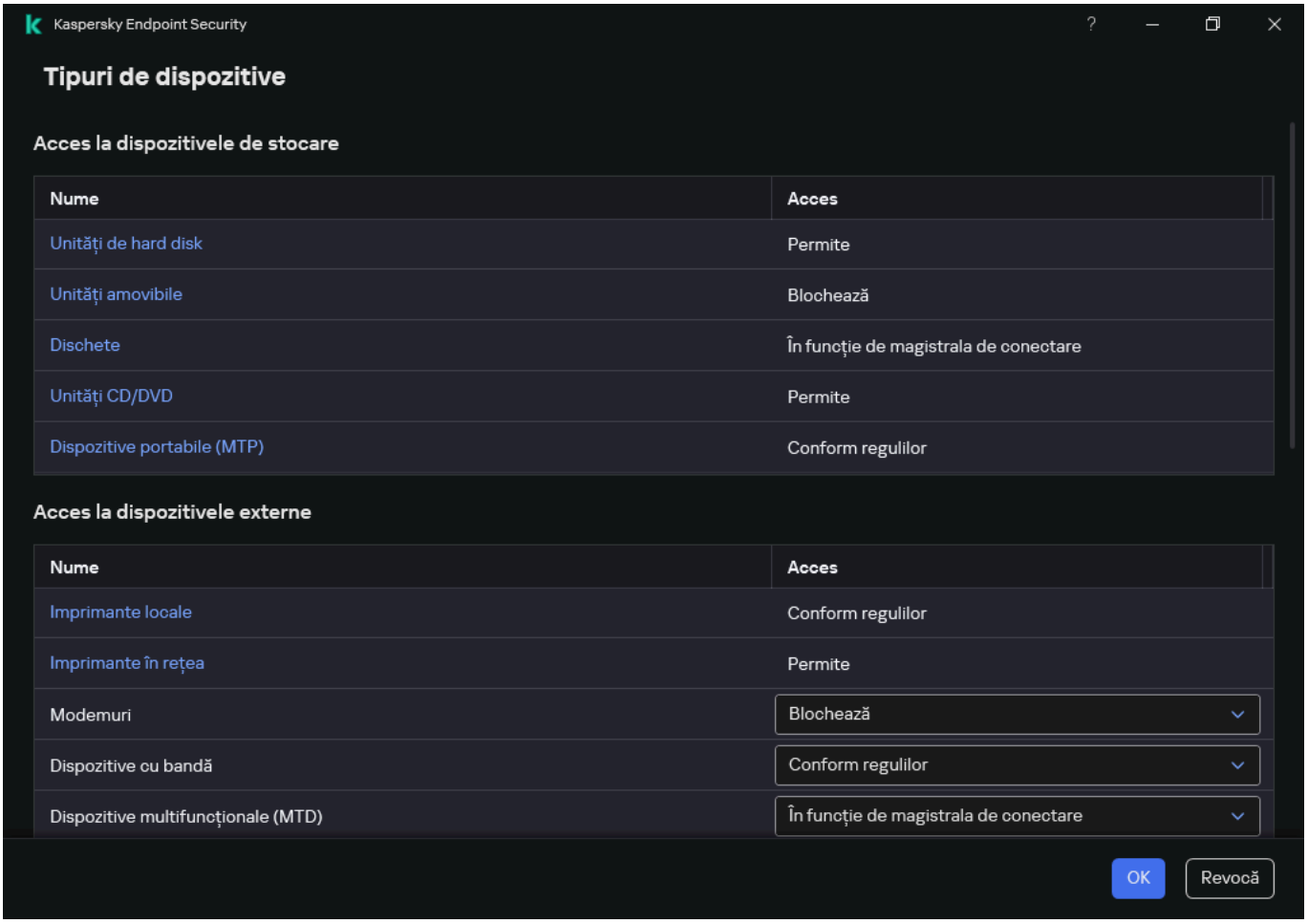
- monitorizarea operațiunilor asupra fișierelor de pe unitățile amovibile,
- monitorizarea conectării și deconectării unităților amovibile de încredere.

  Kaspersky Endpoint Security permite monitorizarea conectării și deconectării tuturor dispozitivelor de încredere și nu numai a unităților amovibile. Puteți activa înregistrarea în jurnal a evenimentelor în setări notificări pentru componenta Control dispozitive. Evenimentele au nivelul de securitate *Mesaj de informare*.

Pentru a permite monitorizarea utilizării unității amovibile:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Security Controls → Control dispozitive**.
3. În blocul **Setări de acces**, fă clic pe butonul **Dispozitive și rețele Wi-Fi**.

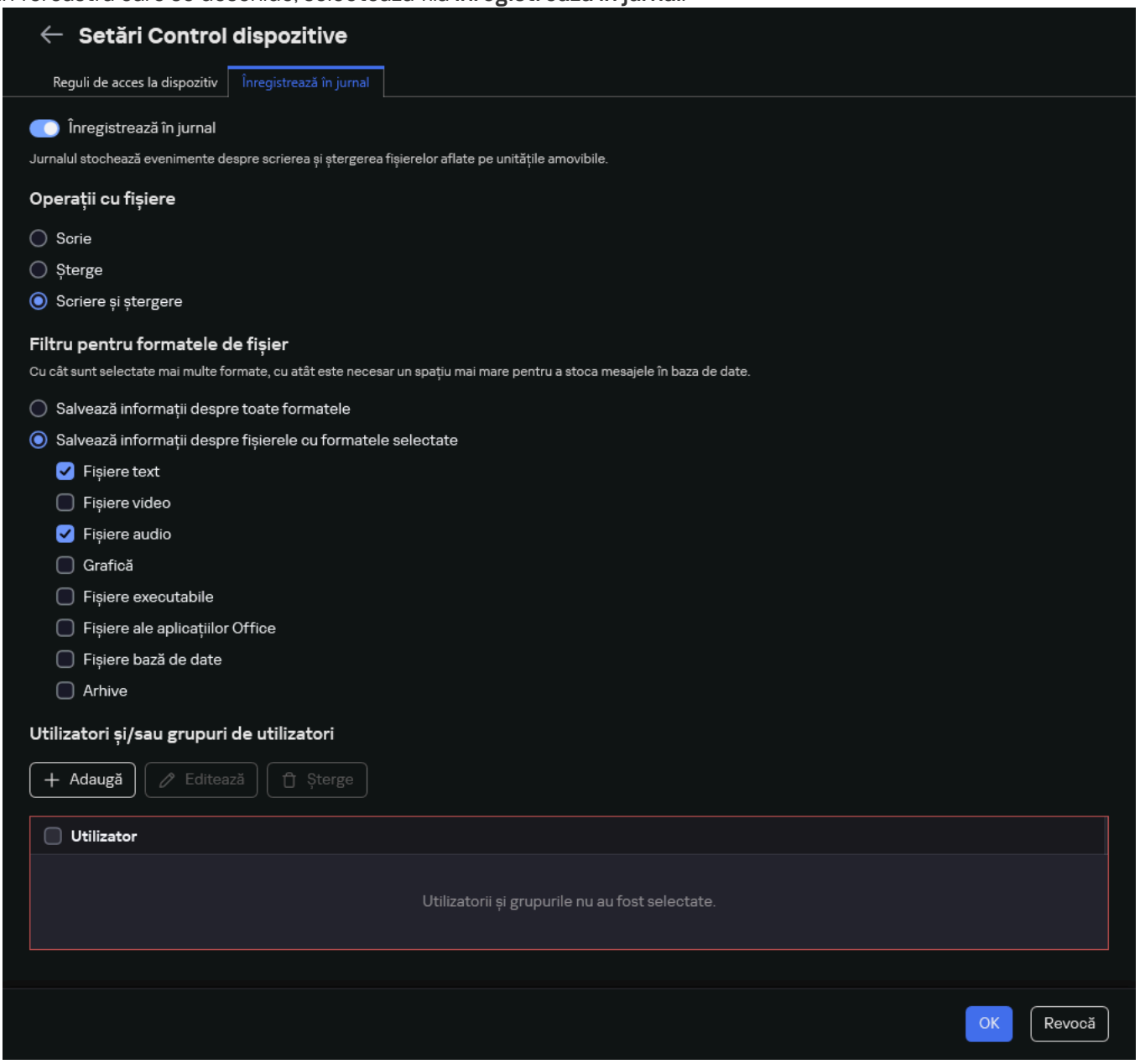
Fereastra deschisă afișează regulile de acces pentru toate dispozitivele care sunt incluse în clasificarea componentelor Control dispozitive.



Tipuri de dispozitive din componenta Control dispozitive

4. În secțiunea **Acces la dispozitivele de stocare**, selectați **Unități amovibile**.

5. În fereastra care se deschide, selectează fila **Înregistrează în jurnal**.



Setările de monitorizare a utilizării unității amovibile

6. Duceți comutatorul **Înregistrează în jurnal** la poziția activat.

7. În blocul **Operații cu fișiere**, selectați operațiile pe care doriți să le monitorizați: **Scrie**, **Șterge**.

8. În blocul **Filtru pentru formatele de fișier**, selectați formatele fișierelor ale căror operațiuni asociate ar trebui înregistrate de Control dispozitive.

9. Selectați utilizatorii sau grupul de utilizatori a căror utilizare a unităților amovibile care doriți să o monitorizați.

10. Salvați-vă modificările.

Ca urmare, când utilizatorii scriu în fișiere amplasate pe unități amovibile sau șterg fișiere de pe unități amovibile, Kaspersky Endpoint Security va salva informații despre aceste operațiuni în jurnalul de evenimente și va trimite evenimente către Kaspersky Security Center. Poți vizualiza evenimente asociate cu fișiere de pe unități amovibile în Consola de administrare Kaspersky Security Center din spațiul de lucru al nodului **Administration Server** din fila **Events**. Pentru ca evenimentele să fie afișate în jurnalul de evenimente Kaspersky Endpoint Security local, trebuie să bifezi caseta de selectare **S-a efectuat o operațiune cu fișiere** în setările de notificare pentru componenta Control dispozitive.

Modificarea duratei memorării în cache

Componenta Control dispozitive înregistrează evenimente legate de dispozitivele monitorizate, cum ar fi conectarea și deconectarea unui dispozitiv, citirea unui fișier de pe un dispozitiv, scrierea unui fișier pe un dispozitiv și alte evenimente. Componenta Control dispozitive permite sau blochează acțiunea în conformitate cu setările Kaspersky Endpoint Security.

Componenta Control dispozitive salvează informații despre evenimente pentru o anumită perioadă de timp numită *perioada memorării în cache*. Dacă informațiile despre un eveniment sunt stocate în cache și acest eveniment se repetă, nu este necesar să anunțați Kaspersky Endpoint Security despre acesta sau să afișați o altă solicitare pentru acordarea accesului la acțiunea corespunzătoare, cum ar fi conectarea unui dispozitiv. Astfel, lucrul cu un dispozitiv este mai convenabil.

Un eveniment este considerat un eveniment dublură dacă toate setările următoare ale evenimentului se potrivesc cu înregistrarea din cache:

- ID-ul dispozitivului
- SID-ul contului de utilizator care încearcă să acceseze
- Categoria dispozitivului
- Acțiunea luată cu dispozitivul
- Permisiunea aplicației pentru această acțiune: permisă sau refuzată
- Calea către procesul utilizat pentru a efectua acțiunea
- Fișierul accesat

Înainte de a schimba perioada memorării în cache, dezactivați Autoprotecția Kaspersky Endpoint Security. După modificarea perioadei memorării în cache, activați Autoprotecția.

Pentru a schimba perioada memorării în cache:

1. Deschideți editorul de registry de pe computer.
2. În editorul de registry, accesați următoarea secțiune:
   - Pentru sistemele de operare pe 64 de biți:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\environment]`
   - Pentru sistemele de operare pe 32 de biți:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES\environment]`
3. Deschideți `DeviceControlEventsCachePeriod` pentru editare.
4. Definiți numărul de minute în care componenta Control dispozitive trebuie să salveze informații despre un eveniment înainte ca aceste informații să fie șterse.

Acțiuni cu dispozitive de încredere

Dispozitivele de încredere sunt dispozitivele la care utilizatorii specificați în setările pentru dispozitive de încredere au acces complet în orice moment.

Pentru a lucra cu dispozitive de încredere, puteți acorda acces unui utilizator individual, unui grup de utilizatori sau tuturor utilizatorilor organizației.

De exemplu, dacă organizația dvs. nu permite utilizarea unităților amovibile, dar administratorii folosesc unități amovibile în activitatea lor, puteți permite unități amovibile numai pentru un grup de administratori. Pentru a face acest lucru, adăugați unitățile amovibile în lista de încredere și configurați permisiunile de acces ale utilizatorului.

Nu este recomandat să adăugați mai mult de 5000 de dispozitive de încredere, deoarece acest lucru poate cauza instabilitatea sistemului.

Kaspersky Endpoint Security vă permite să adăugați un dispozitiv la lista de încredere în următoarele moduri:

- Dacă Kaspersky Security Center nu este implementat în organizația dvs., puteți conecta dispozitivul la computer și să îl adăugați la lista de încredere din setările aplicației. Pentru a distribui lista dispozitivelor de încredere pe toate computerele din organizația dvs., puteți activa îmbinarea listelor dispozitivelor de încredere într-o politică sau puteți utiliza procedura de export/import.

- Dacă Kaspersky Security Center este implementat în organizația dvs., puteți detecta toate dispozitivele conectate de la distanță și puteți crea o listă de dispozitive de încredere în politică. Lista dispozitivelor de încredere va fi disponibilă pe toate computerele cărora li se aplică politica.

Kaspersky Endpoint Security permite controlul utilizării dispozitivelor de încredere (conectare și deconectare). Puteți activa înregistrarea în jurnal a evenimentelor în setări notificări pentru componenta Control dispozitive. Evenimentele au nivelul de securitate *Informational messages*.

Adăugarea unui dispozitiv la lista De încredere din interfața aplicației

În mod implicit, atunci când un dispozitiv este adăugat la lista de dispozitive de încredere, accesul la dispozitiv este acordat tuturor utilizatorilor (grupul de utilizatori Toți).

Pentru a adăuga un dispozitiv la lista De încredere din interfața aplicației:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Security Controls → Control dispozitive**.

3. În blocul **Setări de acces**, fă clic pe butonul **Dispozitive de încredere**.

   Aceasta deschide lista dispozitivelor de încredere.

4. Fă clic pe **Selectează**.

   Aceasta deschide lista dispozitivelor conectate. Lista de dispozitive depinde de valoarea selectată în lista verticală **Afișează dispozitive conectate**.

5. În lista de dispozitive, selectați dispozitivul pe care doriți să îl adăugați la lista de încredere.

   Kaspersky Endpoint Security nu acceptă adăugarea de dispozitive de tip **Dischete** în lista de încredere.

6. În câmpul **Comentariu**, puteți furniza orice informații relevante despre dispozitivul de încredere.

7. Selectează utilizatorii sau grupul de utilizatori pentru care dorești să permiți accesul la dispozitive de încredere.

   Poți selecta utilizatori în Active Directory, în lista de conturi din Kaspersky Security Center sau introducând manual un nume de utilizator local. Kaspersky recomandă utilizarea conturilor de utilizator locale numai în cazuri speciale, când nu este posibilă utilizarea conturilor de utilizator de domeniu.

8. Salvați-vă modificările.

Adăugarea unui dispozitiv la lista De încredere din Kaspersky Security Center

Kaspersky Security Center primește informații despre dispozitive dacă Kaspersky Endpoint Security este instalat pe computere și funcția Control dispozitive este activată. Nu este posibil să adăugați un dispozitiv la lista de încredere, cu excepția cazului în care informații despre acel dispozitiv sunt disponibile în Kaspersky Security Center.

Puteți adăuga un dispozitiv la lista de încredere conform următoarelor date:

- **Dispozitive după ID**. Fiecare dispozitiv are un identificator unic (ID-ul hardware sau HWID). Poți vedea ID-ul în proprietățile dispozitivului utilizând instrumentele sistemului de operare. Exemplu de ID dispozitiv: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Adăugarea dispozitivelor după ID este convenabilă dacă doriți să adăugați mai multe dispozitive specifice.

- **Dispozitive după model**. Fiecare dispozitiv are un ID de vânzător (VID) și un ID de produs (PID). Poți vedea ID-urile în proprietățile dispozitivului utilizând instrumentele sistemului de operare. Șablon pentru introducerea VID și PID: `VID_1234&PID_5678`. Adăugarea dispozitivelor după model este convenabilă dacă utilizați dispozitive ale unui anumit model în organizația dvs. În acest fel, puteți adăuga toate dispozitivele acestui model.

- **Dispozitive după masca de ID**. Dacă utilizați mai multe dispozitive cu ID-uri similare, puteți adăuga dispozitive la lista de încredere folosind măști. Caracterul `*` înlocuiește orice set de caractere. Kaspersky Endpoint Security nu acceptă caracterul `?` atunci când introduceți o mască. De exemplu, `WDC_C*`.

- **Dispozitive după masca modelului**. Dacă utilizați mai multe dispozitive cu VID sau PID similare (de exemplu, dispozitive de la același producător), puteți adăuga dispozitive la lista de încredere folosind măști. Caracterul `*` înlocuiește orice set de caractere. Kaspersky Endpoint Security nu acceptă caracterul `?` atunci când introduceți o mască. De exemplu, `VID_05AC&PID_*`.

Modificarea listei de dispozitive de încredere poate fi blocată de proprietățile politicii părinte. Pentru a modifica lista, trebuie să permiteți modificarea setărilor zonei de încredere în Web Console („lacătul" trebuie să fie deblocat).

Zonele de încredere sunt grupate diferit în Consola de administrare (MMC) și în Web Console. De asemenea, modul în care se împiedică modificarea parametrilor zonei de încredere este diferit („lacăte" diferite). Vă recomandăm să utilizați exclusiv Web Console pentru gestionarea aplicației. În cazul în care configurați zona de încredere pe console diferite, este posibil ca plug-inul de gestionare să reseteze „lacătul" la starea implicită.

Pentru a adăuga un dispozitiv la lista de dispozitive de încredere:

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Security Controls → Control dispozitive**.
4. În partea dreaptă a ferestrei, selectați fila **Dispozitive de încredere**.
5. Bifați caseta de selectare **Îmbină valorile în momentul moștenirii** dacă doriți să creați o listă consolidată de dispozitive de încredere pentru toate computerele companiei.

   Listele dispozitivelor de încredere din politicile principale și secundare vor fi îmbinate. Listele vor fi îmbinate dacă funcția de îmbinare a valorilor în momentul moștenirii este activată. Dispozitivele de încredere din politica principală sunt afișate în politicile secundare într-o vizualizare numai citire. Nu este posibilă modificarea sau ștergerea dispozitivelor de încredere din politica principală.
6. Faceți clic pe butonul **Adaugă** și selectați o metodă pentru adăugarea unui dispozitiv în lista de încredere.
7. Pentru a filtra dispozitivele, selectați un tip de dispozitiv din lista verticală **Tip dispozitiv** (de exemplu, **Unități amovibile**).

   Kaspersky Endpoint Security nu acceptă adăugarea de dispozitive de tip **Dischete** în lista de încredere.
8. În câmpul **Nume/Model**, introduceți ID-ul (VID-ul și PID-ul) sau masca dispozitivului, în funcție de metoda de adăugare selectată.

   Adăugarea dispozitivelor după masca de model (VID și PID) funcționează după cum urmează: dacă introduceți o mască de model care nu se potrivește cu niciun model, Kaspersky Endpoint Security verifică dacă ID-ul dispozitivului (HWID) se potrivește cu masca. Kaspersky Endpoint Security verifică doar partea din ID-ul dispozitivului care determină producătorul și tipul dispozitivului (`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`). Dacă masca de model se potrivește cu această parte a ID-ului dispozitivului, dispozitivele care se potrivesc cu masca vor fi adăugate la lista dispozitivelor de încredere de pe computer. În același timp, lista dispozitivelor din Kaspersky Security Center rămâne goală când faceți clic pe butonul **Refresh**. Pentru a afișa corect lista dispozitivelor, puteți adăuga dispozitive după masca de ID a dispozitivului.
9. Pentru a filtra dispozitivele, în câmpul **Computer**, introduceți numele computerului sau o mască pentru numele computerului la care este conectat dispozitivul.

   Caracterul `*` înlocuiește orice set de caractere. Caracterul `?` înlocuiește orice caracter.
10. Faceți clic pe butonul **Refresh**.

    Tabelul afișează o listă de dispozitive care îndeplinesc criteriile de filtrare definite.
11. Bifați caseta de selectare de lângă numele dispozitivelor pe care doriți să le adăugați în lista de încredere.
12. În câmpul **Comentariu**, introduceți o descriere a motivului pentru adăugarea dispozitivelor în lista de încredere.
13. Faceți clic pe butonul **Select** din dreapta câmpului **Permite pentru utilizatori și/sau grupuri de utilizatori**.

14. Poți selecta utilizatori în Active Directory, în lista de conturi din Kaspersky Security Center sau introducând manual un nume de utilizator local. Kaspersky recomandă utilizarea conturilor de utilizator locale numai în cazuri speciale, când nu este posibilă utilizarea conturilor de utilizator de domeniu.

    În mod implicit, accesul la dispozitivele de încredere este permis pentru grupul Toți.

15. Salvați-vă modificările.

    Când un dispozitiv este conectat, Kaspersky Endpoint Security verifică lista de dispozitive de încredere pentru un utilizator autorizat. Dacă dispozitivul este de încredere, Kaspersky Endpoint Security permite accesul la dispozitiv cu toate permisiunile, chiar dacă accesul la tipul de dispozitiv sau la magistrala de conexiune este refuzat. Dacă dispozitivul nu este de încredere și accesul este refuzat, puteți solicita accesul la dispozitivul blocat.

Exportul și importul listei de dispozitive de încredere

Pentru a distribui lista de dispozitive de încredere către toate computerele din organizația dvs., puteți utiliza procedura de export/import.

De exemplu, dacă trebuie să distribuiți o listă cu unitățile amovibile disponibile, trebuie să procedați după cum urmează:

1. Conectați succesiv unitățile amovibile la computerul dvs.
2. În setările aplicației Kaspersky Endpoint Security, adăugați unitățile amovibile în lista de încredere. Dacă este necesar, configurați permisiunile de acces ale utilizatorului. De exemplu, permiteți doar administratorului să acceseze unitățile amovibile.
3. Exportați lista de dispozitive de încredere în setările Kaspersky Endpoint Security (consultați instrucțiunile de mai jos).
4. Distribuiți lista de dispozitive de încredere către alte computere din organizația dvs. De exemplu, introduceți fișierul într-un director partajat.
5. Importați lista de dispozitive de încredere în setările Kaspersky Endpoint Security pe alte computere din organizație (consultați instrucțiunile de mai jos).

Pentru a importa sau exporta lista de dispozitive de încredere:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Security Controls** → **Control dispozitive**.
3. În blocul **Setări de acces**, fă clic pe butonul **Dispozitive de încredere**.

    Aceasta deschide lista dispozitivelor de încredere.

4. Pentru a exporta lista de dispozitive de încredere:

    a. Selectați dispozitivele de încredere pe care doriți să le exportați.

    b. Fă clic pe **Exportă**.

    c. În fereastra care se deschide, specificați numele fișierului XML în care doriți să exporți lista de dispozitive de încredere și selectați directorul în care doriți să salvați acest fișier.

d. Salvați fișierul.

Kaspersky Endpoint Security exportă întreaga listă de dispozitive de încredere în fișierul XML.

5. Pentru a importa lista de dispozitive de încredere:

a. În lista verticală **Importă**, selectați acțiunea relevantă: **Importare și adăugare la existente** sau **Importare și înlocuire existente**.

b. În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de dispozitive de încredere.

c. Deschideți fișierul.

6. Salvați-vă modificările.

Când un dispozitiv este conectat, Kaspersky Endpoint Security verifică lista de dispozitive de încredere pentru un utilizator autorizat. Dacă dispozitivul este de încredere, Kaspersky Endpoint Security permite accesul la dispozitiv cu toate permisiunile, chiar dacă accesul la tipul de dispozitiv sau la magistrala de conexiune este refuzat.

Obținerea accesului la un dispozitiv blocat

Atunci când configurați componenta Control dispozitive, puteți bloca accidental accesul la un dispozitiv care este necesar pentru muncă.

Dacă Kaspersky Security Center nu este implementat în organizația dumneavoastră, puteți oferi acces la un dispozitiv în setările Kaspersky Endpoint Security. De exemplu, puteți adăuga dispozitivul la lista de încredere sau dezactiva componenta Control dispozitive temporar.

Dacă Kaspersky Security Center este implementat în organizația dumneavoastră și o politică a fost aplicată pe computere, puteți oferi acces la un dispozitiv în Consolă de administrare.

Modul online pentru acordarea accesului

Puteți acorda acces la un dispozitiv blocat în modul online numai dacă Kaspersky Security Center este implementat în organizație și o politică a fost aplicată pe computer. Calculatorul trebuie să aibă capacitatea de a stabili o conexiune cu serverul de administrare.

Acordarea accesului în modul online constă în următoarele etape:

1. Utilizatorul trimite administratorului un mesaj care conține o solicitare de acces.

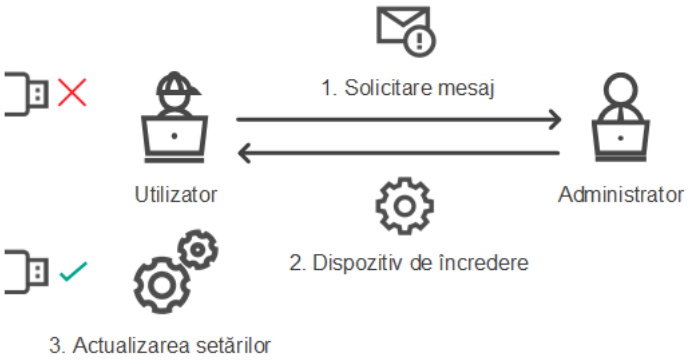
2. Administratorul primește un mesaj cu solicitarea în consola Kaspersky Security Center.

Consola Kaspersky Security Center are o selecție de evenimente prestabilită *User requests* pentru urmărirea ușoară a mesajelor de la utilizatori.

3. Administratorul adaugă dispozitivul în lista de încredere.

Puteți adăuga un dispozitiv de încredere într-o politică pentru grupul de administrare sau în setările locale pentru aplicații pentru un calculator individual.

4. Administratorul actualizează setările Kaspersky Endpoint Security pe computerul utilizatorului.



Schema pentru acordarea accesului la un dispozitiv în modul online

Modul offline pentru acordarea accesului

Puteți acorda acces la un dispozitiv blocat în modul offline doar dacă Kaspersky Security Center este implementat în organizație și o politică a fost aplicată pe computer. În setările politicii, în secțiunea **Control dispozitive**, caseta de selectare **Permite solicitările accesului temporar** trebuie să fie bifată.

Dacă trebuie să acordați acces temporar la un dispozitiv blocat, dar nu puteți adăuga dispozitivul la lista de încredere, puteți acorda acces la dispozitiv în modul offline. În acest fel, puteți acorda acces la un dispozitiv blocat chiar dacă computerul nu are acces la rețea sau dacă computerul este în afara rețelei corporative.

Acordarea accesului în modul offline constă în următoarele etape:

1. Utilizatorul creează un fișier de solicitare acces și îl trimite administratorului.
2. Administratorul creează o cheie de acces din fișierul de solicitare acces și o trimite utilizatorului.
3. Utilizatorul activează cheia de acces.



Schema pentru acordarea accesului la un dispozitiv în modul offline

Modul online pentru acordarea accesului

Puteți acorda acces la un dispozitiv blocat în modul online numai dacă Kaspersky Security Center este implementat în organizație și o politică a fost aplicată pe computer. Calculatorul trebuie să aibă capacitatea de a stabili o conexiune cu serverul de administrare.

Un utilizator solicită acces la un dispozitiv blocat astfel:

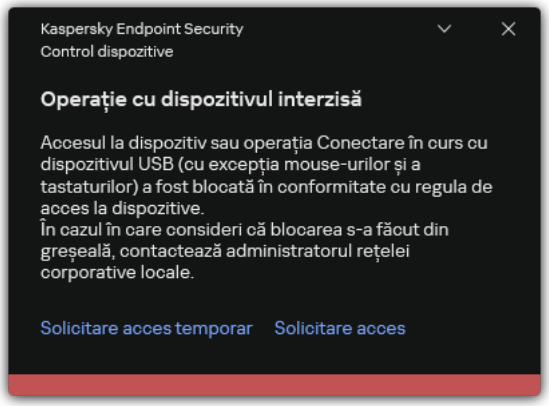
1. Conectați dispozitivul la computer.

   Kaspersky Endpoint Security va afișa o notificare care să ateste că accesul la dispozitiv este blocat (consultați figura de mai jos).

2. Faceți clic pe linkul **Solicitare acces**.

   Se deschide o fereastră cu un mesaj pentru administrator. Acest mesaj conține informații despre dispozitivul blocat.

3. Fă clic pe **Trimitere**.



Notificări ale componentei Control dispozitive

În continuare, administratorul din consola Kaspersky Security Center primește evenimentul *Mesaj către administrator privind blocarea accesului la dispozitiv*. Evenimentul include numele utilizatorului, numele computerului, detalii despre dispozitivul la care utilizatorul încearcă să obțină acces și alte informații. Poți configura modul în care administratorul este notificat cu privire la astfel de evenimente și, de exemplu, poți selecta notificările prin e-mail. Consola Kaspersky Security Center are o selecție de evenimente prestabilită *User requests* pentru urmărirea ușoară a mesajelor de la utilizatori.

Pentru a permite accesul, trebuie să adaugi dispozitivul la lista de încredere. După actualizarea setărilor Kaspersky Endpoint Security pe computer, utilizatorul poate primi acces la dispozitiv.

Modul offline pentru acordarea accesului

Puteți acorda acces la un dispozitiv blocat în modul offline doar dacă Kaspersky Security Center este implementat în organizație și o politică a fost aplicată pe computer. În setările politicii, în secțiunea **Control dispozitive**, caseta de selectare **Permite solicitările accesului temporar** trebuie să fie bifată.

Un utilizator solicită acces la un dispozitiv blocat astfel:

1. Conectați dispozitivul la computer.

   Kaspersky Endpoint Security va afișa o notificare care să ateste că accesul la dispozitiv este blocat (consultați figura de mai jos).

2. Faceți clic pe linkul **Solicitare acces temporar**.

   Acest lucru va deschide o fereastră care conține lista dispozitivelor conectate.

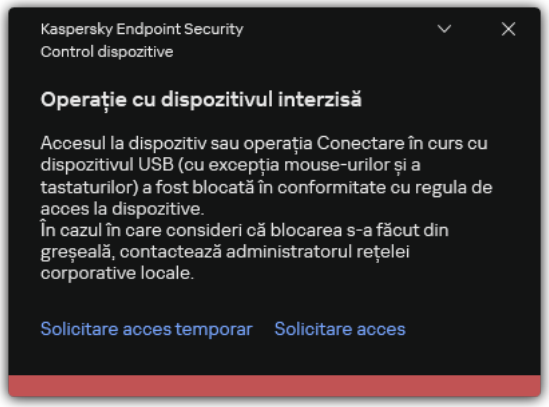
3. Din lista de dispozitive conectate, selectați dispozitivul la care doriți să obțineți acces.

4. Fă clic pe **Generează fișier de solicitare acces**.

5. În câmpul **Durată acces**, specifică perioada de timp pentru care dorești să ai acces la dispozitiv.

6. Salvați fișierul în memoria computerului.

Drept urmare, un fișier de solicitare acces cu extensia *.akey va fi descărcat în memoria computerului. Utilizați orice metodă disponibilă pentru a trimite solicitarea de acces la dispozitiv administratorului rețelei LAN corporative.



Notificări ale componentei Control dispozitive

Cum poate administratorul să creeze o cheie de acces pentru dispozitivul blocat în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.

2. În directorul **Managed devices** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparține computerul client relevant.

3. În spațiul de lucru, selectează fila **Devices**.

4. În lista de computere client, selectați computerul al cărui utilizator trebuie să primească acces temporar la dispozitivul blocat.

5. În meniul contextual al computerului, selectați elementul **Acordare acces în modul offline**.

6. Se deschide o fereastră; în acea fereastră, selectați fila **Control dispozitive**.

7. Faceți clic pe butonul **Răsfoiește** și descărcați fișierul de solicitare acces primit de la utilizator.

   Veți vedea informații despre dispozitivul blocat la care utilizatorul a solicitat acces.

8. Dacă este necesar, modificați valoarea pentru setarea **Durată acces**.

   În mod implicit, setarea **Durată acces** ia valoarea care a fost indicată de utilizator la crearea fișierului de solicitare a accesului.

9. Specifică valoarea pentru setarea **Activare prin**.

   Această setare definește perioada de timp pentru care utilizatorul poate activa accesul la dispozitivul blocat folosind cheia de acces furnizată.

10. Salvați fișierul cheie de acces în memoria computerului.

Cum poate administratorul să creeze o cheie de acces pentru dispozitivul blocat în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Assets (Devices)**.
2. În lista de computere client, selectați computerul al cărui utilizator trebuie să primească acces temporar la dispozitivul blocat.
3. Faceți clic pe butonul puncte de suspensie (...) de deasupra listei de computere și apoi faceți clic pe butonul **Grant access to the device in offline mode**.
4. În fereastra care se deschide, selectați secțiunea **Device Control**.
5. Faceți clic pe butonul **Browse** și descărcați fișierul de solicitare acces primit de la utilizator.

   Veți vedea informații despre dispozitivul blocat la care utilizatorul a solicitat acces.
6. Dacă este necesar, modificați valoarea pentru setarea **Access duration (hours)**.

   În mod implicit, setarea **Access duration (hours)** ia valoarea care a fost indicată de utilizator la crearea fișierului de solicitare a accesului.
7. Specificați perioada de timp în care cheia de acces poate fi activată pe dispozitiv.

   Această setare definește perioada de timp pentru care utilizatorul poate activa accesul la dispozitivul blocat folosind cheia de acces furnizată.
8. Salvați fișierul cheie de acces în memoria computerului.

Drept urmare, cheia de acces a dispozitivului blocat va fi descărcată în memoria computerului. Un fișier cheie de acces are extensia *.acode. Utilizați orice metodă disponibilă pentru a trimite utilizatorului cheia de acces a dispozitivului blocat.

Utilizatorul activează cheia de acces după cum urmează:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Security Controls** → **Control dispozitive**.
3. În blocul **Solicitare acces**, fă clic pe butonul **Solicitare acces la dispozitiv**.
4. În fereastra care se deschide, faceți clic pe butonul **Activare cheie de acces**.
5. În fereastra care se deschide, selectați fișierul cu cheia de acces pentru dispozitiv primit de la administratorul rețelei LAN corporative.

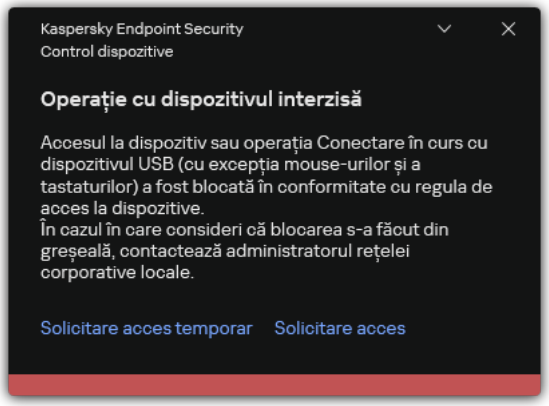
   Aceasta deschide o fereastră care conține informații despre furnizarea accesului.
6. Fă clic pe **OK**.

Drept urmare, utilizatorul primește acces la dispozitiv pentru perioada de timp stabilită de administrator. Utilizatorul primește setul complet de drepturi pentru accesarea dispozitivului (citire și scriere). Când cheia expiră, accesul la dispozitiv va fi blocat. Dacă utilizatorul necesită acces permanent la dispozitiv, adăugați dispozitivul în lista de încredere.

Editarea șabloanelor mesajelor componentei Control dispozitive

Atunci când utilizatorul încearcă să acceseze un dispozitiv blocat, aplicația Kaspersky Endpoint Security afișează un mesaj în care se specifică faptul că dispozitivul este blocat sau că o operațiune cu conținutul dispozitivului este interzisă. Experții Kaspersky oferă utilizatorului un șablon de mesaj care descrie motivele pentru care accesul la dispozitiv a fost blocat (vezi figura de mai jos).

Sunt furnizate variabile speciale pentru gestionarea șabloanelor pentru mesaje (de exemplu, %USER_NAME%). Variabilele permit utilizarea unui singur șablon de mesaj pentru computere diferite. La generarea unui mesaj, Kaspersky Endpoint Security preia valoarea variabilei din setările sistemului de operare și o inserează în mesajul corespunzător computerului, utilizatorului și evenimentului specific.



Notificări ale componentei Control dispozitive

Dacă utilizatorul consideră că accesul la dispozitiv este blocat în mod eronat sau că o operațiune cu conținutul de pe dispozitiv a fost interzisă din greșeală, utilizatorul poate trimite un mesaj către administratorul rețelei locale a companiei făcând clic pe linkul din mesajul afișat despre acțiunea blocată. Pentru a face acest lucru, utilizatorul trebuie să facă clic pe butoanele **Solicitare acces** sau **Solicitare acces temporar** și să trimită administratorului un mesaj care descrie situația. De asemenea, poți pregăti un șablon al mesajului pentru administrator, adăugând la acesta date care pot preciza decizia de a permite sau de a bloca accesul la aplicație. După ce utilizatorul solicită accesul, Kaspersky Endpoint Security trimite un eveniment către Kaspersky Security Center: **Mesaj către administrator privind blocarea accesului la dispozitiv**. Descrierea evenimentului conține un mesaj către administrator cu variabile înlocuite. Puteți vizualiza aceste evenimente în consola Kaspersky Security Center, utilizând selecția de evenimente predefinită **User requests**. Dacă organizația dvs. nu are instalat Kaspersky Security Center sau nu există nicio conexiune la serverul de administrare, aplicația va trimite un mesaj administratorului la adresa de e-mail specificată.

Cum se modifică șablonul de mesaj al componentei Application Control în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Security Controls → Control dispozitive**.
4. În blocul **Setări șablon de mesaje**, fă clic pe butonul **Șabloane**.

5. Aceasta deschide o fereastră; în acea fereastră, configurează șabloanele Application Control:

   - **Mesaj despre blocare**. Șablon al mesajului care apare când un utilizator încearcă să acceseze un dispozitiv blocat. Acest mesaj apare, de asemenea, atunci când un utilizator încearcă să efectueze o operație asupra conținutului dispozitivului care a fost blocat pentru acest utilizator.

   - **Mesaj către administrator**. Șablonul mesajului care va fi trimis administratorului rețelei LAN în cazul în care utilizatorul consideră că accesul la un dispozitiv a fost blocat sau o operațiune cu conținutul de pe dispozitiv a fost interzisă din greșeală.

   Pentru a adăuga o variabilă la textul șablonului, plasează cursorul în poziția dorită, fă clic pe **Variabilă** și selectează variabila necesară din lista de opțiuni disponibile.

   De asemenea, poți restaura textul șablonului implicit.

6. Salvați-vă modificările.

Cum se modifică șablonul de mesaj al componentei Control dispozitive în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **Security Controls** → **Device Control**.

5. În blocul **Message templates**, configurează șabloanele pentru mesajele componentei Application Control:

   - **Message to user**. Șablon al mesajului care apare când un utilizator încearcă să acceseze un dispozitiv blocat. Acest mesaj apare, de asemenea, atunci când un utilizator încearcă să efectueze o operație asupra conținutului dispozitivului care a fost blocat pentru acest utilizator.

   - **Message to administrator**. Șablonul mesajului care va fi trimis administratorului rețelei LAN în cazul în care utilizatorul consideră că accesul la un dispozitiv a fost blocat sau o operațiune cu conținutul de pe dispozitiv a fost interzisă din greșeală.

   Pentru a adăuga o variabilă la textul șablonului, plasează cursorul în poziția dorită, fă clic pe **Add variable** și selectează variabila necesară din lista de opțiuni disponibile.

   De asemenea, poți restaura textul șablonului implicit.

6. Salvați-vă modificările.

Cum se schimbă șablonul de mesaj al componentei Control dispozitive în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Security Controls** → **Application Control**.

3. În blocul **Șabloane de mesaje**, configurează șabloanele pentru mesajele componentei Application Control:

   - **Mesaj despre blocare**. Șablon al mesajului care apare când un utilizator încearcă să acceseze un dispozitiv blocat. Acest mesaj apare, de asemenea, atunci când un utilizator încearcă să efectueze o operație asupra conținutului dispozitivului care a fost blocat pentru acest utilizator.

   - **Mesaj către administrator**. Șablonul mesajului care va fi trimis administratorului rețelei LAN în cazul în care utilizatorul consideră că accesul la un dispozitiv a fost blocat sau o operațiune cu conținutul de pe dispozitiv a fost interzisă din greșeală.

   Pentru a adăuga o variabilă la textul șablonului, plasează cursorul în poziția dorită, fă clic pe **Adaugă variabilă** și selectează variabila necesară din lista de opțiuni disponibile.

   De asemenea, poți restaura textul șablonului implicit.

4. Salvați-vă modificările.

Anti-Bridging

Funcția Anti-Bridging inhibă crearea de punți de rețea prin împiedicarea creării simultane a mai multor conexiuni la rețea pentru un computer. Acest lucru vă permite să protejați o rețea corporativă împotriva atacurilor prin rețelele neprotejate și neautorizate.

Funcția Anti-Bridging reglementează stabilirea conexiunilor la rețea prin utilizarea *regulilor de conectare*.

Regulile de conectare sunt create pentru următoarele tipuri de dispozitive predefinite:

- plăci de rețea;
- adaptoare Wi-Fi;
- modemuri.

Dacă este activată o regulă de conectare, Kaspersky Endpoint Security:

- blochează conexiunea activă atunci când stabilește o conexiune nouă, dacă tipul de dispozitiv specificat în regulă este utilizat pentru ambele conexiuni;
- blochează conexiunile stabilite folosind tipurile de dispozitive pentru care sunt folosite reguli cu prioritate mai mică.

Activarea Anti-Bridging

Funcția Anti-Bridging este dezactivată în mod implicit.

Pentru a activa funcția Anti-Bridging:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Security Controls** → **Control dispozitive**.
3. În blocul **Setări de acces**, fă clic pe butonul **Anti-Bridging**.

4. Utilizați comutatorul **Activare Anti-Bridging** pentru a activa sau a dezactiva această caracteristică.
5. Salvați-vă modificările.

După activarea funcției Anti-Bridging, Kaspersky Endpoint Security blochează conexiunile deja stabilite conform regulilor de conectare.

Modificarea stării unei reguli de conectare

Pentru a modifica starea unei reguli de conectare:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Security Controls** → **Control dispozitive**.
3. În blocul **Setări de acces**, fă clic pe butonul **Anti-Bridging**.
4. În blocul **Reguli pentru dispozitive**, selectați regula a cărei stare doriți să o modificați.
5. Utilizați comutatoarele din coloana **Control** pentru a activa sau a dezactiva regula.
6. Salvați-vă modificările.

Modificarea priorității unei reguli de conectare

Pentru a modifica prioritatea unei reguli de conectare:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Security Controls** → **Control dispozitive**.
3. În blocul **Setări de acces**, fă clic pe butonul **Anti-Bridging**.
4. În blocul **Reguli pentru dispozitive**, selectați regula a cărei prioritate doriți să o modificați.
5. Utilizați butoanele **Sus** / **Jos** pentru a seta prioritatea regulii de conectare.

   Cu cât o regulă este poziționată mai sus în lista de reguli, cu atât prioritatea sa este mai mare. Anti-Bridging blochează toate conexiunile, cu excepția uneia, cea stabilită folosind tipul de dispozitiv pentru care se utilizează regula cu cea mai mare prioritate.
6. Salvați-vă modificările.

Control adaptiv al anomaliilor

Această componentă este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Windows pentru stații de lucru. Această componentă nu este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Windows pentru servere.

Componenta Control adaptiv al anomaliilor monitorizează și blochează acțiunile care nu sunt specifice pentru computerele din rețeaua unei companii. Componenta Control adaptiv al anomaliilor utilizează un set de reguli pentru a urmări comportamentul atipic (de exemplu, regula *Pornire Microsoft PowerShell din aplicația Office*). Regulile sunt create de specialiștii Kaspersky pe baza scenariilor tipice de activitate periculoasă. Puteți configura modul în care componenta Control adaptiv al anomaliilor controlează fiecare regulă și, de exemplu, permite executarea scripturilor PowerShell care automatizează anumite activități ale fluxului de lucru. Kaspersky Endpoint Security actualizează setul de reguli împreună cu bazele de date ale aplicațiilor. Actualizările seturilor de reguli trebuie să fie confirmate manual.

Setările componentei Control adaptiv al anomaliilor

Configurarea componentei Control adaptiv al anomaliilor constă în următorii pași:

1. Instruire componentă Control adaptiv al anomaliilor.

   După ce activați componenta Control adaptiv al anomaliilor, regulile sale funcționează în *modul instruire*. În timpul instruirii, componenta Control adaptiv al anomaliilor monitorizează regulile de declanșare și trimite evenimente de declanșare către Kaspersky Security Center. Fiecare regulă are propria sa durată a modului de instruire. Durata modului de instruire este setată de către experții de la Kaspersky. În mod normal, modul de instruire este activ timp de două săptămâni.

   Dacă o regulă nu este declanșată deloc în timpul instruirii, componenta Control adaptiv al anomaliilor va considera acțiunile asociate cu această regulă ca fiind nespecifice. Kaspersky Endpoint Security va bloca toate acțiunile asociate cu acea regulă.

   Dacă o regulă a fost declanșată în timpul instruirii, Kaspersky Endpoint Security înregistrează evenimentele în jurnal în raportul de declanșare a evenimentului și în depozitul **Rule triggers in Smart Training state**.

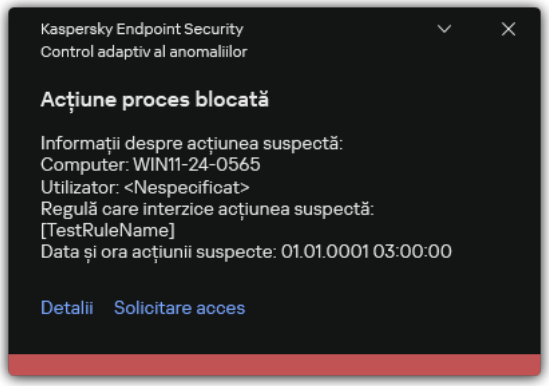
2. Analizarea raportului declanșării regulii.

   Administratorul analizează raportul de declanșare regulii sau conținutul depozitului **Rule triggers in Smart Training state**. Apoi, administratorul poate selecta comportamentul componentei Control adaptiv al anomaliilor atunci când regula este declanșată: să o blocheze sau să o accepte. De asemenea, administratorul poate continua să monitorizeze modul în care funcționează regula și să extindă durata modului de instruire. Dacă administratorul nu întreprinde nicio măsură, aplicația va continua, de asemenea, să funcționeze în modul de instruire. Termenul modului de instruire este repornit.

Componenta Control adaptiv al anomaliilor este configurată în timp real prin următoarele canale:

- Componenta Control adaptiv al anomaliilor începe automat să blocheze acțiunile asociate cu regulile care nu au fost declanșate niciodată în modul de instruire.
- Kaspersky Endpoint Security adaugă noi reguli sau le elimină pe cele învechite.
- Administratorul configurați funcționarea componentei Control adaptiv al anomaliilor după ce a examinat raportul declanșării regulii și conținutul depozitului **Rule triggers in Smart Training state**. Îți recomandăm să verifici raportul privind declanșarea regulilor și conținutul spațiului de stocare **Rule triggers in Smart Training state**.

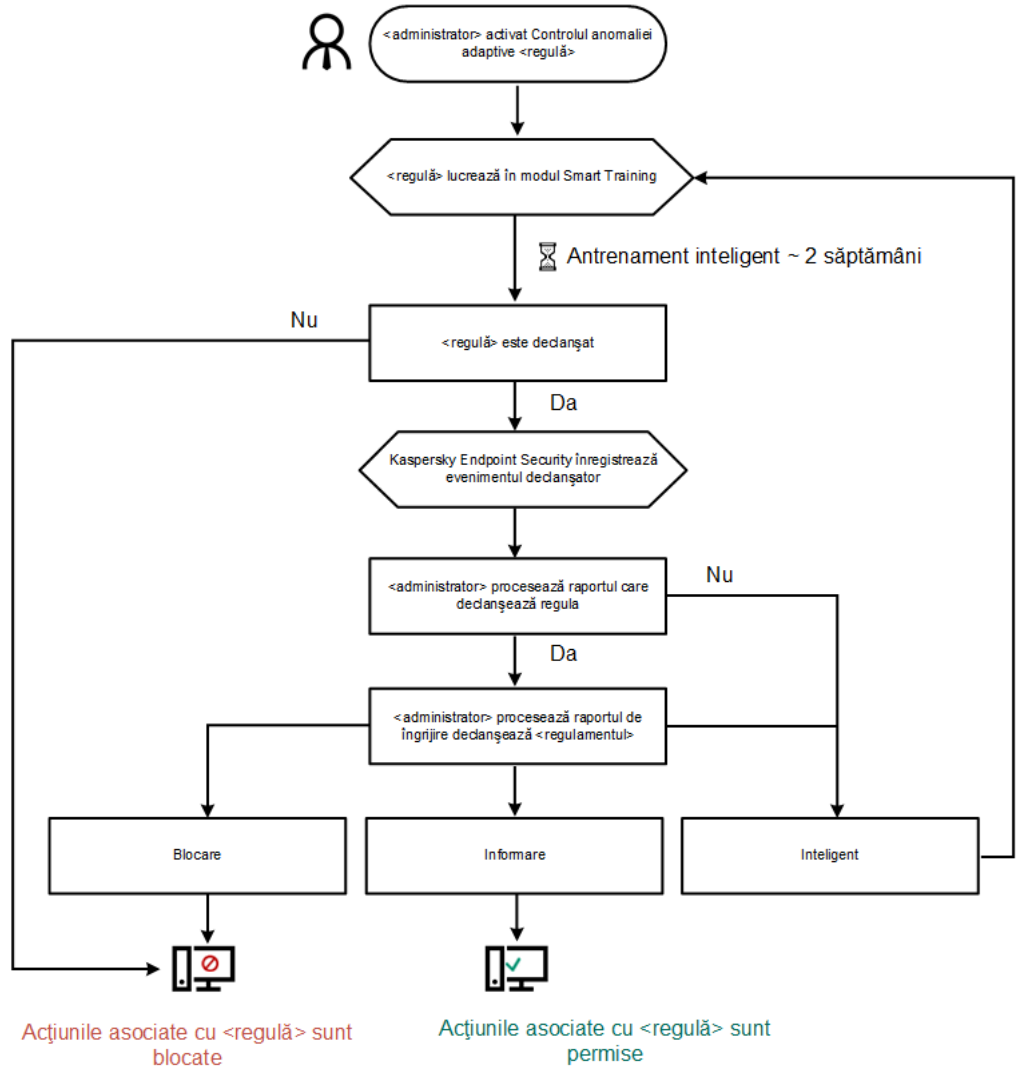
Când o aplicație periculoasă încearcă să efectueze o acțiune, Kaspersky Endpoint Security va bloca acțiunea și va afișa o notificare (consultați figura de mai jos).



Notificările componentei Control adaptiv al anomaliilor

Algoritmul de funcționare al componentei Control adaptiv al anomaliilor

Kaspersky Endpoint Security decide dacă va permite sau va bloca o acțiune asociată cu o regulă pe baza următorului algoritm (consultați figura de mai jos).



Algoritmul de funcționare al componentei Control adaptiv al anomaliilor

Instruire componentă Control adaptiv al anomaliilor

Componenta Control adaptiv al anomaliilor include un set de reguli (modele de comportament). După ce activați componenta Control adaptiv al anomaliilor, regulile sale funcționează în *modul instruire*. În timpul instruirii, componenta Control adaptiv al anomaliilor monitorizează regulile de declanșare și trimite evenimente de declanșare către Kaspersky Security Center. Componenta Control adaptiv al anomaliilor nu blochează activitatea aplicațiilor pe computer, ci doar informează administratorul. De asemenea, poți selecta manual acțiunea care este efectuată atunci când este declanșată o regulă Control adaptiv al anomaliilor.

Cum se vizualizează lista de reguli Control adaptiv al anomaliilor în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.

2. În arborele consolei, selectați **Policies**.

3. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

4. În fereastra politicii, selectați **Security Controls → Adaptive Anomaly Control**.

5. Bifați caseta de selectare **Control adaptiv al anomaliilor**.

6. În **Setări reguli Control adaptiv al anomaliilor**, consultă lista de reguli.
   În mod implicit, toate regulile funcționează în modul **Inteligent**.

7. Dacă este necesar, confirmă actualizarea regulii Control adaptiv al anomaliilor.

8. Dacă este necesar, selectează o acțiune atunci când este declanșată o regulă Control adaptiv al anomaliilor:

   - **Blochează**. Dacă este selectată această acțiune, atunci când o regulă de Control adaptiv al anomaliilor este declanșată, Kaspersky Endpoint Security blochează activitatea acoperită de regulă și introduce o înregistrare ce conține informațiile despre activitate.

   - **Informează**. Dacă este selectată această acțiune, atunci când o regulă de Control adaptiv al anomaliilor este declanșată, Kaspersky Endpoint Security permite activitatea acoperită de regulă și introduce o înregistrare ce conține informațiile despre activitate.

9. Dacă este necesar, dezactivează regulile pe care nu dorești să le utilizezi.

10. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se vizualizează regulile componentei Control adaptiv al anomaliilor în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați fila **Asset management → Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.
   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **Security Controls → Adaptive Anomaly Control**.

5. Duceți comutatorul **Adaptive Anomaly Control ENABLED** la poziția activat.

6. În **Rules**, consultă lista de reguli.
   În mod implicit, toate regulile funcționează în modul **Smart**.

7. Dacă este necesar, confirmă actualizarea regulii Control adaptiv al anomaliilor.

8. Dacă este necesar, selectează o acțiune atunci când este declanșată o regulă Control adaptiv al anomaliilor:

   - **Block**. Dacă este selectată această acțiune, atunci când o regulă de Control adaptiv al anomaliilor este declanșată, Kaspersky Endpoint Security blochează activitatea acoperită de regulă și introduce o înregistrare ce conține informațiile despre activitate.

   - **Inform**. Dacă este selectată această acțiune, atunci când o regulă de Control adaptiv al anomaliilor este declanșată, Kaspersky Endpoint Security permite activitatea acoperită de regulă și introduce o înregistrare ce conține informațiile despre activitate.

9. Dacă este necesar, dezactivează regulile pe care nu dorești să le utilizezi.

10. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se vizualizează lista de reguli Control adaptiv al anomaliilor în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Security Controls** → **Adaptive Anomaly Control**.

3. Duceți comutatorul **Control adaptiv al anomaliilor** la poziția activat.

4. În blocul **Reguli**, faceți clic pe linkul **Editează regulile**.

   Se deschide lista regulilor de control adaptiv al anomaliilor. În mod implicit, toate regulile funcționează în modul **Inteligentă**.

5. Dacă este necesar, confirmă actualizarea regulii Control adaptiv al anomaliilor.

6. Dacă este necesar, selectează o acțiune atunci când este declanșată o regulă Control adaptiv al anomaliilor:

   - **Blochează**. Dacă este selectată această acțiune, atunci când o regulă de Control adaptiv al anomaliilor este declanșată, Kaspersky Endpoint Security blochează activitatea acoperită de regulă și introduce o înregistrare ce conține informațiile despre activitate.

   - **Informează**. Dacă este selectată această acțiune, atunci când o regulă de Control adaptiv al anomaliilor este declanșată, Kaspersky Endpoint Security permite activitatea acoperită de regulă și introduce o înregistrare ce conține informațiile despre activitate.

7. Dacă este necesar, dezactivează regulile pe care nu dorești să le utilizezi.

8. Salvați-vă modificările.

Fiecare regulă are propria sa durată a modului de instruire. Durata modului de instruire este setată de către experții de la Kaspersky. În mod normal, modul de instruire este activ timp de două săptămâni.

Dacă, în timpul instruirii, o regulă nu s-a declanșat niciodată, Control adaptiv al anomaliilor consideră un astfel de comportament atipic și modifică starea regulii în **Blocare inteligentă**. Ulterior, aplicația blochează orice activitate care corespunde acestei reguli.

Dacă o regulă se declanșează în timpul instruirii, trebuie să configurezi manual acțiunea pe care aplicația o aplică activității detectate care corespunde acestei reguli. Dacă nu selectezi acțiunea atunci când regula este declanșată, componenta Control adaptiv al anomaliilor continuă în modul de instruire.

Activarea și dezactivarea unei reguli Control adaptiv al anomaliilor

Pentru a activa sau a dezactiva o regulă Control adaptiv al anomaliilor:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Security Controls** → **Control adaptiv al anomaliilor**.

3. În blocul **Reguli**, fă clic pe butonul **Editează regulile**.

   Se deschide lista regulilor de control adaptiv al anomaliilor.

4. În tabel, selectați un set de reguli (de exemplu, *Activitatea aplicațiilor Office*) și extindeți setul.
5. Selectați o regulă (de exemplu, *Pornire Microsoft PowerShell din aplicația Office*).
6. Utilizați comutatorul din coloana **Condiție** pentru a activa sau a dezactiva regula Control adaptiv al anomaliilor.
7. Salvați-vă modificările.

Modificarea acțiunii efectuate la declanșarea unei reguli Control adaptiv al anomaliilor

Pentru a edita acțiunea efectuată la declanșarea unei reguli Control adaptiv al anomaliilor:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Security Controls → Control adaptiv al anomaliilor**.
3. În blocul **Reguli**, fă clic pe butonul **Editează regulile**.
   Se deschide lista regulilor de control adaptiv al anomaliilor.
4. Selectați o regulă din tabel.
5. Fă clic pe **Editează**.
   Se deschide fereastra de proprietăți a regulii de control adaptiv al anomaliilor.
6. În blocul **Acțiune**, selectați una dintre următoarele opțiuni:
   - **Inteligent**. Dacă este selectată această opțiune, regula Control adaptiv al anomaliilor funcționează în starea Instruire inteligentă pentru o perioadă de timp definită de experții Kaspersky. În acest mod, atunci când este declanșată o regulă Control adaptiv al anomaliilor, Kaspersky Endpoint Security permite activitatea acoperită de regulă și înregistrează în jurnal o intrare în spațiul de stocare **Rule triggers in Smart Training state** al Kaspersky Security Center Administration Server. Atunci când perioada de timp setată pentru a lucra în starea Instruire inteligentă se încheie, Kaspersky Endpoint Security blochează activitatea acoperită de regula Control adaptiv al anomaliilor și înregistrează în jurnal o intrare care conține informații despre activitate.
   - **Blochează**. Dacă este selectată această acțiune, atunci când o regulă de Control adaptiv al anomaliilor este declanșată, Kaspersky Endpoint Security blochează activitatea acoperită de regulă și introduce o înregistrare ce conține informațiile despre activitate.
   - **Informează**. Dacă este selectată această acțiune, atunci când o regulă de Control adaptiv al anomaliilor este declanșată, Kaspersky Endpoint Security permite activitatea acoperită de regulă și introduce o înregistrare ce conține informațiile despre activitate.
7. Salvați-vă modificările.

Crearea unei excluderi pentru o regulă Control adaptiv al anomaliilor

Nu poți crea mai mult de 1.000 excluderi pentru regulile de Control adaptiv al anomaliilor. Este nerecomandată crearea a mai mult de 200 de excluderi. Pentru a reduce numărul de excluderi utilizate, se recomandă utilizarea măștilor în setările excluderilor.

O excludere pentru o regulă Control adaptiv al anomaliilor include o descriere a obiectelor sursă și țintă. *Obiectul sursă* este obiectul care efectuează acțiunile. *Obiectul țintă* este obiectul asupra căruia se efectuează acțiunile. De exemplu, ați deschis un fișier denumit `file.xlsx`. Ca rezultat, un fișier bibliotecă cu extensia DLL este încărcat în memoria computerului. Această bibliotecă este utilizată de un browser (fișierul executabil denumit `browser.exe`). În acest exemplu, `file.xlsx` este obiectul sursă, Excel este procesul sursă, `browser.exe` este obiectul țintă, iar Browser este procesul țintă.

Pentru a crea o excludere pentru o regulă de control adaptiv al anomaliilor:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Security Controls → Control adaptiv al anomaliilor**.
3. În blocul **Reguli**, fă clic pe butonul **Editează regulile**.

   Se deschide lista regulilor de control adaptiv al anomaliilor.
4. Selectați o regulă din tabel.
5. Fă clic pe **Editează**.

   Se deschide fereastra de proprietăți a regulii de control adaptiv al anomaliilor.
6. În blocul **Excluderi**, fă clic pe butonul **Adaugă**.

   Se deschide fereastra de proprietăți ale excluderii.
7. Selectați utilizatorul pentru care dorești să configurezi o excludere.

   Poți selecta utilizatori în Active Directory, în lista de conturi din Kaspersky Security Center sau introducând manual un nume de utilizator local. Kaspersky recomandă utilizarea conturilor de utilizator locale numai în cazuri speciale, când nu este posibilă utilizarea conturilor de utilizator de domeniu.

   Caracteristica Control adaptiv al anomaliilor nu acceptă excluderi pentru grupuri de utilizatori. Dacă selectați un grup de utilizatori, Kaspersky Endpoint Security nu aplică excluderea.
8. În câmpul **Descriere**, introdu o descriere a excluderii.
9. Definiți setările obiectului sursă sau ale proceselor sursă pornite de obiect:

   - **Proces sursă**. Calea sau masca pentru calea către fișierul sau directorul care conține fișiere (de exemplu, `C:\Dir\File.exe` sau `Dir\*.exe`).
   - **Cod hash proces sursă**. Codul hash SHA256 al fișierului.

- **Obiect sursă**. Calea sau masca pentru calea către fișierul sau directorul care conține fișiere (de exemplu, `C:\Dir\File.exe` sau `Dir\*.exe`). De exemplu, calea fișierului `document.docm`, care folosește un script sau un macro pentru a porni procesele țintă.

  Poți, de asemenea, să specifici alte obiecte de exclus, cum ar fi o adresă Web, o macrocomandă, o comandă din linia de comandă, o cale de registru sau altele. Specificați obiectul după următorul șablon: `object://<object>`, unde `<object>` se referă la numele obiectului, de exemplu, `object://web.site.example.com`, `object://VBA`, `object://ipconfig`, `object://HKEY_USERS`. Puteți utiliza, de asemenea, măști, de exemplu, `object://*C:\Windows\temp\*`.

- **Hash obiect sursă**. Codul hash SHA256 al fișierului.

Regula Control adaptiv al anomaliilor nu se aplică acțiunilor efectuate de către obiect sau proceselor pornite de către obiect.

10. Specificați setările obiectului țintă sau ale proceselor țintă pornite pe obiect.

    - **Proces țintă**. Calea sau masca pentru calea către fișierul sau directorul care conține fișiere (de exemplu, `C:\Dir\File.exe` sau `Dir\*.exe`).

    - **Cod hash proces țintă**. Codul hash SHA256 al fișierului.

    - **Obiect țintă**. Comanda pentru pornirea procesului țintă. Specifică comanda utilizând următorul model `object://<command>`, de exemplu, `object://cmdline:powershell -Command "$result = 'C:\Windows\temp\result_local_users_pwdage.txt'"`. Puteți utiliza, de asemenea, măști, de exemplu, `object://*C:\Windows\temp\*`.

    - **Cod hash obiect țintă**. Codul hash SHA256 al fișierului.

    Regula Control adaptiv al anomaliilor nu se aplică acțiunilor efectuate asupra obiectului sau proceselor pornite pe obiect.

11. Salvați-vă modificările.

Exportarea și importarea de excluderi pentru reguli Control adaptiv al anomaliilor

Pentru a exporta sau importa lista de excluderi pentru regulile selectate:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Security Controls** → **Control adaptiv al anomaliilor**.
3. În blocul **Reguli**, fă clic pe butonul **Editează regulile**.

   Se deschide lista regulilor de control adaptiv al anomaliilor.
4. Pentru a exporta lista de reguli:
   a. Selectați regulile ale căror excepții doriți să le exportați.
   b. Fă clic pe **Exportă**.
   c. În fereastra care se deschide, specificați numele fișierului XML în care doriți să exporți lista de excluderi și selectați directorul în care doriți să salvați acest fișier.

d. Confirmați că doriți să exportați numai excluderile selectate sau exportați întreaga listă de excluderi.

e. Salvați fișierul.

5. Pentru a importa lista de excluderi:

a. Fă clic pe **Importă**.

b. În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de excluderi.

c. Deschideți fișierul.

În cazul în care computerul are deja o listă de excluderi, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul XML.

6. Salvați-vă modificările.

Aplicarea de actualizări pentru reguli Control adaptiv al anomaliilor

Se pot adăuga reguli Control adaptiv al anomaliilor noi la tabelul de reguli și se pot șterge reguli Control adaptiv al anomaliilor din tabelul de reguli la actualizarea bazelor de date antivirus. Kaspersky Endpoint Security distinge reguli Control adaptiv al anomaliilor care trebuie șterse sau adăugate la tabel dacă nu a fost aplicată o actualizare pentru aceste reguli.

Până la aplicarea actualizării, Kaspersky Endpoint Security afișează în tabelul de reguli setul de reguli Control adaptiv al anomaliilor care trebuie șterse de către actualizare și le atribuie starea *Dezactivată*. Nu este posibilă modificarea setărilor acestor reguli.

Pentru a aplica actualizări pentru reguli Control adaptiv al anomaliilor:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Security Controls → Control adaptiv al anomaliilor**.

3. În blocul **Reguli**, fă clic pe butonul **Editează regulile**.

Se deschide lista regulilor de control adaptiv al anomaliilor.

4. În fereastra care se deschide, faceți clic pe butonul **Aprobă actualizările**.

Butonul **Aprobă actualizările** este disponibil dacă este disponibilă o actualizare pentru reguli Control adaptiv al anomaliilor.

5. Salvați-vă modificările.

Editarea șabloanelor de mesaje aferente componentei Control adaptiv al anomaliilor

Când un utilizator încearcă să efectueze o acțiune blocată de regulile Control adaptiv al anomaliilor, Kaspersky Endpoint Security afișează un mesaj care indică faptul că acțiunile potențial dăunătoare sunt blocate. Dacă utilizatorul consideră că o acțiune a fost blocată din greșeală, el poate utiliza linkul din mesajul text pentru a trimite un mesaj administratorului rețelei locale a companiei.

Sunt disponibile șabloane speciale pentru mesajele către administrator despre blocarea acțiunilor potențial dăunătoare. Sunt furnizate variabile speciale pentru gestionarea șabloanelor pentru mesaje (de exemplu, `%USER_NAME%`). Variabilele permit utilizarea unui singur șablon de mesaj pentru computere diferite. La generarea unui mesaj, Kaspersky Endpoint Security preia valoarea variabilei din setările sistemului de operare și o inserează în mesajul corespunzător computerului, utilizatorului și evenimentului specific.

Pentru a edita un șablon de mesaj:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Security Controls** → **Control adaptiv al anomaliilor**.
3. În blocul **Șabloane**, configurați șabloanele pentru mesajele Control adaptiv al anomaliilor:
   - **Mesaj despre blocare**. Șablonul mesajului afișat unui utilizator atunci când este declanșată regula de Control adaptiv al anomaliilor care blochează o acțiune nespecifică.
   - **Mesaj către administrator**. Șablonul mesajului potrivit căruia un utilizator poate fi trimis către administratorului rețelei corporative locale, dacă utilizatorul consideră că blocarea este o greșeală. După ce utilizatorul solicită accesul, Kaspersky Endpoint Security trimite un eveniment către Kaspersky Security Center: **Mesaj către administrator privind blocarea activității aplicației**. Descrierea evenimentului conține un mesaj către administrator cu variabile înlocuite. Puteți vizualiza aceste evenimente în consola Kaspersky Security Center, utilizând selecția de evenimente predefinită **User requests**. Dacă organizația dvs. nu are instalat Kaspersky Security Center sau nu există nicio conexiune la serverul de administrare, aplicația va trimite un mesaj administratorului la adresa de e-mail specificată.

   Pentru a adăuga o variabilă la textul șablonului, plasează cursorul în poziția dorită, fă clic pe **Adaugă variabilă** și selectează variabila necesară din lista de opțiuni disponibile.

   De asemenea, poți restaura textul șablonului implicit utilizând butonul **Resetează**.
4. Salvați-vă modificările.

Monitorizarea operațiunilor componentei Control adaptiv al anomaliilor

Componenta Control adaptiv al anomaliilor include mai multe instrumente de monitorizare. Scopul principal al monitorizării componentei Control adaptiv al anomaliilor este de a configura componenta în timpul instruirii.

Rapoartele componentei Control adaptiv al anomaliilor

Componenta Control adaptiv al anomaliilor utilizează următoarele rapoarte:

- **Raport cu privire la starea regulilor funcției Control adaptiv al anomaliilor**. Raportul conține informații despre starea regulilor de Control adaptiv al anomaliilor (*Off*, *Smart Training*, *Smart Block*, *Notify*, *Block*). Acest raport permite analizarea nivelului de instruire al componentei Control adaptiv al anomaliilor și evaluarea numărului de reguli care au fost comutate de la modul *Smart Training* la modul de funcționare normal (de exemplu, *Smart Block*).

- **Raport privind regulile declanșate ale funcției Control adaptiv al anomaliilor**. Raportul conține informații despre declanșatoarele regulilor. Raportul arată și modul de declanșare a regulii: *Block* (inclusiv *Smart Block*) sau *Notify*. Aceste rapoarte permit evaluarea activității componentei Control adaptiv al anomaliilor pe computerele utilizatorilor.

Cum se vizualizează rapoartele componentei Control adaptiv al anomaliilor în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectează **Security Controls → Control adaptiv al anomaliilor**.
4. Efectuează una dintre următoarele acțiuni:
   - Dacă dorești să vezi raportul cu privire la starea regulilor componentei Control adaptiv al anomaliilor, fă clic pe linkul **Raport cu privire la starea regulilor funcției Control adaptiv al anomaliilor**.
   - Dacă dorești să vezi raportul privind regulile declanșate ale componentei Control adaptiv al anomaliilor, fă clic pe linkul **Raport privind regulile declanșate ale funcției Control adaptiv al anomaliilor**.
5. Începe procesul de generare a raportului.

   Raportul este afișat într-o fereastră nouă.

Cum se vizualizează rapoartele componentei Control adaptiv al anomaliilor în Web Console

1. În fereastra principală a Web Console, selectați fila **Asset management → Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Security Controls → Adaptive Anomaly Control**.

5. În blocul **Rules**, efectuează una dintre următoarele acțiuni:

   - Dacă dorești să vezi raportul cu privire la starea regulilor funcției Control adaptiv al anomaliilor, selectează **View report** → **Rules state**.

   - Dacă dorești să vezi raportul privind regulile declanșate de funcția Control adaptiv al anomaliilor, fă clic pe **View report** → **Detections**.

6. Începe procesul de generare a raportului.

Raportul este afișat într-o fereastră nouă.

Pentru a genera rapoarte în consola Kaspersky Security Center, trebuie să activezi transferul de date către Serverul de administrare. Transferul de date este activat în mod implicit.

Cum se activează transferul de date pentru componenta Control adaptiv al anomaliilor în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.

2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

3. În fereastra politicii, selectați **Setări generale** → **Rapoarte și Spații de stocare**.

4. În blocul **Transfer de date pe serverul de administrare**, fă clic pe butonul **Setări**.

5. Bifează următoarele casete:

   - **Raport cu privire la starea regulilor funcției Control adaptiv al anomaliilor**.

   - **Raport privind regulile declanșate ale funcției Control adaptiv al anomaliilor**.

6. Salvați-vă modificările.

Cum se activează transferul de date pentru componenta Control adaptiv al anomaliilor în Web Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **General Settings** → **KSC Integration**.

5. În **Data transfer to Administration Server**, bifează următoarele casete de selectare:

   - **Report on Adaptive Anomaly Control rules state**.

   - **Report on triggered Adaptive Anomaly Control rules**.

6. Salvați-vă modificările.

Spațiul de stocare Rule triggers in Smart Training state

În modul de instruire, componenta Control adaptiv al anomaliilor trimite informații despre regulile declanșate către un spațiu de stocare separat, **Rule triggers in Smart Training state**. Informațiile despre regulile declanșate sunt reprezentate în spațiul de stocare sub forma unei liste de evenimente. Pentru a ajusta componenta Control adaptiv al anomaliilor, poți fie să confirmi comportamentul atipic pe computer, fie să adaugi o excludere de la regulă.

Evenimentele componentei Control adaptiv al anomaliilor

Componenta Control adaptiv al anomaliilor înregistrează în jurnal evenimentele care declanșează regulile în modurile *Block* (inclusiv *Smart Block*) și *Notify*. Următoarele evenimente sunt prevăzute în acest scop:

Process action blocked

Process action skipped

Evenimentele conțin informații despre activitatea suspectă, inclusiv sumele de control ale fișierelor, utilizatorii implicați, ora de declanșare a regulii și numele computerului. După analizarea evenimentului, poți adăuga imediat excluderi de la regulă în cazul în care consideri că activitatea este legitimă.

Application Control

Application Control administrează pornirea aplicațiilor pe computerele utilizatorilor. Acest lucru vă permite să implementați o politică de securitate corporativă atunci când utilizați aplicații. Application Control reduce, de asemenea, riscul de infectare a computerului prin restricționarea accesului la aplicații.

Configurarea componentei Application Control constă în următorii pași:

1. Crearea categoriilor de aplicații.

   Administratorul creează categorii de aplicații pe care administratorul dorește să le administreze. Categoriile de aplicații sunt destinate tuturor computerelor din rețeaua corporativă, indiferent de grupurile de administrare. Pentru a crea o categorie, puteți utiliza următoarele criterii: Categoria KL (de exemplu, *Browsere* sau altă categorie), cod hash fișier, producător aplicație și alte criterii.

2. Crearea regulilor Application Control.

   Administratorul creează reguli pentru componenta Application Control în politica pentru grupul de administrare. Regula include categoriile de aplicații și starea de pornire a aplicațiilor din aceste categorii: blocate sau permise. Administratorul poate crea mai multe reguli. O aplicație poate îndeplini criteriile mai multor reguli. Prioritatea pentru o regulă de blocare este mai mare decât prioritatea pentru o regulă de permitere. Kaspersky Endpoint Security verifică dacă o aplicație corespunde unei reguli de fiecare dată când este pornită. Kaspersky Endpoint Security compară secvențial aplicația cu toate regulile Application Control.

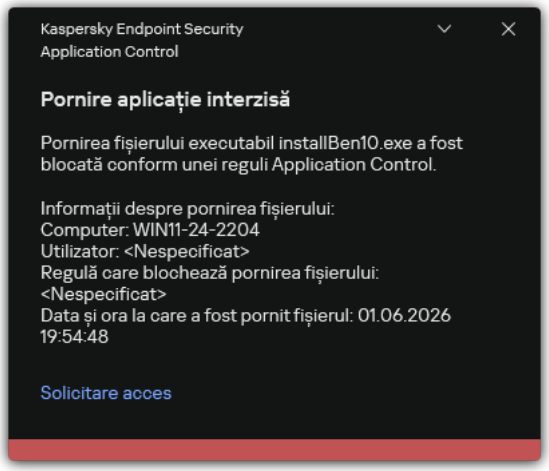
3. Selectarea modului Application Control.

   Administratorul alege modul de lucru cu aplicațiile care nu sunt incluse în niciuna dintre reguli (lista de aplicații respinse sau lista permise).

Când un utilizator încearcă să pornească o aplicație interzisă, Kaspersky Endpoint Security va bloca pornirea aplicației și va afișa o notificare (consultați figura de mai jos).

Este oferit un *mod de testare* pentru a verifica configurația componentei Application Control. În acest mod, Kaspersky Endpoint Security face următoarele:

- Permite pornirea aplicațiilor, inclusiv a celor interzise.
- Afișează o notificare despre pornirea unei aplicații interzise și adaugă informații la raportul de pe computerul utilizatorului.
- Trimite date despre pornirea aplicațiilor interzise către Kaspersky Security Center.



Notificarea Application Control

Modurile de funcționare pentru componenta Application Control

Componenta Application Control funcționează în două moduri:

- **Listă respinse**. În acest mod, Application Control permite utilizatorilor să pornească toate aplicațiile, cu excepția aplicațiilor care sunt interzise în regulile Application Control.

  Acest mod al componentei Application Control este activat în mod implicit.

- **Listă permise**. În acest mod, Application Control blochează posibilitatea utilizatorilor să pornească orice aplicații, cu excepția aplicațiilor care sunt permise și nu sunt interzise în regulile Application Control.

  Dacă regulile de permitere Application Control sunt complet configurate, componenta blochează pornirea tuturor aplicațiilor noi care nu au fost verificate de administratorul rețelei LAN, permițând însă funcționarea sistemului de operare și a aplicațiilor de încredere pe care utilizatorii se bazează în activitatea lor.

  Puteți citi recomandările privind configurarea regulilor Application Control în modul listei permise.

Componenta Application Control poate fi configurată să funcționeze în aceste moduri atât folosind interfața locală Kaspersky Endpoint Security, cât și folosind Kaspersky Security Center.

Cu toate acestea, Kaspersky Security Center oferă instrumente care nu sunt disponibile în interfața locală Kaspersky Endpoint Security, cum ar fi instrumentele care sunt necesare pentru următoarele activități:

- Crearea categoriilor de aplicații.

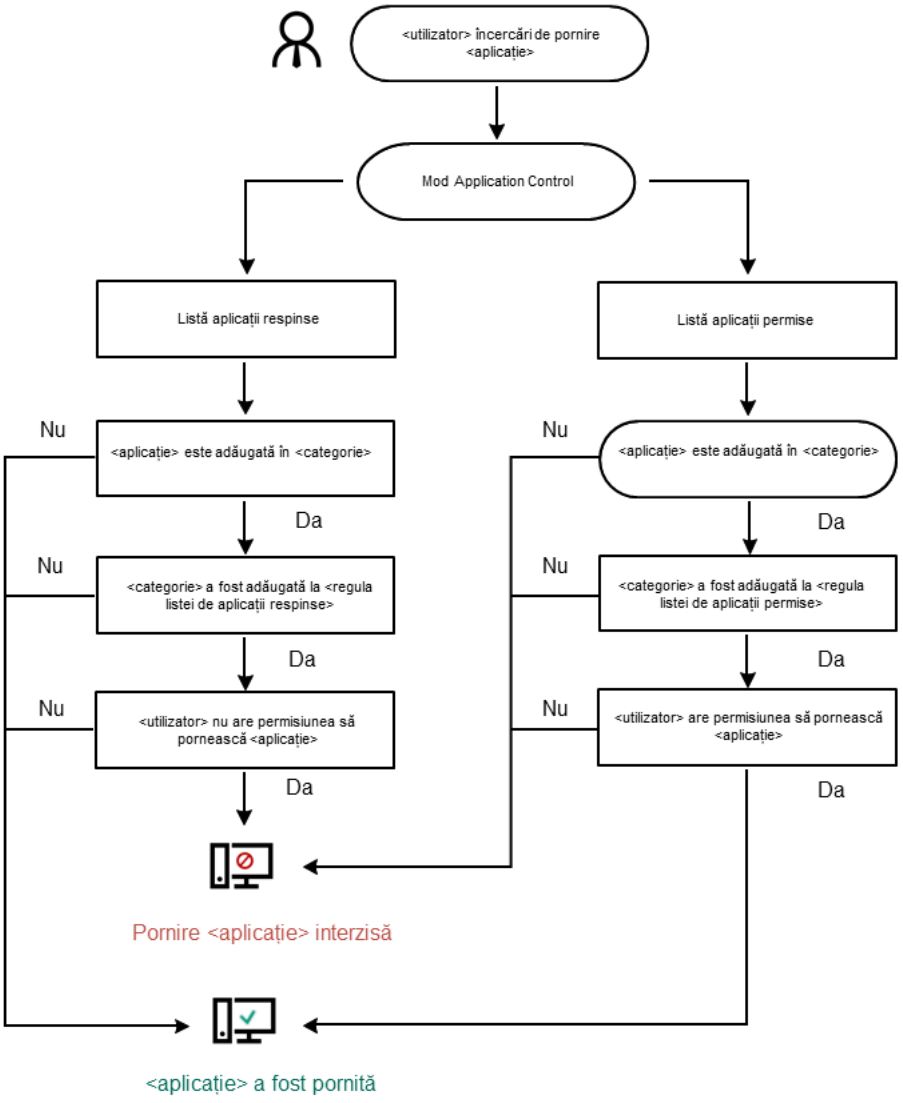
  Regulile Application Control create în Consola de administrare Kaspersky Security Center se bazează pe categorii tale particularizate de aplicații și nu pe condițiile de includere și de excludere, ca în cazul interfeței locale Kaspersky Endpoint Security.

- Primirea informațiilor despre aplicațiile instalate pe computerele din rețeaua LAN corporativă.

De aceea se recomandă utilizarea Kaspersky Security Center pentru a configura funcționarea componentei Application Control.

Algoritmul de funcționare al componentei Application Control

Kaspersky Endpoint Security folosește un algoritm pentru a lua o decizie cu privire la pornirea unei aplicații (consultați figura de mai jos).



Algoritmul de funcționare al componentei Application Control

Limitări în funcționalitatea componentei Application Control

Funcționalitatea componentei Application Control este limitată în următoarele cazuri:

- Atunci când se face upgrade versiunii aplicației, importul setărilor componentei Application Control nu este acceptat.
- Dacă nu există o conexiune cu serverele KSN, Kaspersky Endpoint Security primește informații despre reputația aplicațiilor și a modulelor lor de la bazele de date locale.

  Lista aplicațiilor pe care Kaspersky Endpoint Security le desemnează ca aparținând categoriei KL **Alt software\Aplicații, considerate de încredere în funcție de reputația din KSN** poate diferi în funcție de faptul dacă este disponibilă sau nu o conexiune la serverele KSN.

- În baza de date Kaspersky Security Center pot fi stocate informații despre 150.000 de fișiere procesate. După atingerea acestui număr de înregistrări, nu vor mai fi procesate fișiere noi. Pentru a relua operațiunile de inventariere, trebuie să ștergi fișierele inventariate anterior în baza de date Kaspersky Security Center de pe computerul pe care este instalată aplicația Kaspersky Endpoint Security.
- Componenta nu controlează pornirea scripturilor, cu excepția cazurilor în care scriptul este trimis către interpretor prin linia de comandă.

  Dacă pornirea unui interpretor este permisă de regulile Application Control, componenta nu va bloca un script pornit de la acest interpretor.

  Dacă cel puțin unul dintre scripturile specificate în linia de comandă a interpretorului este blocat să pornească de către regulile Application Control, componenta blochează toate scripturile specificate în linia de comandă a interpretorului.

- Componenta nu controlează pornirea scripturi de la interpretoare neacceptate de către Kaspersky Endpoint Security.

  Kaspersky Endpoint Security acceptă următoarele interpretoare:

  - Java
  - PowerShell

  Sunt acceptate următoarele tipuri de interpretoare:

  - %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

Primirea de informații despre aplicațiile instalate pe computerele utilizatorilor

Pentru a crea reguli Application Control optime, se recomandă mai întâi să analizezi aplicațiile folosite pe computerele din rețeaua LAN a companiei. Pentru aceasta poți obține următoarele informații:

- Vânzători, versiuni și localizări ale aplicațiilor folosite în rețeaua LAN a companiei.
- Frecvența actualizărilor aplicației.
- Politicile de utilizare a aplicației adoptate în companie (acestea pot fi politici de securitate sau politici administrative).
- Locația de stocare pentru pachetele de distribuție a aplicației.

Vizualizarea informațiilor despre aplicație

Informațiile despre aplicațiile instalate sunt furnizate de către Kaspersky Security Center Network Agent. Informațiile despre aplicațiile instalate sunt disponibile în consola Kaspersky Security Center din directorul **Applications registry**. Agentul de rețea actualizează informațiile la fiecare sincronizare cu Kaspersky Security Center. Pentru detalii suplimentare despre instalarea Agentului de rețea, vezi secțiunea de Ajutor pentru Kaspersky Security Center.

Pentru a deschide fereastra cu proprietățile aplicației în directorul Applications registry:

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele Consolă de administrare, selectează **Advanced** → **Application management** → **Applications registry**.
3. Selectați o aplicație.
4. În meniul contextual al aplicației, selectați **Properties**.

Vizualizarea informațiilor despre fișierele executabile

Poți reduce încărcarea bazei de date atunci când interogați informații despre fișierele executabile. Pentru a realiza acest lucru, recomandăm rularea sarcinii *Inventar* pe mai multe computere de referință care au instalat setul tău standard de produse software.

Poți obține o listă de fișiere executabile folosind sarcina *Inventar* din cadrul Kaspersky Endpoint Security. Poți vizualiza lista fișierelor executabile din consola Kaspersky Security Center în directorul **Executable files**.

Înainte de a rula sarcina *Inventar*, asigură-te că baza de date îndeplinește recomandările Kaspersky Security Center. Pentru detalii despre limitările bazei de date, vezi secțiunea de Ajutor pentru Kaspersky Security Center.

Cum se execută activitatea Inventar în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **New task**.

   Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Selectarea tipului activității

Selectați **Kaspersky Endpoint Security for Windows (14.1)** → **Inventar**.

Pasul 2. Domeniu inventar

Creează o listă de foldere în care vrei ca Kaspersky Endpoint Security să caute fișiere executabile. Configurează setările de inventar (vezi tabelul de mai jos).

Pasul 3. Selectarea dispozitivelor cărora le va fi atribuită activitatea

Selectați computerele pe care se va efectua activitatea. Sunt disponibile următoarele opțiuni:

- Atribuirea activității unui grup de administrare. În acest caz, activitatea este atribuită computerelor incluse într-un grup de administrare creat anterior.
- Selectare computere detectate în rețea de Serverul de administrare: *dispozitive neatribuite*. Dispozitivele specifice pot include dispozitive din grupuri de administrare, precum și dispozitive neatribuite.
- Specificarea manuală a adreselor computerelor sau importarea adreselor dintr-o listă. Poți specifica nume NetBIOS, adrese IP și subrețele IP ale dispozitivelor cărora dorești să le atribui activitatea.

Pasul 4. Selectarea contului pentru executarea activității

Selectați un cont pentru a executa activitatea *Inventar*. În mod implicit, Kaspersky Endpoint Security începe activitatea cu drepturile unui cont de utilizator local. Dacă domeniul de inventar include unități de rețea sau alte obiecte cu acces restricționat, selectează un cont de utilizator cu drepturile de acces suficiente.

Pasul 5. Configurarea unei planificări de pornire a activității

Configurează planificarea activității, de exemplu, manual.

Pasul 6. Definirea numelui activității

Introdu un nume pentru activitate, de exemplu, *Inventar de referință*.

Pasul 7. Finalizarea creării activității

Ieșiți din Expert. Dacă este necesar, bifați caseta de selectare **Run the task after the wizard finishes**. Puteți monitoriza progresul activității în proprietățile activității. Ca urmare, se efectuează o căutare a fișierelor executabile pe computerele utilizatorilor în conformitate cu programul configurat.

Cum se execută o activitate Inventar în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **Add**.

   Expertul de activitate pornește.

3. Configurați setările pentru activitate:

   a. În lista verticală **Application**, selectează **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. În lista verticală **Task type**, selectează **Inventory**.

   c. În câmpul **Task name**, introdu o descriere succintă, de exemplu *Inventar de referință*.

   d. În blocul **Devices to which the task will be assigned**, selectați domeniul activității.

4. Selectați dispozitive în funcție de opțiunea selectată pentru domeniul activității. Mergeți la pasul următor.

5. Selectează un cont pentru a executa activitatea. În mod implicit, Kaspersky Endpoint Security începe activitatea cu drepturile unui cont de utilizator local.

6. Ieșiți din Expert.

   Se va afișa o activitate nouă în lista de activități.

7. Pentru a configura sarcina, accesează proprietățile sarcinii (vezi tabelul de mai jos).

8. Bifați caseta de selectare de lângă activitate.

9. Fă clic pe **Start**.

   Poți monitoriza starea activității și numărul de dispozitive pe care activitatea a fost finalizată cu succes sau finalizată cu o eroare. Ca rezultat, fișierele executabile vor fi căutate pe computerele utilizatorului în conformitate cu programul specificat.

Setări de inventar

Parametru	Descriere
Inventory scopes	Lista obiectelor care vor forma sfera inventarului.
DLL modules inventory	Kaspersky Endpoint Security caută module DLL în domeniul inventarului și trimite informații către Kaspersky Security Center. Activarea inventarului modulelor DLL crește semnificativ timpul necesar pentru finalizarea sarcinii de inventar și dimensiunea bazei de date.
Script files inventory	Kaspersky Endpoint Security caută scripturi în domeniul inventarului și trimite informațiile către Kaspersky Security Center. Activarea inventarului fișierelor de script crește semnificativ timpul necesar pentru a finaliza sarcina de inventar și dimensiunea bazei de date.
Run only when the computer is idle	Amânarea începerii activității atunci când resursele computerului sunt ocupate. Kaspersky Endpoint Security pornește activitatea de scanare dacă computerul este blocat sau dacă economizorul de ecran este pornit. Dacă ați întrerupt executarea activității, de exemplu prin deblocarea computerului, Kaspersky Endpoint Security execută automat activitatea, continuând din punctul în care a fost întreruptă. Această opțiune de planificare vă permite să conservați resursele computerului atunci când acesta este utilizat.
Scan only new and modified files	Scanează numai fișierele noi și acele fișiere care au fost modificate de la ultima dată când au fost scanate. Acest lucru reduce durata unei scanări. Acest mod se aplică atât fișierelor simple, cât și celor compuse.
Skip file that is scanned for longer than (sec) N sec	Limitarea timpului de executare a activității. După scurgerea duratei specificate, Kaspersky Endpoint Security oprește activitatea. Activitatea nu este marcată ca finalizată. Data viitoare când Kaspersky Endpoint Security execută activitatea, aceasta va fi executată de la început și conform planificării.
Scan archives	Scanarea arhivelor ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE și a altor arhive. Aplicația scanează arhivele nu doar după extensie, dar și după format. La verificarea arhivelor, aplicația efectuează o dezarhivare recursivă. Acest lucru permite detectarea amenințărilor din arhivele cu mai multe niveluri (o arhivă într-o arhivă).

Parametru	Descriere
Scan distribution packages	Scanarea pachetelor de distribuție ale aplicațiilor terțe.
Do not unpack large compound files	Dacă această casetă de selectare este bifată, aplicația nu scanează fișierele compuse a căror dimensiune depășește valoarea specificată. În cazul în care această casetă de selectare este nebifată, aplicația scanează fișierele compuse indiferent de dimensiuni. Aplicația scanează fișierele mari extrase din arhive, indiferent dacă această casetă de selectare este bifată sau nu.

Pentru a deschide fereastra cu proprietăți pentru un fișier executabil în directorul Executable files:

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele Consolă de administrare, selectează **Advanced → Application management → Executable files**.
3. Selectați un fișier executabil.
4. În meniul contextual al fișierului executabil, selectați **Properties**.

Pentru a vizualiza informații generale despre aplicație și despre fișierele sale executabile, precum și despre lista de computere pe care este instalată o aplicație, deschide fereastra de proprietăți pentru o aplicație selectată în directorul **Applications registry** sau în directorul **Executable files**.

Actualizarea informațiilor despre aplicațiile și fișierele executabile instalate

Începând cu Kaspersky Endpoint Security 12.3 for Windows, este optimizată funcționarea componentei Application Control cu baza de date a fișierelor executabile. Kaspersky Endpoint Security 12.3 for Windows actualizează automat baza de date după ce fișierul este șters de pe computer. Acest lucru permite păstrarea bazei de date actualizată și economisirea resurselor Kaspersky Security Center.

Pentru a menține actualizată baza de date cu aplicațiile instalate, trimiterea informațiilor despre aplicații către Serverul de administrare trebuie să fie activată (este activată implicit).

Cum se activează trimiterea informațiilor despre aplicație în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Setări generale → Rapoarte și Spații de stocare**.
4. În blocul **Transfer de date pe serverul de administrare**, fă clic pe butonul **Setări**.
5. Bifați caseta de selectare **Aplicații pornite**.
6. Salvați-vă modificările.

Cum se activează trimiterea informațiilor despre aplicație în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management → Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **General Settings** → **KSC Integration**.

5. În blocul **Data transfer to Administration Server**, fă clic pe butonul **Advanced settings**.

6. În fereastra care se deschide, bifați caseta de selectare **About started applications**.

7. Salvați-vă modificările.

Cum se activează modul Aplicații blocate

Modul *Aplicații blocate* este modul în care Application Control permite utilizatorilor să pornească toate aplicațiile, cu excepția aplicațiilor care sunt interzise în regulile Application Control. Adică, dacă nu există nicio regulă de refuzare, Application Control permite pornirea aplicației. Acest mod al componentei Application Control este activat în mod implicit.

Înainte de a activa modul *Aplicații blocate*, îți recomandăm să testezi regulile Application Control. În acest scop, poți activa modul de testare.

Cum se selectează modul Aplicații blocate în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.

2. În arborele consolei, selectați **Policies**.

3. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

4. În fereastra politicii, selectați **Security Controls** → **Application Control**.

5. Bifați caseta de selectare **Application Control**.

6. În blocul **Setări Application Control**, utilizează lista verticală **Mod control** pentru a selecta **Listă respinse**.

7. În lista verticală **Acțiune**, selectează acțiunea pentru Application Control:

   - **Testează regulile**. Application Control nu blochează aplicațiile a căror executare este împiedicată de reguli, ci generează evenimente despre executarea aplicațiilor care altfel ar fi blocate.

   - **Aplica reguli**. Application Control blochează aplicațiile blocate și generează evenimente corespunzătoare.

8. Selectează starea regulilor Application Control:

   - **Pornit**. Această stare înseamnă că regula este utilizată atunci când se execută componenta Application Control.

   - **Oprit**. Această stare înseamnă că regula este ignorată atunci când se execută componenta Application Control.

   - **Test**. Această stare înseamnă că Kaspersky Endpoint Security permite întotdeauna pornirea aplicațiilor cărora li se aplică regulile, dar înregistrează în raport informații despre pornirea aplicațiilor respective.

Dacă este necesar, adaugă noi reguli Application Control.

9. Configurează setările avansate pentru Application Control:

   - **Monitorizați încărcarea modulelor DLL (crește semnificativ sarcina asupra sistemului)**. Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security controlează încărcarea modulelor DLL atunci când utilizatorii încearcă să pornească aplicații. Informațiile despre modulul DLL și aplicația care a încărcat acest modul DLL sunt înregistrate în raport.

     Atunci când activați controlul asupra încărcării modulelor și driverelor DLL, asigurați-vă că în setările componentei Application Control este activată una dintre următoarele reguli: regula implicită **Imagine de aur** sau o altă regulă care conține categoria KL „**Imagine de aur\Certificate de încredere**" și care se asigură că modulele și driverele DLL de încredere sunt încărcate înainte de pornirea Kaspersky Endpoint Security. Activarea controlului încărcării modulelor și driverelor DLL când regula **Imagine de aur** este dezactivată poate duce la instabilitatea sistemului de operare.

     Kaspersky Endpoint Security monitorizează numai modulele și driverele DLL care au fost încărcate după bifarea casetei de selectare. După bifarea casetei de selectare, este recomandat să reporniți computerul pentru a vă asigura că aplicația monitorizează toate modulele și driverele DLL, inclusiv cele încărcate înainte de pornirea Kaspersky Endpoint Security.

   - **Utilizează o verificare strictă a semnăturii digitale**. Poți selecta un certificat drept condiție de declanșare pentru o regulă Application Control. Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security aplică reguli aplicațiilor semnate cu certificate numai din depozitul de certificate de sistem de încredere. Aplicațiile semnate cu un astfel de certificat sunt, de asemenea, considerate de încredere de către componentele de protecție, de exemplu, activitatea *Scanare malware*. Cu toate acestea, dacă specifici un certificat dintr-un alt depozit într-o regulă Application Control, Kaspersky Endpoint Security nu aplică o astfel de regulă.

     Dacă această casetă de selectare este debifată, Kaspersky Endpoint Security aplică reguli aplicațiilor semnate printr-un certificat din Trusted Root Certificate Store. Astfel de aplicații nu fac parte din zona de încredere. Componentele de protecție monitorizează activitatea unor astfel de aplicații.

   - **Mesaj despre blocare**. Șablonul mesajului care se afișează atunci când este declanșată o regulă Application Control care blochează pornirea unei aplicații.

   - **Mesaj către administrator**. Șablon al mesajului pe care un utilizator îl poate trimite administratorului rețelei LAN corporative dacă utilizatorul consideră că o aplicație a fost blocată din greșeală.

10. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se activează modul Aplicații blocate în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați fila **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Security Controls** → **App Control**.
5. Duceți comutatorul **Application Control ENABLED** la poziția activat.

6. În secțiunea **Operating mode**, selectați **Block all except the rules list**.

7. În blocul **Action**, selectează acțiunea pentru Application Control:

   - **Inform**. Application Control nu blochează aplicațiile a căror executare este împiedicată de reguli, ci generează evenimente despre executarea aplicațiilor care altfel ar fi blocate.
   - **Apply rules**. Application Control blochează aplicațiile blocate și generează evenimente corespunzătoare.

8. Selectează starea regulilor Application Control:

   - **Enabled**. Această stare înseamnă că regula este utilizată atunci când se execută componenta Application Control.
   - **Disabled**. Această stare înseamnă că regula este ignorată atunci când se execută componenta Application Control.
   - **Test mode**. Această stare înseamnă că Kaspersky Endpoint Security permite întotdeauna pornirea aplicațiilor cărora li se aplică regulile, dar înregistrează în raport informații despre pornirea aplicațiilor respective.

   Dacă este necesar, adaugă noi reguli Application Control.

9. Configurează setările avansate pentru Application Control:

   - **Monitor loading of DLL modules**. Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security controlează încărcarea modulelor DLL atunci când utilizatorii încearcă să pornească aplicații. Informațiile despre modulul DLL și aplicația care a încărcat acest modul DLL sunt înregistrate în raport.

     Atunci când activați controlul asupra încărcării modulelor și driverelor DLL, asigurați-vă că în setările componentei Application Control este activată una dintre următoarele reguli: regula implicită **Imagine de aur** sau o altă regulă care conține categoria KL „**Imagine de aur\Certificate de încredere**" și care se asigură că modulele și driverele DLL de încredere sunt încărcate înainte de pornirea Kaspersky Endpoint Security. Activarea controlului încărcării modulelor și driverelor DLL când regula **Imagine de aur** este dezactivată poate duce la instabilitatea sistemului de operare.

     Kaspersky Endpoint Security monitorizează numai modulele și driverele DLL care au fost încărcate după bifarea casetei de selectare. După bifarea casetei de selectare, este recomandat să reporniți computerul pentru a vă asigura că aplicația monitorizează toate modulele și driverele DLL, inclusiv cele încărcate înainte de pornirea Kaspersky Endpoint Security.

   - **Use strict digital signature verification**. Poți selecta un certificat drept condiție de declanșare pentru o regulă Application Control. Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security aplică reguli aplicațiilor semnate cu certificate numai din depozitul de certificate de sistem de încredere. Aplicațiile semnate cu un astfel de certificat sunt, de asemenea, considerate de încredere de către componentele de protecție, de exemplu, activitatea *Scanare malware*. Cu toate acestea, dacă specifici un certificat dintr-un alt depozit într-o regulă Application Control, Kaspersky Endpoint Security nu aplică o astfel de regulă.

     Dacă această casetă de selectare este debifată, Kaspersky Endpoint Security aplică reguli aplicațiilor semnate printr-un certificat din Trusted Root Certificate Store. Astfel de aplicații nu fac parte din zona de încredere. Componentele de protecție monitorizează activitatea unor astfel de aplicații.

- **Message to user**. Șablonul mesajului care se afișează atunci când este declanșată o regulă Application Control care blochează pornirea unei aplicații.

- **Message to administrator**. Șablon al mesajului pe care un utilizator îl poate trimite administratorului rețelei LAN corporative dacă utilizatorul consideră că o aplicație a fost blocată din greșeală.

10. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se activează modul Aplicații blocate în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Security Controls** → **Application Control**.

3. Duceți comutatorul **Application Control** la poziția activat.

4. În secțiunea **Modul Control la pornirea aplicației**, selectați **Lista de respinse. Sunt permise toate aplicațiile, cu excepția celor din lista de reguli**.

5. În blocul **Acțiune la pornirea aplicațiilor blocate de reguli**, selectează acțiunea pentru Application Control:

   - **Informează (Modul Testare) și înregistrează evenimentele în raport**. Application Control nu blochează aplicațiile a căror funcționare este împiedicată de reguli, dar generează evenimente privind executarea aplicațiilor care altfel ar fi blocate.

   - **Blochează**. Application Control blochează aplicațiile blocate și generează evenimente corespunzătoare.

6. Selectează starea regulilor Application Control:

   - **Activată**. Această stare înseamnă că regula este utilizată atunci când se execută componenta Application Control.

   - **Dezactivată**. Această stare înseamnă că regula este ignorată atunci când se execută componenta Application Control.

   - **Modul Testare**. Această stare înseamnă că Kaspersky Endpoint Security permite întotdeauna pornirea aplicațiilor cărora li se aplică regulile, dar înregistrează în raport informații despre pornirea aplicațiilor respective.

   Dacă este necesar, adaugă noi reguli Application Control.

7. Configurează setările avansate pentru Application Control:

   - **Monitorizează încărcarea modulelor DLL**. Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security controlează încărcarea modulelor DLL atunci când utilizatorii încearcă să pornească aplicații. Informațiile despre modulul DLL și aplicația care a încărcat acest modul DLL sunt înregistrate în raport.

     Atunci când activați controlul asupra încărcării modulelor și driverelor DLL, asigurați-vă că în setările componentei Application Control este activată una dintre următoarele reguli: regula implicită **Imagine de aur** sau o altă regulă care conține categoria KL „**Imagine de aur\Certificate de încredere**” și care se asigură că modulele și driverele DLL de încredere sunt încărcate înainte de pornirea Kaspersky Endpoint Security. Activarea controlului încărcării modulelor și driverelor DLL când regula **Imagine de aur** este dezactivată poate duce la instabilitatea sistemului de operare.

Kaspersky Endpoint Security monitorizează numai modulele și driverele DLL care au fost încărcate după bifarea casetei de selectare. După bifarea casetei de selectare, este recomandat să reporniți computerul pentru a vă asigura că aplicația monitorizează toate modulele și driverele DLL, inclusiv cele încărcate înainte de pornirea Kaspersky Endpoint Security.

- **Utilizează o verificare strictă a semnăturii digitale**. Poți selecta un certificat drept condiție de declanșare pentru o regulă Application Control. Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security aplică reguli aplicațiilor semnate cu certificate numai din depozitul de certificate de sistem de încredere. Aplicațiile semnate cu un astfel de certificat sunt, de asemenea, considerate de încredere de către componentele de protecție, de exemplu, activitatea *Scanare malware*. Cu toate acestea, dacă specifici un certificat dintr-un alt depozit într-o regulă Application Control, Kaspersky Endpoint Security nu aplică o astfel de regulă.

  Dacă această casetă de selectare este debifată, Kaspersky Endpoint Security aplică reguli aplicațiilor semnate printr-un certificat din Trusted Root Certificate Store. Astfel de aplicații nu fac parte din zona de încredere. Componentele de protecție monitorizează activitatea unor astfel de aplicații.

- **Șabloanele mesajelor despre blocarea aplicației**. Șablonul mesajului care se afișează atunci când este declanșată o regulă Application Control care blochează pornirea unei aplicații.

- **Textul mesajului șablonului afișat la blocarea pornirii unei aplicații**. Șablon al mesajului pe care un utilizator îl poate trimite administratorului rețelei LAN corporative dacă utilizatorul consideră că o aplicație a fost blocată din greșeală.

8. Salvați-vă modificările.

Prin urmare, Application Control blochează aplicațiile blocate. Kaspersky Endpoint Security generează, de asemenea, evenimente *Pornire aplicație interzisă*. Poți folosi aceste evenimente pentru a genera raportul *Report on prohibited applications* în consola Kaspersky Security Center. În rezumatul raportului, poți vizualiza lista de aplicații și computere pe care s-a declanșat regula Application Control.

Application Control bazat pe un sistem de referință

Poți utiliza un sistem de referință pentru a crea o imagine cu un set de aplicații de care ai nevoie. Apoi, poți utiliza această imagine pentru a implementa sistemul de operare și aplicațiile pe alte computere. Nu este întotdeauna posibil să menținem imaginea actualizată. Application Control îți permite să menții o listă de aplicații permise pe baza unui sistem de referință. Application Control stabilește automat ce aplicații sunt instalate pe sistemul de referință și actualizează categoria. În acest fel, computerele primesc o listă actualizată cu aplicațiile permise.

Configurarea componentei Application Control pe baza unui sistem de referință implică următorii pași:

1. Crearea unei categorii cu actualizare automată. Când creezi noua categorie, selectează categoria **Category that includes executable files from a specific folder** și selectează sistemul de referință.

   Cum se creează o categorie cu actualizare automată în Consola de administrare (MMC)

   1. Deschide Consolă de administrare a Kaspersky Security Center.

   2. În arborele Consolă de administrare, selectează **Advanced** → **Application management** → **Application categories**.

3. Faceți clic pe butonul **New category** în spațiul de lucru.

   Această acțiune pornește expertul de creare a categoriei de aplicații.

4. Urmează instrucțiunile din Expertul pentru crearea categoriei de aplicații.

Pasul 1. Selectarea tipului de categorie

Selectează **Category that includes executable files from selected devices** ca tipul categoriei.

Pasul 2. Introducerea numelui unei categorii a utilizatorului

La acest pas, specifică numele categoriei de aplicații.

Pasul 3. Setări

> Acest pas este disponibil dacă ai selectat tipul de categorie **Category that includes executable files from selected devices**.

La acest pas, faceți clic pe butonul **Add** și specifică computerele ale căror fișiere executabile Kaspersky Security Center le va adăuga la categoria de aplicații. Toate fișierele executabile de pe computerele specificate, existente în directorul **Executable files**, vor fi adăugate la categoria de aplicații de către Kaspersky Security Center.

La acest pas, mai poți configura setările următoare:

- Algorithm for hash function calculation. Pentru a selecta un algoritm, trebuie să bifezi cel puțin una dintre casetele de selectare următoare:
  - **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)**.
- Caseta de selectare **Synchronize data with Administration Server repository**. Bifați această casetă dacă vrei ca Kaspersky Security Center să golească periodic categoria de aplicații și să adauge în aceasta toate fișierele executabile de pe computerele specificate, existente în directorul **Executable files**.

  În cazul în care caseta de selectare **Synchronize data with Administration Server repository** este debifată, Kaspersky Security Center nu va efectua nicio modificare pentru o categorie de aplicații după crearea sa.

Pasul 4. Filtru

În acest pas, configurează un filtru pentru fișiere.

Poți specifica tipul de fișier pe care dorești să îl utilizezi pentru a crea categoria de aplicații.

- **All files**. Categoria se va potrivi cu toate fișierele. Această opțiune este selectată în mod implicit.
- **Only files outside the application categories**. Categoria se va potrivi doar cu fișierele din afara categoriilor de aplicații.

Poți specifica directoarele computerelor selectate care conțin fișierele pe care dorești să le utilizezi pentru a crea categoria de aplicații.

- **All folders**. Categoria se va potrivi cu toate directoarele. Această opțiune este selectată în mod implicit.
- **Specified folder**. Categoria se va potrivi doar cu directorul specificat. Dacă selectezi această opțiune, trebuie să specifici o cale către director.

Pasul 5. Crearea unei categorii particularizate

Ieșiți din Expert.

Cum se creează o categorie cu conținut adăugat automat în Web Console și Cloud Console

1. În fereastra principală a componentei Web Console, selectați **Operations → Third-party applications → Application categories**.

   Această acțiune deschide lista categoriilor de aplicații.

2. Fă clic pe **Add**.

   Această acțiune pornește expertul de creare a categoriei de aplicații.

3. Configurează setările generale ale categoriei de aplicații:

   - Numele categoriei.
   - Metoda de creare a categoriei. Selectează **Category that includes executable files from selected devices** ca tipul categoriei.

   Mergeți la pasul următor.

4. Configurează setările avansate ale categoriei de aplicații:

   - Precizează computerele de pe care Kaspersky Security Center va adăuga fișiere executabile în categoria de aplicații. Toate fișierele executabile de pe computerele specificate, existente în directorul **Executable files**, vor fi adăugate la categoria de aplicații de către Kaspersky Security Center.
   - Selectează un algoritm pentru calculul funcției hash.

- Configurează un interval pentru sincronizarea datelor cu spațiul de stocare al Serverului de administrare.
- Configurează un filtru pentru fișiere.

5. Ieșiți din Expert.

Când creezi o categorie cu actualizare automată, poate fi util să împarți fișierele în mai multe categorii. De exemplu, fișierele sistemului de operare și fișierele din directorul Program Files. Pentru a face acest lucru, poți utiliza un filtru în setările categoriei și poți selecta directoare individuale.

2. Selectarea modului Application Control. Trebuie să împiedici executarea tuturor aplicațiilor care nu sunt permise în mod explicit. Pentru aceasta, selectează modul *Aplicații blocate*.

3. Crearea unei reguli Application Control. În setările regulii, selectează categoria căreia îi aparțin fișierele executabile de pe sistemul de referință.

Cum se configurează componenta Application Control bazată pe un sistem de referință în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați **Policies**.
3. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
4. În fereastra politicii, selectați **Security Controls** → **Application Control**.
5. Bifați caseta de selectare **Application Control**.
6. În blocul **Setări Application Control**, utilizează lista verticală **Mod control** pentru a selecta **Listă respinse**.
7. În lista verticală **Acțiune**, selectează acțiunea pentru Application Control:
   - **Testează regulile**. Application Control nu blochează aplicațiile a căror executare este împiedicată de reguli, ci generează evenimente despre executarea aplicațiilor care altfel ar fi blocate.
   - **Aplica reguli**. Application Control blochează aplicațiile blocate și generează evenimente corespunzătoare.
8. În lista de reguli Application Control, fă clic pe butonul **Adaugă**.

   Această acțiune pornește expertul pentru adăugarea unei reguli Application Control.
9. În lista verticală **Categorie**, selectează o categorie cu actualizare automată pe baza sistemului de referință.
10. Selectați utilizatorii sau grupurile de utilizatori cărora doriți să le aplicați regula Application Controlregula.
11. Configurează setările avansate ale regulii Application Control:
    - **Refuză pentru alți utilizatori**. Aplicația împiedică lansarea aplicațiilor care aparțin categoriei selectate pentru toți utilizatorii care nu se află pe listă.
    - **Programe de actualizare de încredere**. Kaspersky Endpoint Security consideră aplicațiile incluse în categoria selectată ca fiind programe de actualizare de încredere care au permisiunea să creeze alte fișiere executabile care, la rândul lor, vor avea permisiunea să se execute ulterior.
12. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se configurează Application Control bazat pe un sistem de referință în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați fila **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Security Controls** → **App Control**.
5. Duceți comutatorul **Application Control ENABLED** la poziția activat.
6. În secțiunea **Operating mode**, selectați **Block all except the rules list**.
7. În blocul **Action**, selectează acțiunea pentru Application Control:

   - **Inform**. Application Control nu blochează aplicațiile a căror executare este împiedicată de reguli, ci generează evenimente despre executarea aplicațiilor care altfel ar fi blocate.
   - **Apply rules**. Application Control blochează aplicațiile blocate și generează evenimente corespunzătoare.
8. În lista de reguli Application Control, fă clic pe butonul **Add**.

   Această acțiune pornește expertul pentru adăugarea unei reguli Application Control.
9. În **Categories/Applications**, selectează o categorie cu actualizare automată bazată pe sistemul de referință.
10. Selectați utilizatorii sau grupurile de utilizatori cărora doriți să le aplicați regula Application Controlregula.
11. Configurează setările avansate ale regulii Application Control:

    - **Users**. Aplicația împiedică lansarea aplicațiilor care aparțin categoriei selectate pentru toți utilizatorii care nu se află pe listă.
    - **Trusted Updaters**. Kaspersky Endpoint Security consideră aplicațiile incluse în categoria selectată ca fiind programe de actualizare de încredere care au permisiunea să creeze alte fișiere executabile care, la rândul lor, vor avea permisiunea să se execute ulterior.
12. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se configurează Application Control bazat pe un sistem de referință în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Security Controls** → **Application Control**.
3. Duceți comutatorul **Application Control** la poziția activat.
4. În secțiunea **Modul Control la pornirea aplicației**, selectați **Lista de respinse. Sunt permise toate aplicațiile, cu excepția celor din lista de reguli**.

5. În blocul **Acțiune la pornirea aplicațiilor blocate de reguli**, selectează acțiunea pentru Application Control:

   - **Informează (Modul Testare) și înregistrează evenimentele în raport**. Application Control nu blochează aplicațiile a căror funcționare este împiedicată de reguli, dar generează evenimente privind executarea aplicațiilor care altfel ar fi blocate.

   - **Blochează**. Application Control blochează aplicațiile blocate și generează evenimente corespunzătoare.

6. În lista de reguli Application Control, fă clic pe butonul **Adaugă**.

   Această acțiune pornește expertul pentru adăugarea unei reguli Application Control.

7. În **Categorie**, selectează o categorie cu actualizare automată bazată pe sistemul de referință.

8. Selectați utilizatorii sau grupurile de utilizatori cărora doriți să le aplicați regula Application Controlregula.

9. Configurează setările avansate ale regulii Application Control:

   - **Refuză pentru alți utilizatori**. Aplicația împiedică lansarea aplicațiilor care aparțin categoriei selectate pentru toți utilizatorii care nu se află pe listă.

   - **Programe de actualizare de încredere**. Kaspersky Endpoint Security consideră aplicațiile incluse în categoria selectată ca fiind programe de actualizare de încredere care au permisiunea să creeze alte fișiere executabile care, la rândul lor, vor avea permisiunea să se execute ulterior.

10. Salvați-vă modificările.

Administrarea regulilor Application Control

Kaspersky Endpoint Security controlează pornirea aplicațiilor de către utilizatori utilizând regulile. O regulă Application Control specifică condițiile de declanșare și acțiunile efectuată de Application Control atunci când regula este declanșată (permițând sau blocând pornirea aplicației de către utilizatori).

Condiții de declanșare a regulii

O condiție de declanșare a regulilor are următoarea corelație: „tipul condiției – criteriul condiției – valoarea condiției”. Pe baza condițiilor de declanșare a regulii, Kaspersky Endpoint Security aplică (sau nu aplică) o regulă unei aplicații.

Următoarele tipuri de condiții sunt utilizate în reguli:

- *Condiții de includere*. Kaspersky Endpoint Security aplică regula aplicației dacă aplicația corespunde cel puțin uneia dintre condițiile de includere.

- *Condiții excludere*. Kaspersky Endpoint Security nu aplică regula aplicației dacă aplicația corespunde cel puțin uneia dintre condițiile de excludere și nu corespunde niciuneia dintre condițiile de includere.

Condițiile de declanșare a regulii sunt create folosind criterii. Următoarele criterii sunt folosite pentru a crea reguli în Kaspersky Endpoint Security:

- Calea către directorul care conține fișierul executabil al aplicației sau calea către fișierul executabil al aplicației.
- Metadate: nume fișier executabil al aplicației, versiune fișier executabil al aplicației, nume aplicație, versiune aplicație, vânzător aplicație.
- Codul hash al fișierului executabil al aplicației.
- Certificat: emitent, subiect, amprentă.
- Includerea aplicației într-o categorie KL.
- Locația fișierului executabil al aplicației pe o unitate amovibilă.

Valoarea criteriului trebuie specificată pentru fiecare criteriu folosit în condiție. Dacă parametrii aplicației pornite corespund valorilor criteriilor specificate în condiția de includere, regula este declanșată. În acest caz, componenta Application Control efectuează acțiunea prescrisă de regulă. Dacă parametrii aplicației pornite corespund valorilor criteriilor specificate în condiția de excludere, componenta Application Control nu controlează pornirea aplicației.

Dacă ai selectat un certificat ca și condiție de declanșare a regulii, trebuie să te asiguri că acest certificat este adăugat la spațiul de stocare de încredere al sistemului de pe computer și să verifici setările de utilizare a spațiului de stocare de încredere al sistemului în aplicație.

Deciziile luate de componenta Application Control atunci când o regulă este declanșată

Atunci când o regulă este declanșată, componenta Application Control permite utilizatorilor sau grupurilor de utilizatori să pornească aplicații sau blochează pornirea conform regulii. Poți selecta utilizatori individuali sau grupuri de utilizatori cărora li se permite sau nu li se permite să pornească aplicații care declanșează o regulă.

Dacă o regulă nu specifică utilizatorii care au permisiunea să pornească aplicații care satisfac regula, atunci această regulă este denumită regulă de *blocare*.

Dacă o regulă care nu specifică niciun utilizator care nu are permisiunea de a porni aplicații care satisfac regula, atunci această regulă este denumită regulă de *permitere*.

Prioritatea pentru o regulă de blocare este mai mare decât prioritatea pentru o regulă de permitere. De exemplu, dacă o regulă de permitere pentru componenta Application Control a fost atribuită unui grup de utilizatori, iar o regulă de blocare pentru componenta Application Control a fost atribuită unui utilizator din acest grup de utilizatori, atunci pornirea aplicației de către respectivul utilizator va fi blocată.

Starea operațională a unei reguli

Regulile Application Control pot avea una dintre următoarele stări operaționale:

- **Activată**. Această stare înseamnă că regula este utilizată atunci când se execută componenta Application Control.
- **Dezactivată**. Această stare înseamnă că regula este ignorată atunci când se execută componenta Application Control.
- **Modul Testare**. Această stare înseamnă că Kaspersky Endpoint Security permite pornirea aplicațiilor cărora li se aplică regula, dar înregistrează în raport informații despre pornirea aplicațiilor respective.

Adăugarea unei condiții de declanșare pentru o regulă Application Control

Pentru simplificarea creării regulilor Application Control, poți crea categorii de aplicații.

Se recomandă crearea unei categorii „Aplicații pentru serviciu”, care acoperă setul standard de aplicații care sunt folosite în companie. Dacă diferite grupuri de utilizatori folosesc diferite seturi de aplicații la locul lor de muncă, se poate crea o categorie separată de aplicații pentru fiecare grup de utilizatori.

Pentru a crea o categorie de aplicații în Consola de administrare:

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele Consolă de administrare, selectează **Advanced → Application management → Application categories**.
3. Faceți clic pe butonul **New category** în spațiul de lucru.

   Pornește expertul de creare a categoriilor de utilizatori.
4. Urmează instrucțiunile din Expertul pentru crearea categoriilor de utilizatori.

Pasul 1. Selectarea tipului de categorie

La acest pas poți selecta una dintre următoarele categorii de aplicații:

- Category with content added manually. Data of executable files is manually added to the category Dacă ai selectat acest tip de categorie, în cadrul pasului *Configuring conditions for inclusion of applications in categories* și pasului *Configuring conditions for exclusion of applications from categories* vei putea defini criteriile prin care fișierele executabile vor fi incluse în categorie.

- Category that includes executable files from selected devices. These executable files are processed automatically and their metrics are added to the category Dacă ai selectat acest tip de categorie, la pasul *Settings* vei putea să specifici un computer ale cărui fișiere executabile vor fi incluse automat în 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 Dacă ai selectat acest tip de categorie, la pasul *Repository folder* vei putea să specifici un director din care fișierele executabile vor fi incluse automat în categorie.

La crearea unei categorii cu conținut adăugat automat, Kaspersky Security Center realizează inventarul fișierelor cu următoarele formate: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX și SCR.

Pasul 2. Introducerea numelui unei categorii a utilizatorului

La acest pas, specifică numele categoriei de aplicații.

Pasul 3. Configurarea condițiilor de includere a aplicațiilor într-o categorie

Atunci când se adaugă un număr mare de condiții la regulile Application Control (de exemplu, hash-uri de fișiere), consumul de resurse ale computerului crește. Când numărul total de condiții ajunge la 50.000, pot apărea probleme de performanță. Pentru a optimiza performanța, se recomandă revizuirea și reducerea numărului de condiții.

Acest pas este disponibil dacă ai selectat tipul de categorie **Category with content added manually**.

La acest pas, în lista verticală **Add**, selectați condițiile pentru includerea aplicațiilor în categorie:

- **From the list of executable files**. Adaugă în categoria particularizată aplicații din lista fișierelor executabile pe dispozitivul client.

- **From file properties**. Specifică datele detaliate ale fișierelor executabile drept condiție pentru adăugarea aplicațiilor în categoria particularizată.

- **Metadata from files in folder**. Selectați pe dispozitivul client un director care conține fișiere executabile. Kaspersky Security Center va indica metadatele acestor fișiere executabile drept condiție pentru adăugarea aplicațiilor în categoria particularizată.

- **Checksums of the files in the folder**. Selectați pe dispozitivul client un director care conține fișiere executabile. Kaspersky Security Center va indica codul hash al acestor fișiere executabile drept condiție pentru adăugarea aplicațiilor în categoria particularizată.

- **Certificates for the files from the folder**. Selectați pe dispozitivul client un director care conține fișiere executabile semnate cu certificate. Kaspersky Security Center va indica certificatele acestor fișiere executabile drept condiție pentru adăugarea aplicațiilor în categoria particularizată.

  Nu este recomandat să folosești condiții ale căror proprietăți nu au specificat parametrul **Certificate fingerprint**.

- **MSI installer files metadata**. Selectați pachetul MSI. Kaspersky Security Center va indica metadatele fișierelor executabile cuprinse în acest pachet MSI drept condiție pentru adăugarea aplicațiilor în categoria particularizată.

- **Checksums of the files from the MSI installer of the application**. Selectați pachetul MSI. Kaspersky Security Center va indica hash-urile fișierelor executabile cuprinse în acest pachet MSI drept condiție pentru adăugarea aplicațiilor în categoria particularizată.

- **From KL category**. Specifică o categorie KL drept condiție pentru adăugarea aplicațiilor în categoria particularizată. O *KL category* este o listă de aplicații care partajează atribute de temă. Lista este întreținută de experții Kaspersky. De exemplu, categoria KL cu numele „*Office Applications*" include toate aplicațiile din suita Microsoft Office, Adobe Acrobat și altele.

  Poți selecta toate categoriile KL ca să generezi o listă extinsă cu aplicații de încredere.

- **Specify path to application (masks supported)**. Selectați un director pe dispozitivul client. Kaspersky Security Center va adăuga fișierele executabile din acest director în categoria particularizată.

- **Select certificate from repository**. Selectați certificatele care au fost utilizate pentru a semna fișierele executabile drept condiție pentru adăugarea de aplicații la categoria particularizată.

  Nu este recomandat să folosești condiții ale căror proprietăți nu au specificat parametrul **Certificate fingerprint**.

  Poți alege depozitul de certificate. În mod implicit, componenta Application Control aplică reguli numai pentru aplicațiile semnate cu un certificat din depozitul de certificate de sistem de încredere. Acest lucru este activat prin caseta de selectare **Utilizează o verificare strictă a semnăturii digitale**.

- **Drive type**. Specifică tipul de dispozitiv de stocare (toate unitățile de hard disk și cele amovibile sau numai unitățile amovibile) drept condiție pentru adăugarea aplicațiilor în categoria particularizată.

Pasul 4. Configurarea condițiilor de excludere a aplicațiilor dintr-o categorie

Acest pas este disponibil dacă ai selectat tipul de categorie **Category with content added manually**.

Aplicațiile specificate la acest pas sunt excluse din categorie chiar dacă aceste aplicații au fost specificate la pasul „Configurarea condițiilor de includere a aplicațiilor într-o categorie".

La acest pas, în lista verticală **Add**, selectați condițiile pentru excluderea aplicațiilor din categorie:

- **From the list of executable files**. Adaugă în categoria particularizată aplicații din lista fișierelor executabile pe dispozitivul client.
- **From file properties**. Specifică datele detaliate ale fișierelor executabile drept condiție pentru adăugarea aplicațiilor în categoria particularizată.
- **Metadata from files in folder**. Selectați pe dispozitivul client un director care conține fișiere executabile. Kaspersky Security Center va indica metadatele acestor fișiere executabile drept condiție pentru adăugarea aplicațiilor în categoria particularizată.
- **Checksums of the files in the folder**. Selectați pe dispozitivul client un director care conține fișiere executabile. Kaspersky Security Center va indica codul hash al acestor fișiere executabile drept condiție pentru adăugarea aplicațiilor în categoria particularizată.
- **Certificates for the files from the folder**. Selectați pe dispozitivul client un director care conține fișiere executabile semnate cu certificate. Kaspersky Security Center va indica certificatele acestor fișiere executabile drept condiție pentru adăugarea aplicațiilor în categoria particularizată.
- **MSI installer files metadata**. Selectați pachetul MSI. Kaspersky Security Center va indica metadatele fișierelor executabile cuprinse în acest pachet MSI drept condiție pentru adăugarea aplicațiilor în categoria particularizată.
- **Checksums of the files from the MSI installer of the application**. Selectați pachetul MSI. Kaspersky Security Center va indica hash-urile fișierelor executabile cuprinse în acest pachet MSI drept condiție pentru adăugarea aplicațiilor în categoria particularizată.
- **From KL category**. Specifică o categorie KL drept condiție pentru adăugarea aplicațiilor în categoria particularizată. O *KL category* este o listă de aplicații care partajează atribute de temă. Lista este întreținută de experții Kaspersky. De exemplu, categoria KL cu numele „*Office Applications*" include toate aplicațiile din suita Microsoft Office, Adobe Acrobat și altele.

  Poți selecta toate categoriile KL ca să generezi o listă extinsă cu aplicații de încredere.
- **Specify path to application (masks supported)**. Selectați un director pe dispozitivul client. Kaspersky Security Center va adăuga fișierele executabile din acest director în categoria particularizată.
- **Select certificate from repository**. Selectați certificatele care au fost utilizate pentru a semna fișierele executabile drept condiție pentru adăugarea de aplicații la categoria particularizată.
- **Drive type**. Specifică tipul de dispozitiv de stocare (toate unitățile de hard disk și cele amovibile sau numai unitățile amovibile) drept condiție pentru adăugarea aplicațiilor în categoria particularizată.

Pasul 5. Setări

Acest pas este disponibil dacă ai selectat tipul de categorie **Category that includes executable files from selected devices**.

La acest pas, faceți clic pe butonul **Add** și specifică computerele ale căror fișiere executabile Kaspersky Security Center le va adăuga la categoria de aplicații. Toate fișierele executabile de pe computerele specificate, existente în directorul **Executable files**, vor fi adăugate la categoria de aplicații de către Kaspersky Security Center.

La acest pas, mai poți configura setările următoare:

- Algorithm for hash function calculation. Pentru a selecta un algoritm, trebuie să bifezi cel puțin una dintre casetele de selectare următoare:
  - **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)**.
- Caseta de selectare **Synchronize data with Administration Server repository**. Bifați această casetă dacă vrei ca Kaspersky Security Center să golească periodic categoria de aplicații și să adauge în aceasta toate fișierele executabile de pe computerele specificate, existente în directorul **Executable files**.

  În cazul în care caseta de selectare **Synchronize data with Administration Server repository** este debifată, Kaspersky Security Center nu va efectua nicio modificare pentru o categorie de aplicații după crearea sa.

Pasul 6. Directorul depozitului

Acest pas este disponibil dacă ai selectat tipul de categorie **Category that includes executable files from a specific folder**.

La acest pas, specificați directorul în care Kaspersky Security Center va căuta fișierele executabile pentru a adăuga automat aplicațiile în categoria de aplicații.

La acest pas, mai poți configura setările următoare:

- Caseta de selectare **Include dynamic-link libraries (DLL) in this category**. Bifați această casetă de selectare dacă doriți ca bibliotecile cu legare dinamică (fișiere DLL) să fie incluse în categoria aplicațiilor.

  Includerea fișierelor DLL în categoria de aplicații poate reduce performanța produsului Kaspersky Security Center.

- Caseta de selectare **Include script data in this category**. Bifați această casetă de selectare dacă doriți ca scripturile să fie incluse în categoria aplicațiilor.

  Includerea scripturilor în categoria aplicațiilor poate reduce performanța aplicației Kaspersky Security Center.

- Algorithm for hash function calculation. Pentru a selecta un algoritm, trebuie să bifezi cel puțin una dintre casetele de selectare următoare:

  - **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)**.

- Caseta de selectare **Force folder scan for changes**. Bifați această casetă de selectare dacă vrei ca Kaspersky Security Center să caute periodic fișiere executabile în directorul folosit pentru adăugarea automată în categoria de aplicații.

  Dacă este debifată caseta de selectare **Force folder scan for changes**, Kaspersky Security Center caută fișiere executabile în directorul folosit pentru adăugarea automată în categoria de aplicații numai dacă au avut loc modificări în director, dacă s-au adăugat fișiere în director sau dacă s-au șters fișiere din acesta.

- Câmpul **Scan interval (1–168 hours)**. În acest câmp, poți specifica intervalul de timp (în ore) după care Kaspersky Security Center caută fișierele executabile în directorul folosit pentru adăugarea automată a aplicațiilor în categoria de aplicații.

  Câmpul este disponibil dacă bifați caseta de selectare **Force folder scan for changes**.

Pasul 7. Crearea unei categorii particularizate

Ieșiți din Expert.

Pentru a adăuga o condiție nouă de declanșare pentru o regulă Application Control în interfața aplicației:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Security Controls → Application Control**.
3. Fă clic pe butonul **Aplicații blocate** sau **Aplicații permise**.

   Aceasta deschide lista regulilor Application Control.
4. Selectați regula pentru care doriți să configurați o condiție de declanșare.

   Se deschid proprietățile regulii Application Control.
5. Selectați fila **Condiții: N** sau fila **Excluderi: N** și faceți clic pe butonul **Adaugă**.

6. Selectați condițiile de declanșare pentru regula Application Control:

   - **Condiții din proprietățile aplicațiilor pornite**. În lista aplicațiilor care rulează, puteți selecta aplicațiile cărora li se va aplica regula Application Control. Kaspersky Endpoint Security listează, de asemenea, aplicațiile care rulau anterior pe computer. Trebuie să selectați criteriul pe care doriți să îl utilizați pentru a crea una sau mai multe condiții de declanșare a regulilor: **Hash fișier**, **Certificat**, **Categorie KL**, **Metadate** sau **Calea către fișier sau director**.

   - **Condiții „categoria KL”**. O *KL category* este o listă de aplicații care partajează atribute de temă. Lista este întreținută de experții Kaspersky. De exemplu, categoria KL cu numele „Aplicații Office” include toate aplicațiile din suita Microsoft Office, Adobe® Acrobat® și altele.

   - **Condiție personalizată**. Puteți selecta fișierul aplicației și puteți selecta una dintre condițiile de declanșare a regulii: **Hash fișier**, **Certificat**, **Metadate** sau **Calea către fișier sau director**.

   - **Condiție în funcție de unitatea fișierului (unitatea amovibilă)**. Regula Application Control se aplică numai fișierelor care sunt rulate pe o unitate amovibilă.

   - **Condiții din proprietățile fișierului în directorul specificat**. Regula Application Control se aplică numai fișierelor care se află în directorul specificat. De asemenea, puteți include sau exclude fișiere din subdirectoare. Trebuie să selectați criteriul pe care doriți să îl utilizați pentru a crea una sau mai multe condiții de declanșare a regulilor: **Hash fișier**, **Certificat**, **Categorie KL**, **Metadate** sau **Calea către fișier sau director**.

7. Salvați-vă modificările.

Când adăugați condiții, vă rugăm să țineți cont de următoarele considerații speciale pentru Application Control:

- Kaspersky Endpoint Security acceptă caracterele `*` și `?` pentru introducerea unei măști în metadate: **File name**, **Application name**, **Vendor**.

- Kaspersky Endpoint Security nu acceptă cod hash MD5 de fișiere și nu controlează pornirea aplicațiilor pe baza unui hash MD5. Drept condiție de declanșare a regulii este folosit un cod hash SHA256.

- Să recomandă folosirea doar a criteriilor **Emitent** și **Titular certificat** drept condiții de declanșare a regulii. Utilizarea acestor criterii nu este fiabilă.

- Dacă utilizezi un link simbolic în câmpul **Calea către fișier sau director**, te sfătuim să rezolvi linkul simbolic pentru funcționarea corectă a regulii Application Control. Pentru aceasta, fă clic pe butonul **Convertește link simbolic**.

Adăugarea fișierelor executabile din directorul Fișiere executabile în categoria de aplicații

În directorul **Executable files** este afișată lista de fișiere executabile detectate pe computere. Kaspersky Endpoint Security generează o listă de fișiere executabile după executarea activității Inventar.

Pentru a adăuga fișiere executabile din directorul Executable files în categoria de aplicații:

1. Deschide Consolă de administrare a Kaspersky Security Center.

2. În arborele Consolă de administrare, selectează **Advanced** → **Application management** → **Executable files**.

3. În spațiul de lucru, selectați fișierele executabile pe care dorești să le adaugi în categoria de aplicații.

4. Faceți clic dreapta pentru a deschide meniul contextual pentru fișierele executabile selectate și selectați **Add to category**.

5. În fereastra care se deschide, procedează după cum urmează:

   - În partea de sus a ferestrei, alege una dintre următoarele opțiuni:

     - **Add to a new application category**. Alege această opțiune dacă dorești să creezi o nouă categorie de aplicații și să adaugi fișiere executabile în aceasta.

     - **Add to an existing application category**. Alege această opțiune dacă dorești să selectezi o categorie de aplicații existentă și să adaugi fișiere executabile în aceasta.

   - În blocul **Rule type**, selectați una dintre următoarele opțiuni:

     - **Rules for adding to inclusions**. Selectați această opțiune dacă dorești să creezi o condiție care adaugă fișiere executabile în categoria de aplicații.

     - **Rules for adding to exclusions**. Selectați această opțiune dacă dorești să creezi o condiție care exclude fișiere executabile în categoria de aplicații.

   - În blocul **Parameter used as a condition**, selectați una dintre următoarele opțiuni:

     - **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. Salvați-vă modificările.

Adăugarea fișierelor executabile asociate evenimentelor în categoria de aplicații

Pentru a adăuga fișiere executabile asociate cu evenimente Application Control în categoria de aplicații:

1. Deschide Consolă de administrare a Kaspersky Security Center.

2. În nodul **Administration Server** din arborele consolei de administrare, selectați fila **Events**.

3. Alege o selecție de evenimente legate de funcționarea componentei Application Control (Vizualizarea evenimentelor rezultate din funcționarea componentei Application Control, Vizualizarea evenimentelor rezultate din operațiunea de testare a componentei Application Control) în lista verticală **Event selections**.

4. Faceți clic pe butonul **Run selection**.

5. Selectați evenimentele ale căror fișiere executabile asociate dorești să le adaugi în categoria de aplicații.

6. Faceți clic dreapta pentru a deschide meniul contextual pentru evenimentele selectate și selectați **Add to category**.

7. În fereastra care se deschide, configurați setările categoriei aplicației:

   - În partea de sus a ferestrei, alege una dintre următoarele opțiuni:

     - **Add to a new application category**. Alege această opțiune dacă dorești să creezi o nouă categorie de aplicații și să adaugi fișiere executabile în aceasta.

     - **Add to an existing application category**. Alege această opțiune dacă dorești să selectezi o categorie de aplicații existentă și să adaugi fișiere executabile în aceasta.

   - În blocul **Rule type**, selectați una dintre următoarele opțiuni:

     - **Rules for adding to inclusions**. Selectați această opțiune dacă dorești să creezi o condiție care adaugă fișiere executabile în categoria de aplicații.

     - **Rules for adding to exclusions**. Selectați această opțiune dacă dorești să creezi o condiție care exclude fișiere executabile în categoria de aplicații.

   - În blocul **Parameter used as a condition**, selectați una dintre următoarele opțiuni:

     - **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. Salvați-vă modificările.

Adăugarea unei reguli Application Control

Pentru a adăuga o regulă Application Control folosind Kaspersky Security Center:

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.

2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

3. În fereastra politicii, selectați **Security Controls → Application Control**.
   În partea dreaptă a ferestrei se afișează setările componentei Application Control.

4. Fă clic pe **Adaugă**.
   Se deschide fereastra **Regulă Application Control**.

5. Efectuează una dintre următoarele acțiuni:

   - Dacă dorești să creezi o categorie nouă:

     a. Fă clic pe **Creare categorie**.
        Pornește expertul de creare a categoriilor de utilizatori.

b. Urmează instrucțiunile din Expertul pentru crearea categoriilor de utilizatori.

c. În lista verticală **Categorie**, selectați categoria de aplicații creată.

- Dacă dorești să editezi o categorie existentă:

  a. În lista verticală **Categorie**, selectați categoria de aplicații creată pe care dorești să o editezi.

  b. Fă clic pe **Proprietăți**.

  c. Modifică setările categoriei de aplicații selectate.

  d. Salvați-vă modificările.

  e. În lista verticală **Categorie**, selectați categoria de aplicații creată pe baza căreia dorești să creezi o regulă.

6. În tabelul **Utilizatori și drepturile lor**, fă clic pe butonul **Adaugă**.

   Poți selecta utilizatori în Active Directory, în lista de conturi din Kaspersky Security Center sau introducând manual un nume de utilizator local. Kaspersky recomandă utilizarea conturilor de utilizator locale numai în cazuri speciale, când nu este posibilă utilizarea conturilor de utilizator de domeniu.

7. În tabelul **Utilizatori și drepturile lor**, întreprindeți una dintre acțiunile următoare:

   - Dacă dorești să permiți utilizatorilor și/sau grupurilor de utilizatori să pornească aplicațiile care aparțin categoriei selectate, bifați caseta de selectare **Permite** în rândurile relevante.

   - Dacă dorești să blochezi utilizatori și/sau grupuri de utilizatori să pornească aplicațiile care aparțin categoriei selectate, bifați casetele de selectare **Blochează** în rândurile relevante.

8. Bifați caseta de selectare **Refuză pentru alți utilizatori** dacă dorești ca toți utilizatorii care nu apar în coloana **Utilizator sau grup** și care nu fac parte din grupul de utilizatori specificat în coloana **Utilizator sau grup** să nu poată porni aplicațiile care aparțin categoriei selectate.

9. Dacă dorești ca aplicația Kaspersky Endpoint Security să considere aplicațiile incluse în categoria de aplicații selectate ca fiind programe de actualizare de încredere care au permisiunea să creeze alte fișiere executabile care, la rândul lor, vor avea permisiunea să se execute ulterior, bifați caseta de selectare **Programe de actualizare de încredere**.

   Atunci când se migrează setări Kaspersky Endpoint Security, se migrează și lista de fișiere executabile create de către programe de actualizare de încredere.

10. Salvați-vă modificările.

Pentru a adăuga sau a edita o regulă Application Control:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Security Controls** → **Application Control**.

3. Fă clic pe butonul **Aplicații blocate** sau **Aplicații permise**.

   Aceasta deschide lista regulilor Application Control.

4. Fă clic pe **Adaugă**.

   Se deschide fereastra cu setările regulii Application Control.

5. În fila **Setări generale**, definiți principalele setări ale regulii:

   a. În câmpul **Nume regulă**, introduceți numele regulii.

   b. În câmpul **Descriere**, introduceți o descriere a regulii.

   c. În tabelul **Utilizatori și drepturile lor**, fă clic pe butonul **Adaugă**.

   Poți selecta utilizatori în Active Directory, în lista de conturi din Kaspersky Security Center sau introducând manual un nume de utilizator local. Kaspersky recomandă utilizarea conturilor de utilizator locale numai în cazuri speciale, când nu este posibilă utilizarea conturilor de utilizator de domeniu.

   Regula se aplică implicit tuturor utilizatorilor.

   > Dacă în tabel nu este specificat niciun utilizator, regula nu poate fi salvată.

   d. În tabelul **Utilizatori și drepturile lor**, utilizați comutatorul pentru a defini dreptul utilizatorilor de a porni aplicații.

   e. Bifați caseta de selectare **Refuză pentru alți utilizatori** dacă vrei ca aplicația să împiedice aplicațiile care satisfac condițiile de declanșare a regulii să fie executate pentru toți utilizatorii care nu sunt listați în tabelul **Utilizatori și drepturile lor** și nu sunt membri ai grupurilor de utilizatori listate în tabelul **Utilizatori și drepturile lor**.

   > Când caseta de selectare **Refuză pentru alți utilizatori** este debifată, Kaspersky Endpoint Security nu controlează pornirea aplicațiilor de către utilizatori care nu sunt specificați în tabelul **Utilizatori și drepturile lor** și care nu aparțin grupului de utilizatori specificat în tabelul **Utilizatori și drepturile lor**.

   f. Bifează caseta de selectare **Programe de actualizare de încredere** dacă doriști ca Kaspersky Endpoint Security să ia în considerare aplicațiile care se potrivesc condițiilor de declanșare a regulii ca programe de actualizare de încredere. *Programe de actualizare de încredere* sunt aplicații cărora li se permite să creeze alte fișiere executabile care să ruleze ulterior.

   Dacă o aplicație declanșează mai multe reguli, Kaspersky Endpoint Security setează indicatorul *Programe de actualizare de încredere* dacă sunt îndeplinite următoarele condiții:

   - Toate regulile permit rularea aplicației.
   - Cel puțin o regulă are bifată caseta de selectare **Programe de actualizare de încredere**.

6. În fila **Condiții: N**, creați sau editați lista condițiilor de includere pentru declanșarea regulii.

7. În fila **Excluderi: N**, creați sau editați lista condițiilor de excludere pentru declanșarea regulii.

   Atunci când se migrează setări Kaspersky Endpoint Security, se migrează și lista de fișiere executabile create de către programe de actualizare de încredere.

8. Salvați-vă modificările.

Modificarea stării unei reguli Application Control folosind Kaspersky Security Center

Pentru a modifica starea unei reguli Application Control în Consola de administrare:

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Security Controls → Application Control**.

   În partea dreaptă a ferestrei se afișează setările componentei Application Control.
4. În coloana **Stare**, faceți clic stânga pentru a afișa meniul contextual și selectați una dintre opțiunile următoare:

   - **Pornit**. Această stare înseamnă că regula este utilizată atunci când se execută componenta Application Control.
   - **Oprit**. Această stare înseamnă că regula este ignorată atunci când se execută componenta Application Control.
   - **Test**. Această stare înseamnă că Kaspersky Endpoint Security permite întotdeauna pornirea aplicațiilor cărora li se aplică regulile, dar înregistrează în raport informații despre pornirea aplicațiilor respective.
5. Salvați-vă modificările.

Pentru a modifica starea unei reguli Application Control în interfața aplicației:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Security Controls → Application Control**.
3. Fă clic pe butonul **Aplicații blocate** sau **Aplicații permise**.

   Aceasta deschide lista regulilor Application Control.
4. În coloana **Stare**, deschideți meniul contextual și selectați una dintre opțiunile următoare:

   - **Activată**. Această stare înseamnă că regula este utilizată atunci când se execută componenta Application Control.
   - **Dezactivată**. Această stare înseamnă că regula este ignorată atunci când se execută componenta Application Control.
   - **Modul Testare**. Această stare înseamnă că Kaspersky Endpoint Security permite întotdeauna pornirea aplicațiilor cărora li se aplică această regulă, dar înregistrează în raport informații despre pornirea aplicațiilor respective.
5. Salvați-vă modificările.

Exportul și importul regulilor Application Control

Puteți exporta lista de reguli Application Control într-un fișier XML. Puteți utiliza funcția de export/import pentru a face o copie de rezervă a listei de reguli Application Control sau pentru a migra lista pe un alt server.

Când exportați sau importați reguli Application Control, vă rugăm să rețineți următoarele aspecte:

- Kaspersky Endpoint Security exportă lista de reguli numai pentru modul Application Control activ. Cu alte cuvinte, dacă Application Control funcționează în modul Listă respinse, Kaspersky Endpoint Security exportă regulile numai pentru acest mod. Pentru a exporta lista de reguli pentru modul Listă permise, trebuie să comutați modul și să executați operațiunea de export din nou.

- Kaspersky Endpoint Security utilizează categorii de aplicații pentru ca regulile Application Control să funcționeze. Când migrați lista de reguli Application Control către un server diferit, trebuie să migrați și lista categoriilor de aplicații. Pentru mai multe detalii despre exportul sau importul categoriilor de aplicații, consultați Ajutor pentru Kaspersky Security Center.

Cum se exportă și se importă o listă de reguli Application Control în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Security Controls → Application Control**.
4. Pentru a exporta lista de reguli Application Control:
   a. Selectați regulile pe care doriți să le exportați. Pentru a selecta mai multe porturi, utilizați tastele **CTRL** sau **SHIFT**.
      Dacă nu ați selectat nicio regulă, Kaspersky Endpoint Security va exporta toate regulile.
   b. Faceți clic pe linkul **Exportă**.
   c. În fereastra care se deschide, specificați numele fișierului XML în care doriți să exporți lista de reguli și selectați directorul în care doriți să salvați acest fișier.
   d. Salvați fișierul.
      Kaspersky Endpoint Security exportă lista de reguli în fișierul XML.
5. Pentru a importa o listă de reguli Application Control:
   a. Faceți clic pe linkul **Importă**.
      În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de reguli.
   b. Deschideți fișierul.
      În cazul în care computerul are deja o listă de reguli, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul XML.
6. Salvați-vă modificările.

Cum se exportă și se importă o listă de reguli Application Control în Consola Web și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.
   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Security Controls** → **App Control**.
5. În **Operating mode**, selectează o listă de reguli: lista de aplicații permise sau respinse.
6. Pentru a exporta lista de reguli:
   a. Selectați regulile pe care doriți să le exportați.
   b. Fă clic pe butonul → **Export**.
      Kaspersky Endpoint Security exportă lista de reguli într-un fișier JSON în directorul de descărcări implicit.
7. Pentru a importa lista de reguli:
   a. Fă clic pe butonul → **Import**.
      În fereastra care se deschide, selectați fișierul JSON din care doriți să importați lista de reguli.
   b. Deschideți fișierul.
      În cazul în care computerul are deja o listă de reguli, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul JSON.
8. Salvați-vă modificările.

Vizualizarea evenimentelor rezultate din funcționarea componentei Application Control

Pentru a vizualiza evenimente care rezultă din funcționarea componentei Application Control primite de Kaspersky Security Center:

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În nodul **Administration Server** din arborele consolei de administrare, selectați fila **Events**.
3. Faceți clic pe butonul **Create a selection**.
4. În fereastra care se deschide, selectați secțiunea **Events**.
5. Faceți clic pe butonul **Clear all**.
6. În tabelul **Events**, bifați caseta de selectare **Pornire aplicație interzisă**.
7. Salvați-vă modificările.

8. În lista verticală **Event selections**, selectați selecția creată.

9. Faceți clic pe butonul **Run selection**.

Vizualizarea unui raport despre aplicațiile blocate

Pentru a vizualiza raportul despre aplicațiile blocate:

1. Deschide Consolă de administrare a Kaspersky Security Center.

2. În nodul **Administration Server** din arborele consolei de administrare, selectați fila **Reports**.

3. Fă clic pe **New report template**.

   Se lansează Expertul pentru șablon de raport nou.

4. Urmează instrucțiunile din Expertul pentru șablon de raport. La pasul **Selecting the report template type**, selectați **Other** → **Report on prohibited applications**.

   După ce ai finalizat Expertul pentru șablon de raport nou, un nou șablon de raport apare în tabelul din fila **Reports**.

5. Deschide raportul făcând dublu clic pe acesta.

Începe procesul de generare a raportului. Raportul este afișat într-o fereastră nouă.

Testarea regulilor Application Control

Pentru a te asigura că regulile Application Control nu îți blochează aplicații de care ai nevoie la serviciu, se recomandă să activezi testarea pentru regulile Application Control și să analizezi funcționarea lor după crearea de reguli noi. Când este activată testarea regulilor Application Control, Kaspersky Endpoint Security nu va bloca aplicațiile a căror lansare este interzisă de Application Control, dar va trimite către serverul de administrare notificări despre pornirea lor.

O analiză a funcționării regulilor Application Control implică examinarea evenimentelor componentei Application Control rezultate și raportate către Kaspersky Security Center. Dacă modul de testare are drept rezultat absența evenimentelor blocate la pornire pentru toate aplicațiile necesare utilizatorului computerului, aceasta înseamnă că au fost create regulile corecte. În caz contrar, ți se solicită să actualizezi setările regulilor create, să creezi reguli suplimentare sau să ștergi regulile existente.

În mod implicit, Kaspersky Endpoint Security permite pornirea tuturor aplicațiilor, cu excepția aplicațiilor interzise de reguli.

Activarea și dezactivarea testării regulii Application Control

Pentru a activa sau dezactiva testarea regulilor funcției Application Control în Kaspersky Security Center:

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.

2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

3. În fereastra politicii, selectați **Security Controls** → **Application Control**.

   În partea dreaptă a ferestrei se afișează setările componentei Application Control.

4. În lista verticală **Mod control**, selectați unul dintre elementele următoare:

   - **Listă respinse**. Dacă este selectată această opțiune, Application Control permite tuturor utilizatorilor să pornească orice aplicație, cu excepția cazurilor care satisfac condițiile din regulile de blocare ale Application Control.
   - **Listă permise**. Dacă este selectată această opțiune, Application Control blochează toți utilizatorii să pornească orice aplicație, cu excepția cazurilor care satisfac condițiile din regulile de permitere ale componentei Application Control.

5. Efectuează una dintre următoarele acțiuni:

   - Dacă doriți să activați testarea regulilor Application Control, selectați opțiunea **Testează regulile** în lista verticală **Acțiune**.
   - Dacă doriți să activați componenta Application Control pentru a gestiona pornirea aplicațiilor pe computerele utilizatorului, în lista verticală, selectați **Aplica reguli**.

6. Salvați-vă modificările.

Pentru a activa testarea regulilor Application Control sau pentru a selecta o acțiune de blocare pentru Application Control:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Security Controls** → **Application Control**.
3. Fă clic pe butonul **Aplicații blocate** sau **Aplicații permise**.

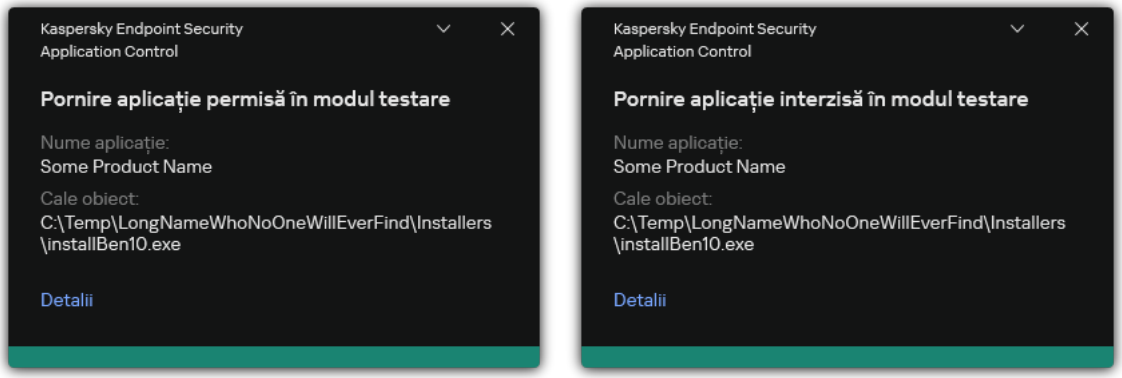
   Aceasta deschide lista regulilor Application Control.

4. În coloana **Stare**, selectați **Modul Testare**.

   Această stare înseamnă că Kaspersky Endpoint Security permite întotdeauna pornirea aplicațiilor cărora li se aplică această regulă, dar înregistrează în raport informații despre pornirea aplicațiilor respective.

5. Salvați-vă modificările.

Kaspersky Endpoint Security nu va bloca aplicațiile a căror lansare este interzisă de componenta Application Control, dar va trimite către serverul de administrare notificări despre pornirea lor. Poți, de asemenea, să configurezi afișarea notificărilor despre testarea regulilor pe computerul utilizatorului (consultă figura de mai jos).



Notificări Application Control în modul de testare

Vizualizarea unui raport despre aplicațiile blocate în modul de testare

Pentru a vizualiza raportul despre aplicațiile blocate în modul de testare:

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În nodul **Administration Server** din arborele consolei de administrare, selectați fila **Reports**.
3. Fă clic pe **New report template**.

   Se lansează Expertul pentru șablon de raport nou.

4. Urmează instrucțiunile din Expertul pentru șablon de raport. La pasul **Selecting the report template type**, selectați **Other → Report on prohibited applications in test mode**.

   După ce ai finalizat Expertul pentru șablon de raport nou, un nou șablon de raport apare în tabelul din fila **Reports**.

5. Deschide raportul făcând dublu clic pe acesta.

Începe procesul de generare a raportului. Raportul este afișat într-o fereastră nouă.

Vizualizarea evenimentelor rezultate din testarea funcționării componentei Application Control

Pentru a vizualiza evenimentelede testare pentru Application Control primite de Kaspersky Security Center:

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În nodul **Administration Server** din arborele consolei de administrare, selectați fila **Events**.
3. Faceți clic pe butonul **Create a selection**.
4. În fereastra care se deschide, selectați secțiunea **Events**.
5. Faceți clic pe butonul **Clear all**.
6. În tabelul **Events**, bifați casetele de selectare **Pornire aplicație interzisă în modul testare** și **Pornire aplicație permisă în modul testare**.
7. Salvați-vă modificările.
8. În lista verticală **Event selections**, selectați selecția creată.
9. Faceți clic pe butonul **Run selection**.

Monitorizare activitate aplicație

Această componentă este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Windows pentru stații de lucru. Această componentă nu este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Windows pentru servere.

Monitorizare activitate aplicație este un instrument destinat vizualizării în timp real a informațiilor despre activitatea aplicațiilor de pe computerul unui utilizator.

Utilizarea funcției Monitorizare activitate aplicație necesită instalarea componentelor Application Control și Host Intrusion Prevention. Dacă aceste componente nu sunt instalate, secțiunea Monitorizare activitate aplicație din fereastra principală a aplicației este ascunsă.

Pentru a porni Monitorizare activitate aplicație:

În fereastra principală a aplicației, în secțiunea **Monitorizare**, faceți clic pe dala **Monitorizare activitate aplicație**.

În această fereastră, sunt prezentate informații despre activitatea aplicațiilor de pe computerul utilizatorului, în trei file:

- Fila **Toate aplicațiile** afișează informații despre toate aplicațiile instalate pe computer.
- Fila **În execuție** tafișează informații în timp real despre consumul de resurse ale computerului de fiecare aplicație. Din această filă, puteți începe să configurați permisiunile pentru o aplicație anume.
- Fila **Execută la pornire** afișează lista de aplicații care pornesc odată cu pornirea computerului.

Dacă dorești să ascunzi informațiile despre activitatea aplicației pe computerul unui utilizator, poți restricționa accesul utilizatorului la instrumentul Monitorizare activitate aplicație.

Cum se ascunde instrumentul Monitorizare activitate aplicație în interfața aplicației utilizând Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Setări generale** → **Interfață**.
4. Utilizați caseta de selectare **Ascundeți secțiunea Monitorizare activitate aplicație** pentru a acorda sau revoca accesul la instrument.
5. Salvați-vă modificările.

Cum se ascunde instrumentul Monitorizare activitate aplicație în interfața aplicației utilizând Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **General Settings** → **User Interaction**.
5. Utilizați caseta de selectare **Hide Application Activity Monitor section** pentru a acorda sau revoca accesul la instrument.
6. Salvați-vă modificările.

Reguli pentru crearea măștilor de nume pentru fișiere sau directoare

O *mască de nume de fișier sau director* este o reprezentare a numelui unui director sau a numelui și a extensiei unui fișier folosind caractere obișnuite.

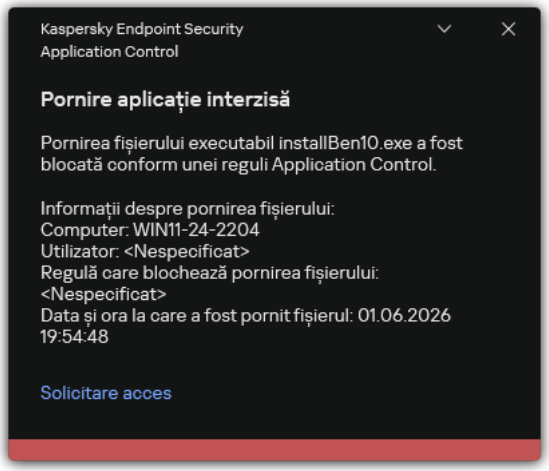
Puteți folosi următoarele caractere obișnuite pentru a crea o mască de nume de fișier sau director:

- Caracterul `*` (asterisc), care ia locul oricărui set de caractere (inclusiv a unui set gol). De exemplu, masca `C:\*.txt` va include toate căile către fișierele cu extensia `txt` din directoarele și subdirectoarele de pe unitatea (C:).

- `?` (semn de întrebare) ține locul oricărui caracter individual, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\???.txt` va include căi pentru toate fișierele din directorul denumit `Folder` care au extensia TXT și un nume format din trei caractere.

Editarea șabloanelor de mesaje aferente componentei Application Control

Atunci când un utilizator încearcă să pornească o aplicație blocată de o regulă Application Control, Kaspersky Endpoint Security afișează un mesaj referitor la blocarea pornirii aplicației. Experții Kaspersky oferă utilizatorului un șablon de mesaj care descrie motivele pentru care aplicația a fost blocată (vezi figura de mai jos). Sunt furnizate variabile speciale pentru gestionarea șabloanelor pentru mesaje (de exemplu, `%USER_NAME%`). Variabilele permit utilizarea unui singur șablon de mesaj pentru computere diferite. La generarea unui mesaj, Kaspersky Endpoint Security preia valoarea variabilei din setările sistemului de operare și o inserează în mesajul corespunzător computerului, utilizatorului și evenimentului specific.



Notificarea Application Control

Dacă utilizatorul consideră că pornirea aplicației a fost blocată din greșeală, el poate utiliza linkul din mesajul text pentru a trimite un mesaj administratorului rețelei locale a companiei. Pentru a face acest lucru, utilizatorul trebuie să facă clic pe butonul **Solicitare acces** și să trimită un mesaj administratorului care descrie situația. De asemenea, poți pregăti un șablon al mesajului pentru administrator, adăugând la acesta date care pot preciza decizia de a permite sau de a bloca accesul la aplicație. După ce utilizatorul solicită accesul, Kaspersky Endpoint Security trimite un eveniment către Kaspersky Security Center: **Mesaj către administrator privind blocarea pornirii aplicației**. Descrierea evenimentului conține un mesaj către administrator cu variabile înlocuite. Puteți vizualiza aceste evenimente în consola Kaspersky Security Center, utilizând selecția de evenimente predefinită **User requests**. Dacă organizația dvs. nu are instalat Kaspersky Security Center sau nu există nicio conexiune la serverul de administrare, aplicația va trimite un mesaj administratorului la adresa de e-mail specificată.

Cum se editează șablonul de mesaj al componentei Application Control în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Security Controls → Application Control**.
4. În blocul **Setări șablon de mesaje**, fă clic pe butonul **Șabloane**.
5. Aceasta deschide o fereastră; în acea fereastră, configurează șabloanele Application Control:

   - **Mesaj despre blocare**. Șablonul mesajului care se afișează atunci când este declanșată o regulă Application Control care blochează pornirea unei aplicații.

     Nu poți configura șabloanele de mesaje pentru Application Control în modul de testare. Componenta Application Control în modul de testare afișează notificări prestabilite.

   - **Mesaj către administrator**. Șablon al mesajului pe care un utilizator îl poate trimite administratorului rețelei LAN corporative dacă utilizatorul consideră că o aplicație a fost blocată din greșeală.

   Pentru a adăuga o variabilă la textul șablonului, plasează cursorul în poziția dorită, fă clic pe **Variabilă** și selectează variabila necesară din lista de opțiuni disponibile.

   De asemenea, poți restaura textul șablonului implicit utilizând butonul **În mod implicit**.
6. Salvați-vă modificările.

Cum se schimbă șablonul de mesaj al componentei Application Control în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management → Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Security Controls → App Control**.
5. În blocul **Message templates**, fă clic pe linkul **Messages about application startup block** și configurează șabloanele pentru mesajele componentei Application Control:

   - **Message to user**. Șablonul mesajului care se afișează atunci când este declanșată o regulă Application Control care blochează pornirea unei aplicații.

     Nu poți configura șabloanele de mesaje pentru Application Control în modul de testare. Componenta Application Control în modul de testare afișează notificări prestabilite.

   - **Message to administrator**. Șablon al mesajului pe care un utilizator îl poate trimite administratorului rețelei LAN corporative dacă utilizatorul consideră că o aplicație a fost blocată din greșeală.

   Pentru a adăuga o variabilă la textul șablonului, plasează cursorul în poziția dorită, fă clic pe **Add variable** și selectează variabila necesară din lista de opțiuni disponibile.

   De asemenea, poți restaura textul șablonului implicit utilizând butonul **Reset to default**.
6. Salvați-vă modificările.

Cum se editează șablonul de mesaj al componentei Application Control în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Security Controls** → **Application Control**.
3. În blocul **Șabloanele mesajelor despre blocarea aplicației**, configurează șabloanele pentru mesajele componentei Application Control:

   - **Mesaj despre blocare**. Șablonul mesajului care se afișează atunci când este declanșată o regulă Application Control care blochează pornirea unei aplicații.

     Nu poți configura șabloanele de mesaje pentru Application Control în modul de testare. Componenta Application Control în modul de testare afișează notificări prestabilite.

   - **Mesaj către administrator**. Șablon al mesajului pe care un utilizator îl poate trimite administratorului rețelei LAN corporative dacă utilizatorul consideră că o aplicație a fost blocată din greșeală.

   Pentru a adăuga o variabilă la textul șablonului, plasează cursorul în poziția dorită, fă clic pe **Adaugă variabilă** și selectează variabila necesară din lista de opțiuni disponibile.

   De asemenea, poți restaura textul șablonului implicit utilizând butonul **Resetează**.

4. Salvați-vă modificările.

Variabile în șabloanele de mesaje pentru Application Control

Poți utiliza următoarele variabile în șabloanele de mesaje pentru utilizatori sau în șabloanele de mesaje pentru administratori:

- **Numele regulii care a fost declanșată** – `%RULE%`.

  Numele regulii care a blocat execuția unui fișier.

- **Dată curentă** – `%DATE%`.

  Data la care executarea fișierului a fost blocată, în formatul ZZ.LL.AAAA.

- **Oră curentă** – `%TIME%`.

  Ora la care executarea fișierului a fost blocată, în formatul HH:MM.

- **Nume utilizator** – `%USER_NAME%`.

  Numele contului de utilizator curent de pe computerul pe care a fost blocată executarea fișierului, în formatul `<device name>\<user alias>` (de exemplu, `DESKTOP-123\John.Smith`).

- **Nume computer** – `%COMPUTER_NAME%`.

  Numele computerului pe care a fost blocată executarea fișierului.

- **Nume fișier executabil** – `%FILE_NAME%`.

  Numele fișierului executabil al aplicației blocate.

- **Categoria KL a fișierului executabil** – `%KL_CAT%`.

  Categoria KL căreia îi aparține aplicația blocată (de exemplu, *Browsere* sau altă categorie).

- **Calea către fișierul executabil** – %FILE_PATH%.

  Calea completă către fișierul executabil al aplicației blocate.

- **Versiunea fișierului executabil** – %FILE_VERSION%.

  Versiunea fișierului executabil al aplicației blocate.

- **Numele original al fișierului executabil** – %ORIGINAL_FILE_NAME%.

  Numele original al fișierului executabil al aplicației blocate. Numele fișierului este specificat în proprietățile fișierului executabil al aplicației.

- **Producător** – %FILE_PUBLISHER%.

  Producătorul aplicației blocate.

- **Nume aplicație** – %FILE_PRODUCT_NAME%.

  Numele aplicației blocate.

- **Versiune aplicație** – %PRODUCT_VERSION%.

  Versiunea aplicației blocate.

- **Cod hash fișier executabil** – %FILE_HASH%.

  Codul hash al fișierului executabil al aplicației blocate.

- **Emitent certificat** – %CERT_ISSUER%.

  Emitentul certificatului cu care este semnat fișierul executabil.

- **Titular certificat** – %CERT_SUBJECT%.

  Subiectul certificatului cu care este semnat fișierul executabil.

- **Amprentă certificat** – %CERT_THUMBPRINT%.

  Amprenta certificatului cu care este semnat fișierul executabil.

Cele mai bune practici pentru implementarea unei liste de aplicații permise

Când planificați implementarea modulului listei albe, vă recomandăm să efectuați acțiunile următoare:

1. Formează următoarele tipuri de grupuri:

   - Grupuri de utilizatori. Grupurile de utilizatori pentru care trebuie să permiți utilizarea diverselor seturi de aplicații.

   - Grupuri de administrare. Unul sau mai multe grupuri de computere cărora Kaspersky Security Center le va aplica lista de aplicații permise. Este necesar să creați mai multe grupuri de computere dacă sunt utilizate setări diferite ale listei permise pentru acele grupuri.

2. Creează o listă de aplicații a căror pornire trebuie permisă.

Înainte de crearea unei liste, ți se recomandă următoarele:

a. Execută activitatea de inventar.

Informațiile despre crearea, reconfigurarea și pornirea unei activități de inventariere sunt disponibile în secțiunea Gestionare activități.

b. Vizualizare listă fișiere executabile.

Configurarea modului listă permise pentru aplicații

Când configurați modul listei permise, vă recomandăm să efectuați acțiunile următoare:

1. Creează categorii de aplicații care să conțină aplicațiile a căror pornire trebuie permisă.

Poți selecta una dintre următoarele metode pentru crearea categoriilor de aplicații:

- **Category with content added manually**. Poți adăuga manual în această categorie folosind condițiile următoare:
  - Metadate fișier. Kaspersky Security Center adaugă în categoria de aplicații toate fișierele executabile alături de metadatele specificate.
  - Cod hash fișier. Kaspersky Security Center adaugă în categoria de aplicații toate fișierele executabile alături de hash-urile specificate.

    Folosirea acestei condiții exclude posibilitatea de instalarea automată a actualizărilor pentru că versiunile diferite ale fișierelor vor avea coduri hash diferite.

  - Certificat fișier. Kaspersky Security Center adaugă în categoria de aplicații toate fișierele executabile alături de certificatul specificat.
  - Categorie KL. Kaspersky Security Center adaugă în categoria de aplicații toate aplicațiile aflate în categoria KL specificată.
  - Directorul aplicației. Kaspersky Security Center adăugă în categoria de aplicații toate fișierele executabile din acest director.

    Folosirea condiției **Application folder** poate fi nesigură pentru că se va permite pornirea oricărei aplicații din directorul specificat. Se recomandă să aplici reguli care utilizează categoriile de aplicații cu condiția **Application folder** doar acelor utilizatori pentru care trebuie permisă instalarea automată a actualizărilor.

- **Category that includes executable files from a specific folder**. Poți specifica un director din care fișierele executabile vor fi atribuite automat categoriei de aplicații create.
- **Category that includes executable files from selected devices**. Poți specifica un computer pentru care toate fișierele executabile vor fi atribuite automat categoriei de aplicații create.

Când se folosește această metodă de creare a categoriilor de aplicații, Kaspersky Security Center primește informații despre aplicațiile de pe computer din directorul **Executable files**.

2. Selectați modul de listă permisă pentru componenta Application Control.

3. Creează reguli Application Control folosind categoriile de aplicații create.

   Regula **Imagine de aur** și regula **Programe de actualizare de încredere** sunt inițial definite pentru modul Listă permise. Aceste reguli Application Control corespund categoriilor KL. Categoria KL *Imagine de aur* include programe care asigură funcționarea normală a sistemului de operare. Categoria KL *Programe de actualizare de încredere* include programe de actualizare de la cei mai reputați distribuitori de software. Nu poți șterge aceste reguli. Setările acestor reguli nu pot fi editate. În mod implicit, regula **Imagine de aur** este activată, iar regula **Programe de actualizare de încredere** este dezactivată. Tuturor utilizatorilor le este permis să pornească aplicații care corespund condițiilor de declanșare din aceste reguli.

4. Stabilește aplicațiile pentru care trebuie permisă instalarea automată a actualizărilor.

   Poți permite instalarea automată a actualizărilor prin una dintre modalitățile următoare:

   - Specifică o listă extinsă de aplicații permise prin activarea pornirii tuturor aplicațiilor care aparțin unei categorii KL.
   - Specifică o listă extinsă de aplicații permise prin activarea pornirii tuturor aplicațiilor semnate cu certificate.

     Pentru a permite pornirea tuturor aplicațiilor semnate cu certificate, poți crea o categorie cu condiție bazată pe certificat care folosește numai parametrul **Subject** cu valoarea `*`.
   - Pentru regula Application Control, selectați parametrul **Programe de actualizare de încredere**. Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security consideră aplicațiile incluse în reguli drept Programe de actualizare de încredere. Kaspersky Endpoint Security permite pornirea aplicațiilor instalate sau actualizate de către aplicații incluse în regulă, cu condiția să nu fie aplicate reguli de blocare respectivelor aplicații.

     Atunci când se migrează setări Kaspersky Endpoint Security, se migrează și lista de fișiere executabile create de către programe de actualizare de încredere.
   - Creează un dosar și plasează în el fișierele executabile ale aplicațiilor pentru care dorești să permiți instalarea automată de actualizări. Apoi creează o categorie de aplicații cu condiția **Application folder** și stabilește calea către respectivul director. Apoi creează o regulă de permitere și selectați această categorie.

     Folosirea condiției **Application folder** poate fi nesigură pentru că se va permite pornirea oricărei aplicații din directorul specificat. Se recomandă să aplici reguli care utilizează categoriile de aplicații cu condiția **Application folder** doar acelor utilizatori pentru care trebuie permisă instalarea automată a actualizărilor.

Testarea modului listă permise

Pentru a te asigura că regulile Application Control nu îți blochează aplicații de care ai nevoie la serviciu, se recomandă să activezi testarea pentru regulile Application Control și să analizezi funcționarea lor după crearea de reguli noi. Când este activată testarea, Kaspersky Endpoint Security nu va bloca aplicațiile a căror lansare este interzisă de regulile Application Control, dar va trimite către serverul de administrare notificări despre pornirea lor.

Când testați modul listei permise, vă recomandăm să efectuați acțiunile următoare:

1. Stabilește perioada de testare (de la câteva zile până la două luni).
2. Activează testarea regulilor Application Control.
3. Examinează evenimentele rezultate în urma testării funcționării componentei Application Control și rapoartele despre aplicațiile blocate în modul de testare pentru a analiza rezultatele testării.
4. În funcție de rezultatele analizei, schimbă setările modului listei permise.

   În mod deosebit, în funcție de rezultatele testului, puteți adăuga fișiere executabile referitoare la evenimente într-o categorie de aplicații.

Compatibilitate pentru modul listă permise

După selectarea unei acțiuni de blocare pentru Application Control, vă recomandăm să continuați compatibilitatea modului listei permise efectuând acțiunile următoare:

- Examinează evenimentele rezultate în urma funcționării componentei Application Control și rapoartele despre executările blocate pentru a analiza eficiența Application Control.
- Analizează solicitările utilizatorilor de accesare a aplicațiilor.
- Analizați fișierele executabile necunoscute verificându-le reputația în Kaspersky Security Network.
- Înainte de instalarea actualizărilor pentru sistemul de operare sau pentru software, instalează actualizările respective pe un grup de computere test pentru a verifica modul în care vor fi procesate de regulile Application Control.
- Adaugă aplicațiile necesare în categoriile utilizate în regulile Application Control.

Monitorizarea porturilor de rețea

În timpul funcționării Kaspersky Endpoint Security, componentele Control Web, Mail Threat Protection, Web Threat Protection, Behavior Detection și Exploit Prevention monitorizează fluxurile de date transmise prin protocoale specifice și care trec prin anumite porturi TCP și UDP deschise de pe computerul utilizatorului. De exemplu, componenta Mail Threat Protection analizează informațiile transmise prin SMTP, în timp ce componenta Web Threat Protection analizează informațiile transmise prin HTTP și FTP.

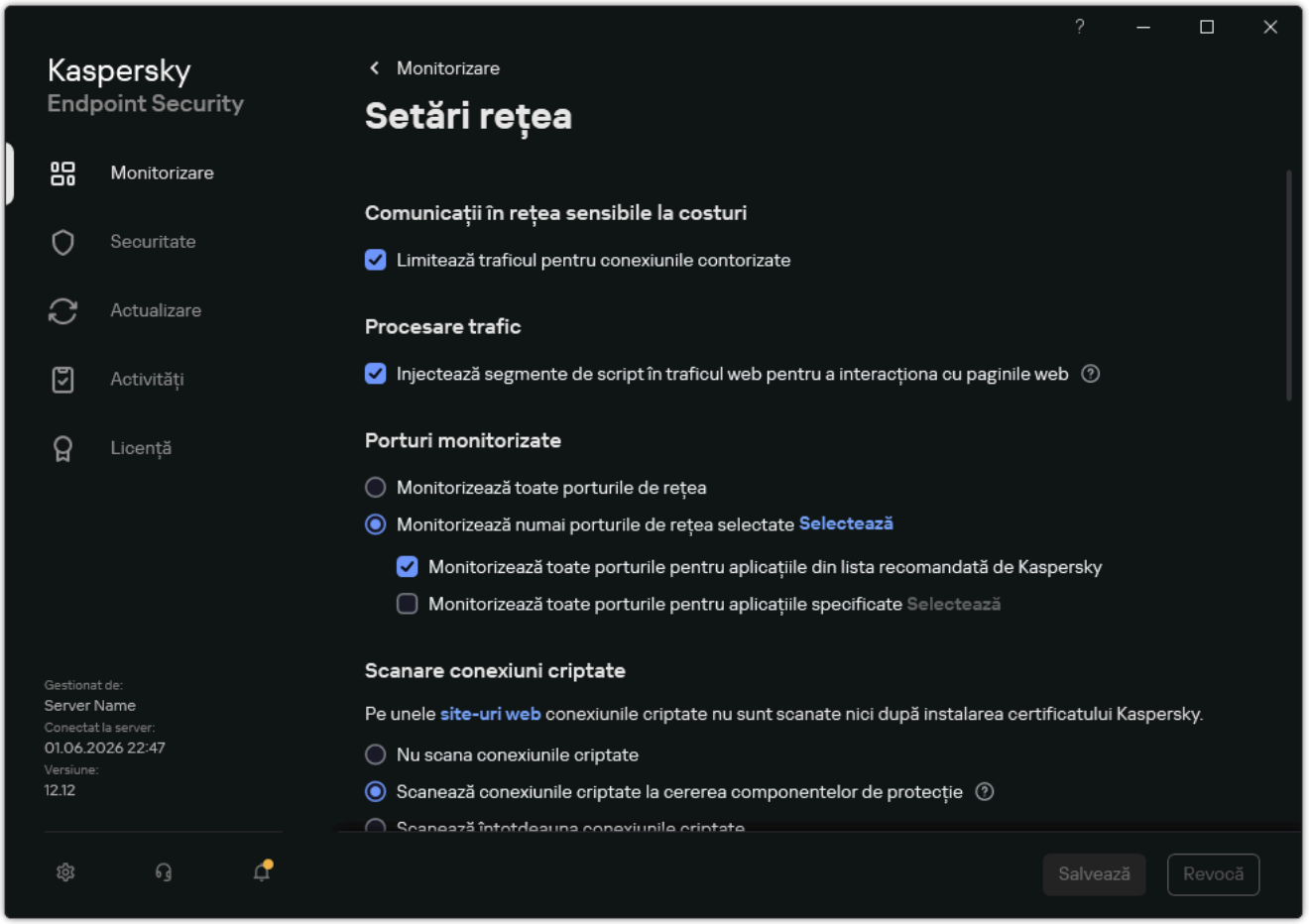
Kaspersky Endpoint Security împarte porturile TCP și UDP ale computerului utilizatorului în mai multe grupuri, în funcție de probabilitatea ca ele să fie compromise. Unele porturi de rețea sunt rezervate serviciilor vulnerabile. Vă recomandăm să monitorizați aceste porturi mai bine, deoarece acestea au o probabilitate mai mare de a fi vizate de un atac de rețea. Dacă utilizezi servicii nestandard care se bazează pe porturi de rețea non-standard, aceste porturi de rețea pot și ele să fie vizate de un computer atacator. Poți specifica o listă de porturi de rețea și o listă de aplicații care solicită acces la rețea. Procedând astfel, aceste porturi și aplicații vor beneficia de atenție specială din partea componentelor Mail Threat Protection și Web Threat Protection în timpul monitorizării traficului de rețea.

Pentru a ajuta la asigurarea securității computerului, componentele Behavior Detection și Exploit Prevention monitorizează și fluxurile de date care trec prin porturile de rețea. Componentele monitorizează continuu traficul de rețea pentru procese individuale care ar putea prezenta amenințări.

Activarea monitorizării tuturor porturilor de rețea

Pentru a activa monitorizarea tuturor porturilor de rețea:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Setări generale** → **Setări rețea**.



Setări monitorizare porturi de rețea

3. În secțiunea **Porturi monitorizate**, selectați **Monitorizează toate porturile de rețea**.
4. Salvați-vă modificările.

Crearea unei liste de porturi de rețea monitorizate

Modificarea listei de porturi de rețea monitorizate poate fi blocată de proprietățile politicii principale. Pentru a modifica lista, trebuie să permiteți modificarea setărilor zonei de încredere în Web Console („lacătul" trebuie să fie deblocat).

Zonele de încredere sunt grupate diferit în Consola de administrare (MMC) și în Web Console. De asemenea, modul în care se împiedică modificarea parametrilor zonei de încredere este diferit („lacăte" diferite). Vă recomandăm să utilizați exclusiv Web Console pentru gestionarea aplicației. În cazul în care configurați zona de încredere pe console diferite, este posibil ca plug-inul de gestionare să reseteze „lacătul" la starea implicită.

Pentru a crea o listă de porturi de rețea monitorizate:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Setări generale** → **Setări rețea**.
3. În secțiunea **Porturi monitorizate**, selectați **Monitorizează numai porturile de rețea selectate**.
4. Fă clic pe **Selectează**.

   Acest lucru deschide o listă de porturi de rețea care, în mod normal, sunt utilizate pentru transmiterea e-mailurilor și a traficului de rețea. Această listă de porturi de rețea este inclusă în pachetul Kaspersky Endpoint Security.
5. Utilizați comutatorul din coloana **Stare** pentru a activa sau a dezactiva monitorizarea portului de rețea.
6. Dacă un port de rețea nu este afișat în lista de porturi de rețea, adaugă-l astfel:
   a. Fă clic pe **Adaugă**.
   b. În fereastra care se deschide, introduceți numărul portului de rețea și o scurtă descriere.
   c. Setați starea **Activă** sau **Inactivă** pentru monitorizarea portului de rețea.
7. Salvați-vă modificările.

Atunci când protocolul FTP se execută în modul pasiv, conexiunea poate fi stabilită printr-un port de rețea aleatoriu, care nu este adăugat în lista de porturi de rețea monitorizate. Pentru a proteja astfel de conexiuni, activați monitorizarea tuturor porturilor de rețea sau configurați controlul porturilor de rețea pentru aplicațiile care stabilesc conexiuni FTP.

Crearea unei liste de aplicații pentru care sunt monitorizate toate porturile de rețea

Poți crea o listă de aplicații pentru care Kaspersky Endpoint Security monitorizează toate porturile de rețea.

Recomandăm includerea aplicațiilor care primesc sau transmit date prin protocolul FTP din lista de aplicații pentru care Kaspersky Endpoint Security monitorizează toate porturile de rețea.

Pentru a crea o listă de aplicații pentru care sunt monitorizate toate porturile de rețea:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Setări generale** → **Setări rețea**.
3. În secțiunea **Porturi monitorizate**, selectați **Monitorizează numai porturile de rețea selectate**.
4. Bifați caseta de selectare **Monitorizează toate porturile pentru aplicațiile din lista recomandată de Kaspersky**.

   Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security monitorizează toate porturile pentru următoarele aplicații:

   - 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. Bifați caseta de selectare **Monitorizează toate porturile pentru aplicațiile specificate**.

6. Fă clic pe **Selectează**.

   Aceasta deschide o listă de aplicații pentru care Kaspersky Endpoint Security monitorizează porturile de rețea.

7. Utilizați comutatorul din coloana **Stare** pentru a activa sau a dezactiva monitorizarea portului de rețea.

8. Dacă o aplicație nu este inclusă în lista de aplicații, adaug-o după cum urmează:

   a. Fă clic pe **Adaugă**.

   b. În fereastra care se deschide, introduceți calea către fișierul executabil al aplicației și o scurtă descriere.

   c. Setați starea **Activă** sau **Inactivă** pentru monitorizarea porturilor de rețea.

9. Salvați-vă modificările.

Exportul și importul listelor de porturi monitorizate

Kaspersky Endpoint Security folosește următoarele liste pentru a monitoriza porturile de rețea: lista porturilor de rețea și lista aplicațiilor ale căror porturi sunt monitorizate de Kaspersky Endpoint Security. Puteți exporta liste de porturi monitorizate într-un fișier XML. Apoi puteți modifica fișierul pentru a adăuga, de exemplu, un număr mare de porturi cu aceeași descriere. De asemenea, puteți utiliza funcția de export/import pentru a face o copie de rezervă a listelor de porturi monitorizate sau pentru a migra listele pe un alt server.

Cum se exportă și se importă liste de porturi monitorizate în Consola de administrare (MMC)

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **General Settings** → **Network Settings**.

5. Pentru a exporta lista de porturi de rețea:

   a. În secțiunea **Monitored ports**, selectați **Monitor selected network ports only**.

   b. Faceți clic pe linkul **N ports selected**.

      Se deschide fereastra **Network ports**. Fereastra **Network ports** afișează o listă de porturi de rețea care, în mod normal, sunt utilizate pentru transmiterea e-mailurilor și a traficului de rețea. Această listă de porturi de rețea este inclusă în pachetul Kaspersky Endpoint Security.

   c. În lista de porturi de rețea, selectați porturile pe care doriți să le exportați.

   d. Fă clic pe **Export**.

   e. În fereastra care se deschide, introdu numele fișierului XML în care dorești să exporți lista cu porturile de rețea și selectează directorul în care dorești să salvezi acest fișier.

   f. Salvați fișierul.

      Kaspersky Endpoint Security exportă întreaga listă de porturi de rețea în fișierul XML.

6. Pentru a exporta lista aplicațiilor ale căror porturi sunt monitorizate de Kaspersky Endpoint Security:

   a. În blocul **Monitored ports**, bifați caseta de selectare **Monitor all ports for specified applications**.

   b. Faceți clic pe linkul **N applications selected**.

   c. În lista de aplicații, selectați aplicațiile pe care doriți să le exportați.

   d. Fă clic pe **Export**.

   e. În fereastra care se deschide, specificați numele fișierului XML în care doriți să exporți lista de aplicații și selectați directorul în care doriți să salvați acest fișier.

   f. Salvați fișierul.

   Kaspersky Endpoint Security exportă întreaga listă de aplicații în fișierul XML.

7. Pentru a importa lista de porturi de rețea:

   a. În lista de porturi de rețea, faceți clic pe butonul din **Import**.

   În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de porturi de rețea.

   b. Deschideți fișierul.

   În cazul în care computerul are deja o listă de porturi de rețea, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul XML.

8. Pentru a importa o listă a aplicațiilor ale căror porturi sunt monitorizate de Kaspersky Endpoint Security:

   a. În lista de aplicații, faceți clic pe butonul **Import**.

   În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de aplicații.

   b. Deschideți fișierul.

   În cazul în care computerul are deja o listă de aplicații, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul XML.

9. Salvați-vă modificările.

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.

2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

3. În fereastra politicii, selectați **Setări generale** → **Setări rețea**.

4. În secțiunea **Porturi monitorizate**, selectați **Monitorizează numai porturile de rețea selectate**.

5. Fă clic pe **Setări**.

   Se deschide fereastra **Porturi de rețea**. Fereastra **Porturi de rețea** afișează o listă de porturi de rețea care, în mod normal, sunt utilizate pentru transmiterea e-mailurilor și a traficului de rețea. Această listă de porturi de rețea este inclusă în pachetul Kaspersky Endpoint Security.

6. Pentru a exporta lista de porturi de rețea:

   a. În lista de porturi de rețea, selectați porturile pe care doriți să le exportați. Pentru a selecta mai multe porturi, utilizați tastele **CTRL** sau **SHIFT**.

      Dacă nu ați selectat niciun port, Kaspersky Endpoint Security va exporta toate porturile.

   b. Fă clic pe **Exportă**.

   c. În fereastra care se deschide, introdu numele fișierului XML în care dorești să exporți lista cu porturile de rețea și selectează directorul în care dorești să salvezi acest fișier.

   d. Salvați fișierul.

      Kaspersky Endpoint Security exportă întreaga listă de porturi de rețea în fișierul XML.

7. Pentru a exporta lista aplicațiilor ale căror porturi sunt monitorizate de Kaspersky Endpoint Security:

   a. Bifați caseta de selectare **Monitorizare toate porturile pentru aplicații specificate**.

   b. În lista de aplicații, selectați aplicațiile pe care doriți să le exportați. Pentru a selecta mai multe porturi, utilizați tastele **CTRL** sau **SHIFT**.

      Dacă nu ați selectat nicio aplicație, Kaspersky Endpoint Security va exporta toate aplicațiile.

   c. Fă clic pe **Exportă**.

   d. În fereastra care se deschide, specificați numele fișierului XML în care doriți să exporți lista de aplicații și selectați directorul în care doriți să salvați acest fișier.

   e. Salvați fișierul.

      Kaspersky Endpoint Security exportă întreaga listă de aplicații în fișierul XML.

8. Pentru a importa lista de porturi de rețea:

   a. În lista de porturi de rețea, faceți clic pe butonul din **Importă**.

      În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de porturi de rețea.

   b. Deschideți fișierul.

      În cazul în care computerul are deja o listă de porturi de rețea, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul XML.

9. Pentru a importa o listă a aplicațiilor ale căror porturi sunt monitorizate de Kaspersky Endpoint Security:

   a. În lista de aplicații, faceți clic pe butonul **Importă**.

      În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de aplicații.

   b. Deschideți fișierul.

      În cazul în care computerul are deja o listă de aplicații, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul XML.

10. Salvați-vă modificările.

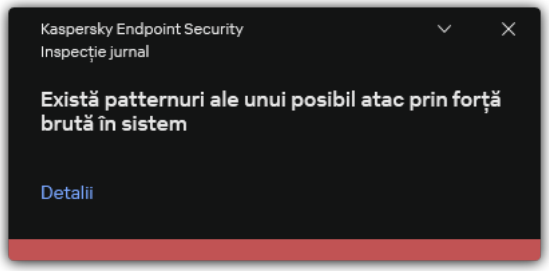
Inspecție jurnal

Această componentă este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Windows pentru servere. Această componentă este indisponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Windows pentru stații de lucru.

Începând cu versiunea 11.11.0, Kaspersky Endpoint Security for Windows include componenta Inspecție jurnal. Componenta Inspecție jurnal monitorizează integritatea mediului protejat pe baza analizei jurnalului de evenimente Windows. Când aplicația detectează semne de comportament atipic în sistem, informează administratorul, deoarece acest comportament poate indica o tentativă de atac cibernetic.

Kaspersky Endpoint Security analizează jurnalele de evenimente Windows și detectează încălcările în conformitate cu regulile. Componenta include reguli predefinite. Regulile predefinite sunt susținute de analiza euristică. Poți, de asemenea, să adăugi propriile reguli (reguli personalizate). Când se declanșează o regulă, aplicația creează un eveniment cu starea *Critical* (vezi figura de mai jos).

Dacă dorești să utilizezi componenta Inspecție jurnal, asigură-te că setările de securitate ale politicii de audit sunt configurate și că sistemul înregistrează în jurnal evenimentele relevante (pentru detalii, consultă site-ul web pentru suport tehnic Microsoft.).



Notificare Inspecție jurnal

Configurarea regulilor predefinite

Regulile predefinite includ șabloane de activitate anormală pe computerul protejat. Activitatea anormală poate semnifica o tentativă de atac. Regulile predefinite sunt susținute de analiza euristică. Sunt disponibile șapte reguli predefinite pentru Inspecție jurnal. Poți să activezi sau să dezactivezi oricare dintre aceste reguli. Regulile predefinite nu pot fi șterse.

Puteți configura criteriile de declanșare pentru regulile care monitorizează evenimentele pentru următoarele operațiuni:

- Detectare prin forță brută a parolei
- Detectare conectare la rețea

Cum să configurați regulile predefinite în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Security Controls → Inspecție jurnal**.
4. Asigurați-vă că este selectată caseta de validare **Inspecție jurnal**.
5. În blocul **Reguli predefinite**, fă clic pe butonul **Setări**.
6. Bifați sau debifați casetele de selectare pentru a configura regulile predefinite:
   - **Există patternuri ale unui posibil atac prin forță brută în sistem**.
   - **A fost detectată o activitate atipică în timpul unei sesiuni de conectare la rețea**.
   - **Există patternuri ale unui posibil abuz asupra Jurnalului de evenimente Windows**.
   - **Au fost detectate acțiuni atipice în numele unui nou serviciu instalat**.
   - **A fost detectată o conectare atipică care folosește acreditări explicite**.
   - **Există patternuri ale unui posibil atac fals al PAC-ului Kerberos (MS14-068) în sistem**.
   - **Au fost detectate modificări suspecte în grupul privilegiat încorporat Administratori**.
7. Dacă este necesar, configurați regula **Există patternuri ale unui posibil atac prin forță brută în sistem**:
   a. Faceți clic pe butonul **Setări** de sub regulă.
   b. În fereastra care se deschide, specificați numărul de încercări și o perioadă de timp în care trebuie efectuate încercările de introducere a unei parole pentru ca regula să se declanșeze.
   c. Fă clic pe **OK**.
8. Dacă selectezi regula **A fost detectată o activitate atipică în timpul unei sesiuni de conectare la rețea**, trebuie să configurezi setările acesteia:
   a. Faceți clic pe butonul **Setări** de sub regulă.
   b. În blocul **Detectare conectare la rețea**, specificați începutul și sfârșitul intervalului de timp.

      Kaspersky Endpoint Security consideră încercările de conectare efectuate în intervalul definit drept activitate anormală.

      În mod implicit, intervalul nu este setat și aplicația nu monitorizează încercările de conectare. Pentru ca aplicația să monitorizeze continuu încercările de conectare, setați intervalul la 00:00 – 23:59. Începutul și sfârșitul intervalului nu trebuie să coincidă. Dacă acestea coincid, aplicația nu monitorizează încercările de conectare.

c. Creați lista de utilizatori de încredere și adrese IP de încredere (IPv4 și IPv6).

Poți selecta utilizatori în Active Directory, în lista de conturi din Kaspersky Security Center sau introducând manual un nume de utilizator local. Kaspersky recomandă utilizarea conturilor de utilizator locale numai în cazuri speciale, când nu este posibilă utilizarea conturilor de utilizator de domeniu. Kaspersky Endpoint Security nu monitorizează încercările de conectare pentru acești utilizatori și aceste computere.

d. Fă clic pe **OK**.

9. Salvați-vă modificările.

Cum se configurează regulile predefinite în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Security Controls** → **Log Inspection**.
5. Asigurați-vă că butonul de comutare **Log Inspection ENABLED** este activat.
6. În blocul **Predefined rules**, activați sau dezactivați regulile predefinite folosind comutatoarele:

   - **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. Dacă este necesar, configurați regula **There are patterns of a possible brute-force attack in the system**:

   a. Fă clic pe **Settings** sub regula.

   b. În fereastra care se deschide, specificați numărul de încercări și o perioadă de timp în care trebuie efectuate încercările de introducere a unei parole pentru ca regula să se declanșeze.

   c. Fă clic pe **OK**.
8. Dacă selectezi regula **There is an atypical activity detected during a network logon session**, trebuie să configurezi setările acesteia:

   a. Fă clic pe **Settings** sub regula.

   b. În blocul **Network logon detection**, specificați începutul și sfârșitul intervalului de timp.

Kaspersky Endpoint Security consideră încercările de conectare efectuate în intervalul definit drept activitate anormală.

În mod implicit, intervalul nu este setat și aplicația nu monitorizează încercările de conectare. Pentru ca aplicația să monitorizeze continuu încercările de conectare, setați intervalul la 00:00 – 23:59. Începutul și sfârșitul intervalului nu trebuie să coincidă. Dacă acestea coincid, aplicația nu monitorizează încercările de conectare.

c. În blocul **Exclusions**, adaugă utilizatori de încredere și adrese IP de încredere (IPv4 și IPv6).

Poți selecta utilizatori în Active Directory, în lista de conturi din Kaspersky Security Center sau introducând manual un nume de utilizator local. Kaspersky recomandă utilizarea conturilor de utilizator locale numai în cazuri speciale, când nu este posibilă utilizarea conturilor de utilizator de domeniu. Kaspersky Endpoint Security nu monitorizează încercările de conectare pentru acești utilizatori și aceste computere.

d. Fă clic pe **OK**.

9. Salvați-vă modificările.

Cum se configurează regulile predefinite în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Security Controls** → **Inspecție jurnal**.
3. Asigurați-vă că butonul de comutare **Inspecție jurnal** este activat.
4. În blocul **Reguli predefinite**, fă clic pe butonul **Configurare**.
5. Bifați sau debifați casetele de selectare pentru a configura regulile predefinite:
   - **Există patternuri ale unui posibil atac prin forță brută în sistem**.
   - **A fost detectată o activitate atipică în timpul unei sesiuni de conectare la rețea**.
   - **Există patternuri ale unui posibil abuz asupra Jurnalului de evenimente Windows**.
   - **Au fost detectate acțiuni atipice în numele unui nou serviciu instalat**.
   - **A fost detectată o conectare atipică care folosește acreditări explicite**.
   - **Există patternuri ale unui posibil atac fals al PAC-ului Kerberos (MS14-068) în sistem**.

   a. **Au fost detectate modificări suspecte în grupul privilegiat încorporat Administratori**.
6. Dacă este necesar, configurați regula **Există patternuri ale unui posibil atac prin forță brută în sistem**:

   a. Fă clic pe **Setări** sub regula.

   b. În fereastra care se deschide, specificați numărul de încercări și o perioadă de timp în care trebuie efectuate încercările de introducere a unei parole pentru ca regula să se declanșeze.

7. Dacă selectezi regula **A fost detectată o activitate atipică în timpul unei sesiuni de conectare la rețea**, trebuie să configurezi setările acesteia:

   a. Fă clic pe **Setări** sub regula.

   b. În blocul **Detectarea conectării la rețea**, specificați începutul și sfârșitul intervalului de timp.

      Kaspersky Endpoint Security consideră încercările de conectare efectuate în intervalul definit drept activitate anormală.

      În mod implicit, intervalul nu este setat și aplicația nu monitorizează încercările de conectare. Pentru ca aplicația să monitorizeze continuu încercările de conectare, setați intervalul la 00:00 – 23:59. Începutul și sfârșitul intervalului nu trebuie să coincidă. Dacă acestea coincid, aplicația nu monitorizează încercările de conectare.

   c. În blocul **Excluderi**, adaugă utilizatori de încredere și adrese IP de încredere (IPv4 și IPv6).

      Poți selecta utilizatori în Active Directory, în lista de conturi din Kaspersky Security Center sau introducând manual un nume de utilizator local. Kaspersky recomandă utilizarea conturilor de utilizator locale numai în cazuri speciale, când nu este posibilă utilizarea conturilor de utilizator de domeniu. Kaspersky Endpoint Security nu monitorizează încercările de conectare pentru acești utilizatori și aceste computere.

8. Salvați-vă modificările.

Ca rezultat, atunci când regula se declanșează, Kaspersky Endpoint Security creează un *Eveniment critic*.

Adăugarea de reguli personalizate

Puteți seta propriile criterii de declanșare a regulii Inspecție jurnal. Pentru a face acest lucru, trebuie să introduceți un ID de eveniment și să selectați o sursă a evenimentului. Puteți căuta ID-ul evenimentului pe site-ul web de suport tehnic Microsoft. Puteți selecta o sursă a evenimentului dintre jurnalele standard: *Application*, *Security* sau *System*. De asemenea, puteți specifica jurnalul unei aplicații terțe. Puteți afla numele jurnalului aplicației terțe folosind instrumentul Vizualizare evenimente. Jurnalele de aplicații terțe sunt păstrate în directorul Jurnale de aplicații și servicii (de exemplu, jurnalul *Windows PowerShell*).

Aplicația nu verifică dacă jurnalul specificat este de fapt prezent în jurnalul de evenimente Windows. Dacă există o greșeală în numele jurnalului, aplicația nu monitorizează evenimentele din acel jurnal.

Lista de reguli personalizate include deja trei reguli create de experții Kaspersky.

Cum se adăugă o regulă personalizată în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Security Controls → Inspecție jurnal**.
4. Asigurați-vă că este selectată caseta de validare **Inspecție jurnal**.
5. În blocul **Reguli personalizate**, fă clic pe butonul **Setări**.
6. În fereastra care se deschide, bifați casetele de selectare de lângă regulile personalizate pe care doriți să le activați.

7. Dacă este necesar, faceți clic pe **Adaugă** pentru a vă crea propriile reguli personalizate.

8. Aceasta deschide o fereastră; în acea fereastră, configurați regula personalizată:

   - **Nume regulă**.
   - **Nume jurnal**. Jurnalele de evenimente Windows. Sunt disponibile următoarele jurnale: *Application*, *Security*, *System*.
   - **Sursă**. Jurnalele aplicațiilor terțe. Puteți afla numele jurnalului aplicației terțe folosind instrumentul Vizualizare evenimente. Jurnalele de aplicații terțe sunt păstrate în directorul Jurnale de aplicații și servicii (de exemplu, jurnalul *Windows PowerShell*).
   - **Identificatori evenimente**. ID-urile evenimentelor în Jurnalul de evenimente Windows. Puteți căuta ID-ul evenimentului în documentația tehnică Microsoft.

9. Salvați-vă modificările.

Cum se adaugă o regulă personalizată în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Security Controls** → **Log Inspection**.
5. Asigurați-vă că butonul de comutare **Log Inspection ENABLED** este activat.
6. În blocul **Custom rules**, selectați regulile personalizate pe care doriți să le activați.
7. Dacă este necesar, faceți clic pe **Add** pentru a vă crea propriile reguli personalizate.
8. Aceasta deschide o fereastră; în acea fereastră, configurați regula personalizată:

   - **Rule name**.
   - **Custom log name**. Jurnalele de evenimente Windows. Sunt disponibile următoarele jurnale: *Application*, *Security*, *System*.
   - **Origin**. Jurnalele aplicațiilor terțe. Puteți afla numele jurnalului aplicației terțe folosind instrumentul Vizualizare evenimente. Jurnalele de aplicații terțe sunt păstrate în directorul Jurnale de aplicații și servicii (de exemplu, jurnalul *Windows PowerShell*).
   - **Event Identifiers**. ID-urile evenimentelor în Jurnalul de evenimente Windows. Puteți căuta ID-ul evenimentului în documentația tehnică Microsoft.

9. Salvați-vă modificările.

Cum se adaugă o regulă personalizată în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Security Controls** → **Inspecție jurnal**.

3. Asigurați-vă că butonul de comutare **Inspecție jurnal** este activat.

4. În blocul **Reguli personalizate**, fă clic pe butonul **Configurare**.

5. În fereastra care se deschide, bifați casetele de selectare de lângă regulile personalizate pe care doriți să le activați.

6. Dacă este necesar, faceți clic pe **Adaugă** pentru a vă crea propriile reguli personalizate.

7. Aceasta deschide o fereastră; în acea fereastră, configurați regula personalizată:

   - **Nume regulă**.
   - **Nume jurnal**. Jurnalele de evenimente Windows. Sunt disponibile următoarele jurnale: *Application*, *Security*, *System*.
   - **Sursă**. Jurnalele aplicațiilor terțe. Puteți afla numele jurnalului aplicației terțe folosind instrumentul Vizualizare evenimente. Jurnalele de aplicații terțe sunt păstrate în directorul Jurnale de aplicații și servicii (de exemplu, jurnalul *Windows PowerShell*).
   - **Identificator eveniment**. ID-urile evenimentelor în Jurnalul de evenimente Windows. Puteți căuta ID-ul evenimentului în documentația tehnică Microsoft.

8. Salvați-vă modificările.

Ca rezultat, atunci când regula se declanșează, Kaspersky Endpoint Security creează un eveniment *Critical*.

Monitorizare integritate sistem

Această componentă este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Windows pentru servere. Această componentă este indisponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Windows pentru stații de lucru.

Începând cu versiunea 12.6 Kaspersky Endpoint Security or Windows include componenta Monitorizare integritate sistem în loc de componenta File Integrity Monitor. Componenta Monitorizare integritate sistem include toate funcționalitățile File Integrity Monitor și, în plus, permite monitorizarea modificărilor registry-ului și conectarea dispozitivelor externe.

Componenta Monitorizare integritate sistem monitorizează modificările din sistemul de operare care pot indica încălcări ale securității computerului. Când sunt detectate astfel de modificări, Kaspersky Endpoint Security generează evenimente corespunzătoare și alertează administratorul. Componenta Monitorizare integritate sistem poate funcționa în modul în timp real și poate efectua, de asemenea, verificări ale integrității sistemului la cerere.

Monitorizare în timp real a integrității sistemului

În modul în timp real, componenta Monitorizare integritate sistem urmărește modificările obiectelor pe care le-ai inclus în fișierul componentei (*domeniul de monitorizare*). Componenta Monitorizare integritate sistem permite, de asemenea, blocarea în timp real a accesului neautorizat la astfel de obiecte.

Componenta Verificare integritate sistem la cerere

Verificare integritate sistem la cerere este o activitate pe care o puteți executa manual sau conform unui program. Pentru a executa activitatea *Verificare integritate sistem*, trebuie să configurați domeniul de aplicare al componentei (*domeniul de monitorizare*) și creați o linie de bază. O *linie de bază* este o stare înregistrată a obiectelor din sistem, pe care aplicația o folosește ca referință atunci când o compară cu starea curentă.

Migrarea setărilor componentei File Integrity Monitor

Când actualizați Kaspersky Endpoint Security la versiunea 12.6, setările componentei File Integrity Monitor sunt migrate automat. Ca parte a migrării, aplicația mută regulile de monitorizare în Monitorizare integritate sistem. Regulile componentei File Integrity Monitor sunt, de asemenea, migrate la componenta Monitorizare integritate sistem atunci când are loc migrarea de la KSWS la KES.

Pentru a asigura funcționarea corectă a componentei Monitorizare integritate sistem, aplicația Kaspersky Endpoint Security și plug-in-ul de gestionare trebuie actualizate la versiunea 12.6. Dacă ai instalată o versiune anterioară a plug-in-ului de gestionare, nu poți configura componenta Monitorizare integritate sistem, deoarece plug-in-ul de gestionare nu conține secțiunea **Monitorizare integritate sistem**.

Despre regulile Monitorizare integritate sistem

Pentru ca soluția Monitorizare integritate sistem să funcționeze, trebuie să adaugi cel puțin o regulă. O *regula Monitorizare integritate sistem* este un set de criterii care definesc accesul utilizatorilor la fișiere și la registry. Monitorizare integritate sistem detectează modificări ale fișierelor și ale registry-ului în limitele *domeniul de monitorizare* specificate. Domeniul de monitorizare este unul dintre criteriile unei reguli Monitorizare integritate sistem.

Monitorizare integritate sistem permite monitorizarea următoarelor obiecte:

- fișiere
- registry
- dispozitive externe

considerații speciale implicate în monitorizarea fișierelor

Monitorizare integritate sistem monitorizează modificările aduse fișierelor și directoarelor, precum și fișierele care sunt adăugate la domeniul de aplicare sau eliminate din acesta. Aceste modificări pot indica o încălcare a securității computerului. Vă recomandăm să adăugați obiecte rar modificate sau obiecte la care doar administratorul are acces. Acest lucru va reduce numărul de evenimente Monitorizare integritate sistem.

> Componenta Monitorizare integritate sistem nu monitorizează modificările aduse fișierelor din directoarele partajate ale serverului. Componenta Monitorizare integritate sistem poate fi utilizată numai local.

Kaspersky Endpoint Security monitorizează modificările fișierelor și directoarelor numai de pe acele discuri care au fost conectate când a început să funcționeze componenta Monitorizare în timp real a integrității sistemului. Dacă un disc nu a fost conectat când a început să funcționeze componenta Monitorizare în timp real a integrității sistemului, aplicația nu monitorizează modificările fișierelor și directoarelor de pe acel disc, chiar dacă fișierele și directoarele sunt adăugate la domeniul de monitorizare.

Considerații speciale implicate în monitorizarea registry-ului

Monitorizare integritate sistem monitorizează registry-ul. Aceste modificări pot indica o încălcare a securității computerului.

Monitorizare integritate sistem monitorizează următoarele chei rădăcină ale registry-ului:

- `HKCR`
- `HKLM`
- `HKU`
- `HKCC`

- HKEY_CLASSES_ROOT
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG (disponibil numai în Monitorizare în timp real a integrității sistemului)
- HKEY_CURRENT_USER (disponibil numai în Monitorizare în timp real a integrității sistemului)

> Activitatea *Verificare integritate sistem* nu acceptă cheia HKEY_CURRENT_USER. Puteți specifica o cheie din HKEY_USERS drept HKEY_USERS\<user profile ID>\<key>.

Considerații speciale implicate în monitorizarea dispozitivului extern

Monitorizare integritate sistem monitorizează conectarea și deconectarea dispozitivelor externe. Acest lucru este necesar pentru a proteja computerul de amenințările la adresa securității care pot rezulta din schimbul de fișiere cu astfel de dispozitive. Monitorizare integritate sistem nu monitorizează accesul la dispozitivele externe și nu blochează schimbul de fișiere. Puteți configura accesul la dispozitive folosind o altă componentă a aplicației, Control dispozitive.

> Când se execută activitatea *Monitorizare a integrității sistemului de referință*, aplicația ignoră reconectarea dispozitivelor externe dacă dispozitivele au aceeași literă de unitate în sistemul de operare. Pentru a fi înregistrate, dispozitivele reconectate trebuie să aibă litere de unitate diferite.

Monitorizare integritate sistem monitorizează conectarea următoarelor tipuri de dispozitive externe:

- Unitate amovibilă (inclusiv unități flash USB)
- Unitate de hard disk
- Placă de rețea externă
- Unitate CD/DVD/Blu-ray
- Scaner / cameră foto

Monitorizare în timp real a integrității sistemului

Componenta Monitorizare integritate sistem permite urmărirea în timp real a modificărilor din sistemul de operare. Puteți urmări modificările care pot indica încălcări de securitate pe computer. Componenta permite blocarea acestor modificări sau pur și simplu înregistrarea evenimentelor de modificare.

Pentru ca Monitorizare integritate sistem să funcționeze, trebuie să adăugați cel puțin o regulă. O *regula Monitorizare integritate sistem* este un set de criterii care definesc accesul utilizatorilor la fișiere și la registry. Monitorizare integritate sistem detectează modificări ale fișierelor și ale registry-ului în limitele *domeniul de monitorizare* specificate. Domeniul de monitorizare este unul dintre criteriile unei reguli Monitorizare integritate sistem.

Moduri Monitorizare în timp real a integrității sistemului

Pentru a vă asigura că regulile Monitorizare integritate sistem nu blochează nicio acțiune cu resurse care sunt critice pentru funcționarea sistemului de operare sau a altor servicii, vă recomandăm să activați modul Testare și să analizați modul în care componenta afectează sistemul. Cu modul Testare activat, Kaspersky Endpoint Security nu blochează activitatea utilizatorului care este interzisă de reguli, ci generează evenimente de tip *Avertisment* ⚠.

Componenta Monitorizarea în timp real a integrității sistemului are două moduri:

- Blochează

  În acest mod, Monitorizare integritate sistem urmărește modificările din sistem și efectuează o acțiune în conformitate cu regulile: **Permite** sau **Blochează**. Monitorizare integritate sistem generează, de asemenea, un eveniment corespunzător și modifică starea dispozitivului în consola Kaspersky Security Center.

- Informează

  În acest mod, Monitorizare integritate sistem permite acțiuni cu fișiere și chei de registry din domeniul de monitorizare. Dacă acțiunea cu fișiere sau cu registry-ul este interzisă, aplicația generează un eveniment: *Operațiunea interzisă a fost permisă în modul de testare*. Pentru a analiza modul în care regulile afectează sistemul, puteți consulta rapoartele.

Activarea componentei Monitorizare în timp real a integrității sistemului

Cum să activați Monitorizare în timp real a integrității sistemului în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Security Controls** → **Monitorizare integritate sistem**.
4. Bifați caseta de selectare **Monitorizare integritate sistem**.
5. În **Modul de funcționare pentru regulile de blocare**, selectați un mod pentru Monitorizare în timp real a integrității sistemului:
   - **Blochează**. În acest mod, Monitorizare integritate sistem blochează acțiuni cu fișiere și chei de registry din domeniul de monitorizare și generează un eveniment corespunzător.
   - **Informează**. În acest mod, Monitorizare integritate sistem permite acțiuni cu fișiere și chei de registry din domeniul de monitorizare și generează un eveniment corespunzător.
6. În blocul **Monitorizare în timp real a integrității sistemului**, bifați caseta de selectare **Monitorizare în timp real a integrității sistemului**.
7. Configurați monitorizarea dispozitivului extern:
   a. Bifați caseta de selectare **Monitorizează dispozitivele**.
   b. În lista verticală **Nivel severitate eveniment**, selectați nivelul de importanță al evenimentelor de monitorizare a dispozitivului extern: *Informațional* ⓘ, *Avertisment* ⚠, *Critic* ⓘ.

Monitorizare integritate sistem înregistrează conexiunea curentă a dispozitivelor externe. Aplicația începe să monitorizeze conectarea și deconectarea dispozitivelor externe după ce componenta este activată în setările aplicației. Ulterior, atunci când un dispozitiv extern este conectat sau deconectat, aplicația generează un eveniment corespunzător.

8. Configurați monitorizarea fișierelor și a registry-ului:

   a. Bifați caseta de selectare **Monitorizează fișierele și registry-ul**.

   b. Fă clic pe **Setări**.

      Astfel, se deschide lista de reguli Monitorizare integritate sistem.

   c. Fă clic pe **Adaugă**.

      Puteți, de asemenea, să importați reguli dintr-o altă sursă.

   d. Configurează regula Monitorizare integritate sistem (consultă tabelul de mai jos).

9. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum să activați Monitorizare în timp real a integrității sistemului în Web Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **Security Controls** → **System Integrity Monitoring**.

5. Duceți comutatorul **System Integrity Monitoring ENABLED** la poziția activat.

6. Selectați fila **Windows**.

7. În **Real-Time System Integrity Monitoring**, selectați un mod pentru Monitorizare în timp real a integrității sistemului:

   - **Apply rules**. În acest mod, Monitorizare integritate sistem blochează acțiuni cu fișiere și chei de registry din domeniul de monitorizare și generează un eveniment corespunzător.

   - **Test rules (Inform)**. În acest mod, Monitorizare integritate sistem permite acțiuni cu fișiere și chei de registry din domeniul de monitorizare și generează un eveniment corespunzător.

8. Configurați monitorizarea fișierelor și a registry-ului:

   a. Bifați caseta de selectare **Monitor files and the registry**.

   b. Fă clic pe **Rules**.

      Astfel, se deschide lista de reguli Monitorizare integritate sistem.

   c. Fă clic pe **Add**.

      Puteți, de asemenea, să importați reguli dintr-o altă sursă.

   d. Configurează regula Monitorizare integritate sistem (consultă tabelul de mai jos).

9. Configurați monitorizarea dispozitivului extern:

    a. Bifați caseta de selectare **Monitor devices**.

    b. În lista verticală **Event severity level**, selectați nivelul de importanță al evenimentelor de monitorizare a dispozitivului extern: *Informational* ⓘ, *Warning* ⚠, *Critical* ⓘ.

    Monitorizare integritate sistem înregistrează conexiunea curentă a dispozitivelor externe. Aplicația începe să monitorizeze conectarea și deconectarea dispozitivelor externe după ce componenta este activată în setările aplicației. Ulterior, atunci când un dispozitiv extern este conectat sau deconectat, aplicația generează un eveniment corespunzător.

10. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum să activați Monitorizare în timp real a integrității sistemului în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Security Controls** → **Monitorizare integritate sistem**.

3. Porniți comutatorul **Monitorizare integritate sistem**.

4. În **Modul de funcționare pentru regulile de blocare**, selectați un mod pentru Monitorizare în timp real a integrității sistemului:

    - **Blochează**. În acest mod, Monitorizare integritate sistem blochează acțiuni cu fișiere și chei de registry din domeniul de monitorizare și generează un eveniment corespunzător.

    - **Informează**. În acest mod, Monitorizare integritate sistem permite acțiuni cu fișiere și chei de registry din domeniul de monitorizare și generează un eveniment corespunzător.

5. În blocul **Monitorizare în timp real a integrității sistemului**, bifați caseta de selectare **Monitorizare în timp real a integrității sistemului**.

6. Configurați monitorizarea dispozitivului extern:

    a. Bifați caseta de selectare **Monitorizează dispozitivele**.

    b. În lista verticală **Nivel severitate eveniment**, selectați nivelul de importanță al evenimentelor de monitorizare a dispozitivului extern: *Informațional* ⓘ, *Avertisment* ⚠, *Critic* ⓘ.

    Monitorizare integritate sistem înregistrează conexiunea curentă a dispozitivelor externe. Aplicația începe să monitorizeze conectarea și deconectarea dispozitivelor externe după ce componenta este activată în setările aplicației. Ulterior, atunci când un dispozitiv extern este conectat sau deconectat, aplicația generează un eveniment corespunzător.

7. Configurați monitorizarea fișierelor și a registry-ului:

    a. Bifați caseta de selectare **Monitorizează fișierele și registry-ul**.

    b. Fă clic pe **Configurează**.

    Astfel, se deschide lista de reguli Monitorizare integritate sistem.

    c. Fă clic pe **Adaugă**.

    Puteți, de asemenea, să importați reguli dintr-o altă sursă.

8. Configurează regula Monitorizare integritate sistem (consultă tabelul de mai jos).

9. Salvați-vă modificările.

Setări reguli Monitorizare în timp real a integrității sistemului

Parametru	Descriere
Nume regulă	Numele regulii Monitorizare în timp real a integrității sistemului:
Operațiuni cu fișiere și registry	• **Permite**. Monitorizare integritate sistem permite acțiuni cu fișiere și chei de registry din domeniul de monitorizare. • **Blochează**. Comportamentul componentei Monitorizare integritate sistem depinde de modul selectat. Dacă ați selectat *modul Protecție sistem*, Componenta Monitorizare integritate sistem blochează acțiunile cu fișiere și chei de registry din domeniul de monitorizare, generează un eveniment corespunzător și modifică starea dispozitivului în consola Kaspersky Security Center. Dacă ați selectat *modul Testare*, Monitorizare integritate sistem permite acțiuni cu fișiere și chei de registry din domeniul de monitorizare.
Nivel severitate eveniment	Kaspersky Endpoint Security înregistrează în jurnal evenimentele de modificare a fișierelor ori de câte ori este modificat un fișier din domeniul de monitorizare. Sunt disponibile următoarele niveluri de severitate: *Informațional*, *Avertisment*, *Critic*.

Domeniu monitorizare	• **Fișier**. Lista fișierelor și directoarelor monitorizate de componentă. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști.
	Folosiți măști:
	  • Caracterul `*` (asterisc) ține locul oricărui set de caractere, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\*\*.txt` va include toate căile către fișierele cu extensia TXT din directoarele de pe unitatea C:, dar nu și din subdirectoare.
	  • Două caractere `*` consecutive țin locul oricărui set de caractere (inclusiv un set gol) din numele de fișier sau director, inclusiv caracterele `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\**\*.txt` va include toate căile către fișierele cu extensia TXT localizată în directoarele imbricate în `Folder`, cu excepția `Folder` în sine. Masca trebuie să includă cel puțin un nivel de imbricare. Masca `C:\**\*.txt` nu este o mască validă.
	  • `?` (semn de întrebare) ține locul oricărui caracter individual, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\???.txt` va include căi pentru toate fișierele din directorul denumit `Folder` care au extensia TXT și un nume format din trei caractere.
	• **Registry**. Lista cheilor și valorilor de registry monitorizate de componentă. Kaspersky Endpoint Security acceptă caracterele `*` și `?` la introducerea unei măști.

Excluderi	• **Fișier**. Lista excluderilor din domeniul de monitorizare. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști. De exemplu, `C:\Folder\Application\*.log`. Intrările de excludere au o prioritate mai mare decât intrările din domeniul de monitorizare.
	Folosiți măști:
	  • Caracterul `*` (asterisc) ține locul oricărui set de caractere, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\*\*.txt` va include toate căile către fișierele cu extensia TXT din directoarele de pe unitatea C:, dar nu și din subdirectoare.
	  • Două caractere `*` consecutive țin locul oricărui set de caractere (inclusiv un set gol) din numele de fișier sau director, inclusiv caracterele `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\**\*.txt` va include toate căile către fișierele cu extensia TXT localizată în directoarele imbricate în `Folder`, cu excepția `Folder` în sine. Masca trebuie să includă cel puțin un nivel de imbricare. Masca `C:\**\*.txt` nu este o mască validă.
	  • `?` (semn de întrebare) ține locul oricărui caracter individual, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\???.txt` va include căi pentru toate fișierele din directorul denumit `Folder` care au extensia TXT și un nume format din trei caractere.
	• **Registry**. Lista excluderilor din domeniul de monitorizare. Kaspersky Endpoint Security acceptă caracterele `*` și `?` la introducerea unei măști. Intrările de excludere au o prioritate mai mare decât intrările din domeniul de monitorizare.

Utilizatori și/sau grupuri de utilizatori de încredere	Un *utilizator de încredere* este un utilizator căruia îi este permis să efectueze acțiuni cu fișiere și chei de registry în domeniul de monitorizare. Dacă Kaspersky Endpoint Security detectează o acțiune efectuată de un utilizator de încredere, componenta Monitorizare integritate sistem generează un eveniment *Informațional*. Poți selecta utilizatori în Active Directory, în lista de conturi din Kaspersky Security Center sau introducând manual un nume de utilizator local. Kaspersky recomandă utilizarea conturilor de utilizator locale numai în cazuri speciale, când nu este posibilă utilizarea conturilor de utilizator de domeniu.

Parametru	Descriere
Markeri operațiune cu fișiere / Operațiuni monitorizate	Markeri care caracterizează acțiunea cu fișiere sau chei de registry pe care aplicația le va monitoriza.
Hashing	Calcularea unui hash de fișier în momentul modificării. Kaspersky Endpoint Security adaugă informații despre hash-ul fișierului atunci când este generat un eveniment.

Componenta Verificare integritate sistem la cerere

Verificare integritate sistem la cerere este o activitate pe care o puteți executa manual sau conform unui program. Când executați activitatea *Verificare integritate sistem*, aplicația compară starea curentă a obiectelor incluse în domeniul de monitorizare cu starea *liniei lor de bază*. Spre deosebire de Monitorizare în timp real a integrității sistemului, activitatea *Verificare integritate sistem* ajută la limitarea numărului de evenimente și vă permite să generați un raport general al modificărilor din sistemul de operare.

Pentru ca Monitorizare integritate sistem să funcționeze, trebuie să adăugați cel puțin o regulă. O *regula Monitorizare integritate sistem* este un set de criterii care definesc accesul utilizatorilor la fișiere și la registry. Monitorizare integritate sistem detectează modificări ale fișierelor și ale registry-ului în limitele *domeniul de monitorizare* specificate. Domeniul de monitorizare este unul dintre criteriile unei reguli Monitorizare integritate sistem. Puteți configura reguli pentru a fi partajate de Monitorizare în timp real a integrității sistemului și activitatea *Verificare integritate sistem* sau să creați reguli separate pentru activitate. Pentru a crea o linie de bază, Kaspersky Endpoint Security aplică domeniul de monitorizare din activitatea *Verificare integritate sistem* activității *Actualizarea liniei de bază*.

Crearea și actualizarea unei linii de bază

Activitatea *Verificare integritate sistem* are nevoie de o linie de bază pentru a funcționa. O *linie de bază* este o stare înregistrată a obiectelor din sistem, pe care aplicația o folosește ca referință atunci când o compară cu starea curentă. Dacă starea curentă a sistemului este diferită de starea sistemului înregistrată în linia de bază, Kaspersky Endpoint Security generează evenimentul corespunzător. Puteți crea sau actualiza o linie de bază folosind activitatea *Actualizarea liniei de bază*.

Puteți actualiza linia de bază în următoarele moduri:

- Actualizare completă.

  Aplicația actualizează toate obiectele din domeniul de monitorizare.

- Actualizare incrementală.

  Aplicația detectează și actualizează doar obiectele modificate sau noi.

Cum se creează sau se actualizează o politică în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **New task**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Selectarea tipului activității

Selectați **Kaspersky Endpoint Security for Windows (14.1)** → **Actualizarea liniei de bază**.

Pasul 2. Selectarea modului de actualizare a liniei de bază

Selectați modul de actualizare a liniei de bază:

- **Actualizare completă**. Aplicația actualizează toate obiectele din domeniul de monitorizare.
- **Actualizare incrementală**. Aplicația detectează și actualizează doar obiectele modificate sau noi.

Pasul 3. Selectarea dispozitivelor cărora le va fi atribuită activitatea

Selectați computerele pe care se va efectua activitatea. Sunt disponibile următoarele opțiuni:

- Atribuirea activității unui grup de administrare. În acest caz, activitatea este atribuită computerelor incluse într-un grup de administrare creat anterior.
- Selectare computere detectate în rețea de Serverul de administrare: *dispozitive neatribuite*. Dispozitivele specifice pot include dispozitive din grupuri de administrare, precum și dispozitive neatribuite.
- Specificarea manuală a adreselor computerelor sau importarea adreselor dintr-o listă. Poți specifica nume NetBIOS, adrese IP și subrețele IP ale dispozitivelor cărora dorești să le atribui activitatea.

Pasul 4. Definirea numelui activității

Introduceți numele activității, de exemplu *Linie de bază 2024*.

Pasul 5. Finalizarea creării activității

Ieșiți din Expert. Dacă este necesar, bifați caseta de selectare **Run the task after the wizard finishes**. Puteți monitoriza progresul activității în proprietățile activității.

Cum se creează sau se actualizează o linie de bază în Web Console

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **Add**.

   Expertul de activitate pornește.

3. Configurați setările pentru activitate:

   a. În lista verticală **Application**, selectează **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. În lista verticală **Task type**, selectează **Baseline update**.

   c. În câmpul **Task name**, introdu o descriere succintă, de exemplu *Linie de bază 2024*.

   d. În blocul **Devices to which the task will be assigned**, selectați domeniul activității.

4. Selectați dispozitive în funcție de opțiunea selectată pentru domeniul activității. Mergeți la pasul următor.

5. Selectează un cont pentru a executa activitatea. În mod implicit, Kaspersky Endpoint Security începe activitatea cu drepturile unui cont de utilizator local.

6. Ieșiți din Expert.

   Se va afișa o activitate nouă în lista de activități.

7. Faceți clic pe activitatea nouă.

   Se va deschide fereastra de proprietăți a activității.

8. Selectați fila **Application settings**.

9. Selectați modul de actualizare a liniei de bază:

   - **Full update**. Aplicația actualizează toate obiectele din domeniul de monitorizare.
   - **Incremental update**. Aplicația detectează și actualizează doar obiectele modificate sau noi.

10. Salvați-vă modificările.

11. Bifați caseta de selectare de lângă activitate.

12. Fă clic pe **Start**.

Configurarea domeniului de monitorizare pentru activitatea Verificare integritate sistem

În mod implicit, domeniul de monitorizare al activității *Verificare integritate sistem* este aceeași cu domeniul de monitorizare al componentei Monitorizare în timp real a integrității sistemului. Puteți configura un domeniu de monitorizare diferit pentru activitate.

Componenta Monitorizare integritate sistem nu acceptă importul cheilor `HKEY_CURRENT_USER` și `HKEY_CURRENT_CONFIG` pentru activitatea *Verificare integritate sistem*. Dacă domeniul de monitorizare al activității conține aceste chei, aplicația generează evenimentul *Domeniul de monitorizare include obiecte incorecte*.

Cum se configurează un alt domeniu de monitorizare pentru activitatea Verificare integritate sistem în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Security Controls** → **Monitorizare integritate sistem**.
4. Bifați caseta de selectare **Monitorizare integritate sistem**.
5. În **Verificare integritate sistem**, selectați modul de configurare a activității: **Setări personalizate**.
6. Configurați monitorizarea dispozitivului extern:
   a. Bifați caseta de selectare **Monitorizează dispozitivele**.
   b. În lista verticală **Nivel severitate eveniment**, selectați nivelul de importanță al evenimentelor de monitorizare a dispozitivului extern: *Informațional*, *Avertisment*, *Critic*.

   Monitorizare integritate sistem înregistrează informații despre dispozitivele externe conectate în momentul creării liniei de bază. Ulterior, atunci când un dispozitiv extern este conectat sau deconectat, aplicația generează un eveniment corespunzător. Când executați activitatea *Verificare integritate sistem*, aplicația nu monitorizează deconectarea dispozitivelor externe.
7. Configurați monitorizarea fișierelor și a registry-ului:
   a. Bifați caseta de selectare **Monitorizează fișierele și registry-ul**.
   b. Fă clic pe **Setări**.

      Astfel, se deschide lista de reguli Monitorizare integritate sistem.
   c. Fă clic pe **Adaugă**.

      Puteți, de asemenea, să importați reguli dintr-o altă sursă.
   d. Configurează regula Monitorizare integritate sistem (consultă tabelul de mai jos).
8. Salvați-vă modificările.

Cum se configurează un alt domeniu de monitorizare pentru activitatea System Integrity Check în Web Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Security Controls** → **System Integrity Monitoring**.
5. Selectați fila **Windows**.
6. Duceți comutatorul **System Integrity Monitoring ENABLED** la poziția activat.

7. În **System Integrity Check**, selectați modul de configurare a activității: **Custom settings**.

8. Configurați monitorizarea dispozitivului extern:

   a. Bifați caseta de selectare **Monitor devices**.

   b. În lista verticală **Event severity level**, selectați nivelul de importanță al evenimentelor de monitorizare a dispozitivului extern: *Informational* ⓘ, *Warning* ⚠, *Critical* ⓘ.

   Monitorizare integritate sistem înregistrează informații despre dispozitivele externe conectate în momentul creării liniei de bază. Ulterior, atunci când un dispozitiv extern este conectat sau deconectat, aplicația generează un eveniment corespunzător. Când executați activitatea *Verificare integritate sistem*, aplicația nu monitorizează deconectarea dispozitivelor externe.

9. Configurați monitorizarea fișierelor și a registry-ului:

   a. Bifați caseta de selectare **Monitor files and the registry**.

   b. Fă clic pe **Rules**.

      Astfel, se deschide lista de reguli Monitorizare integritate sistem.

   c. Fă clic pe **Add**.

      Puteți, de asemenea, să importați reguli dintr-o altă sursă.

   d. Configurează regula Monitorizare integritate sistem (consultă tabelul de mai jos).

10. Salvați-vă modificările.

Cum se configurează un alt domeniu de monitorizare pentru activitatea Verificare integritate sistem în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Security Controls** → **Monitorizare integritate sistem**.

3. Porniți comutatorul **Monitorizare integritate sistem**.

4. În **Verificare integritate sistem**, selectați modul de configurare a activității: **Setări personalizate**.

5. Configurați monitorizarea dispozitivului extern:

   a. Bifați caseta de selectare **Monitorizează dispozitivele**.

   b. În lista verticală **Nivel severitate eveniment**, selectați nivelul de importanță al evenimentelor de monitorizare a dispozitivului extern: *Informațional* ⓘ, *Avertisment* ⚠, *Critic* ⓘ.

   Monitorizare integritate sistem înregistrează informații despre dispozitivele externe conectate în momentul creării liniei de bază. Ulterior, atunci când un dispozitiv extern este conectat sau deconectat, aplicația generează un eveniment corespunzător. Când executați activitatea *Verificare integritate sistem*, aplicația nu monitorizează deconectarea dispozitivelor externe.

6. Configurați monitorizarea fișierelor și a registry-ului:

   a. Bifați caseta de selectare **Monitorizează fișierele și registry-ul**.

   b. Fă clic pe **Configurează**.

      Astfel, se deschide lista de reguli Monitorizare integritate sistem.

   c. Fă clic pe **Adaugă**.

      Puteți, de asemenea, să importați reguli dintr-o altă sursă.

   d. Configurează regula Monitorizare integritate sistem (consultă tabelul de mai jos).

7. Salvați-vă modificările.

Setările unei reguli a activității Verificare integritate sistem

Parametru	Descriere
Nume regulă	Numele regulii activității *Verificare integritate sistem*.
Nivel severitate eveniment	Kaspersky Endpoint Security înregistrează în jurnal evenimentele de modificare a fișierelor ori de câte ori este modificat un fișier din domeniul de monitorizare. Sunt disponibile următoarele niveluri de severitate: *Informațional*, *Avertisment*, *Critic*.

Domeniu monitorizare	• **Fișier**. Lista fișierelor și directoarelor monitorizate de componentă. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști.
	Folosiți măști:
	  • Caracterul `*` (asterisc) ține locul oricărui set de caractere, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\*\*.txt` va include toate căile către fișierele cu extensia TXT din directoarele de pe unitatea C:, dar nu și din subdirectoare.
	  • Două caractere `*` consecutive țin locul oricărui set de caractere (inclusiv un set gol) din numele de fișier sau director, inclusiv caracterele `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\**\*.txt` va include toate căile către fișierele cu extensia TXT localizată în directoarele imbricate în `Folder`, cu excepția `Folder` în sine. Masca trebuie să includă cel puțin un nivel de imbricare. Masca `C:\**\*.txt` nu este o mască validă.
	  • `?` (semn de întrebare) ține locul oricărui caracter individual, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\???.txt` va include căi pentru toate fișierele din directorul denumit `Folder` care au extensia TXT și un nume format din trei caractere.
	• **Registry**. Lista cheilor și valorilor de registry monitorizate de componentă. Kaspersky Endpoint Security acceptă caracterele `*` și `?` la introducerea unei măști.

Excluderi	• **Fișier**. Lista excluderilor din domeniul de monitorizare. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști. De exemplu, `C:\Folder\Application\*.log`. Intrările de excludere au o prioritate mai mare decât intrările din domeniul de monitorizare.
	Folosiți măști:
	  • Caracterul `*` (asterisc) ține locul oricărui set de caractere, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\*\*.txt` va include toate căile către fișierele cu extensia TXT din directoarele de pe unitatea C:, dar nu și din subdirectoare.
	  • Două caractere `*` consecutive țin locul oricărui set de caractere (inclusiv un set gol) din numele de fișier sau director, inclusiv caracterele `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\**\*.txt` va include toate căile către fișierele cu extensia TXT localizată în directoarele imbricate în `Folder`, cu excepția `Folder` în sine. Masca trebuie să includă cel puțin un nivel de imbricare. Masca `C:\**\*.txt` nu este o mască validă.
	  • `?` (semn de întrebare) ține locul oricărui caracter individual, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\???.txt` va include căi pentru toate fișierele din directorul denumit `Folder` care au extensia TXT și un nume format din trei caractere.
	• **Registry**. Lista excluderilor din domeniul de monitorizare. Kaspersky Endpoint Security acceptă caracterele `*` și `?` la introducerea unei măști. Intrările de excludere au o prioritate mai mare decât intrările din domeniul de monitorizare.

Executarea activității Verificare integritate sistem

Activitatea *Verificare integritate sistem* permite verificarea fișierelor sau cheilor de registry pentru modificări și, de asemenea, verificarea conectării dispozitivelor externe. Pentru a verifica dacă fișierele au fost modificate, puteți executa activitatea *Verificare integritate sistem* în următoarele moduri:

- Scanare rapidă.

  Când verifică dacă fișierele au fost modificate, aplicațiile verifică numai atributele fișierului. Aplicația nu verifică conținutul fișierelor.

- Scanare completă.

  Când verifică dacă fișierele au fost modificate, aplicațiile verifică toate atributele și conținutul fișierelor.

Modul în care se execută activitatea nu afectează verificarea registry-ului sau a dispozitivelor externe.

Cum se execută activitatea Verificare integritate sistem în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați **Tasks**.

   Lista activităților se deschide.
3. Fă clic pe **New task**.

   Expertul de activitate pornește. Urmează instrucțiunile din expert.
4. Selectați **Kaspersky Endpoint Security → Monitorizare a integrității sistemului de referință**. Selectează un mod Monitorizare integritate sistem:

   - **Scanare completă**. În acest mod, aplicația verifică toate atributele și hash-urile fișierelor.
   - **Scanare rapidă**. În acest mod, aplicația verifică numai atributele fișierelor.
5. Selectați computerele pe care se va efectua activitatea. Sunt disponibile următoarele opțiuni:

   - Selectare computere detectate în rețea de Serverul de administrare: dispozitive neatribuite. Dispozitivele specifice pot include dispozitive din grupuri de administrare, precum și dispozitive neatribuite.
   - Specificarea manuală a adreselor computerelor sau importarea adreselor dintr-o listă. Poți specifica nume NetBIOS, adrese IP și subrețele IP ale dispozitivelor cărora dorești să le atribui activitatea.
   - Specifică selecția dispozitivelor pentru care dorești să execuți activitatea.
   - Atribuirea activității unui grup de administrare. În acest caz, activitatea este atribuită computerelor incluse într-un grup de administrare creat anterior.
6. Selectează un cont pentru a executa activitatea. În mod implicit, Kaspersky Endpoint Security începe activitatea cu drepturile unui cont de utilizator local.
7. Configurează o planificare pentru începerea unei activități, de exemplu, manual sau într-o anumită zi a săptămânii.

8. Introdu un nume pentru activitate.

9. Ieșiți din Expert. Dacă este necesar, bifați caseta de selectare **Run the task after the wizard finishes**. Puteți monitoriza progresul activității în proprietățile activității.

Cum se execută o activitate System Integrity Check în Web Console

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **Add**.

   Expertul de activitate pornește.

3. Configurați setările pentru activitate:

   a. În lista verticală **Application**, selectează **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. În lista verticală **Task type**, selectează **System Integrity Check**.

   c. În câmpul **Task name**, introdu o descriere succintă, de exemplu *Verificare integritate sistem săptămânală*.

   d. În blocul **Devices to which the task will be assigned**, selectați domeniul activității.

4. Selectați dispozitive în funcție de opțiunea selectată pentru domeniul activității. Mergeți la pasul următor.

5. Selectează un cont pentru a executa activitatea. În mod implicit, Kaspersky Endpoint Security începe activitatea cu drepturile unui cont de utilizator local.

6. Ieșiți din Expert.

   Se va afișa o activitate nouă în lista de activități.

7. Faceți clic pe activitatea nouă.

   Se va deschide fereastra de proprietăți a activității.

8. Selectați fila **Application settings**.

9. Selectați un mod Verificare integritate sistem:

   - **Quick Scan**. Aplicația verifică numai atributele fișierului. Aplicația nu verifică conținutul fișierelor.
   - **Full Scan**. Aplicația verifică toate atributele fișierelor, precum și conținutul acestora.

10. Salvați-vă modificările.

11. Bifați caseta de selectare de lângă activitate.

12. Fă clic pe **Start**.

Pentru ca activitatea *Verificare integritate sistem* să se finalizeze cu succes, domeniul de monitorizare al activității *Verificare integritate sistem* trebuie să se potrivească complet cu linia de bază. Dacă domeniul de monitorizare este diferit, activitatea se termină cu o eroare. Pentru a sincroniza domeniile de monitorizare, executați activitatea *Actualizarea liniei de bază* cu un nou domeniu de monitorizare.

Exportul și importul regulilor Monitorizare integritate sistem

Puteți exporta lista de reguli Monitorizare integritate sistem într-un fișier XML. Apoi puteți modifica fișierul pentru a adăuga, de exemplu, un număr de înregistrări de același tip. Puteți utiliza funcția de export/import pentru a face o copie de rezervă a listei de reguli Monitorizare integritate sistem sau pentru a migra lista pe un alt server.

Componenta Monitorizare integritate sistem nu acceptă importul cheilor `HKEY_CURRENT_USER` și `HKEY_CURRENT_CONFIG` pentru activitatea *Verificare integritate sistem*. Dacă domeniul de monitorizare al activității conține aceste chei, aplicația generează evenimentul *Domeniul de monitorizare include obiecte incorecte*.

Cum se exportă și se importă o listă de reguli Monitorizare integritate sistem în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Security Controls → Monitorizare integritate sistem**.
4. Pentru a exporta sau a importa reguli *Monitorizare în timp real a integrității sistemului*:
   a. În blocul **Monitorizare în timp real a integrității sistemului**, fă clic pe butonul **Setări**.
   b. Pentru a exporta o listă de reguli Monitorizare în timp real a integrității sistemului:
      1. Selectați regulile pe care doriți să le exportați. Pentru a selecta mai multe porturi, utilizați tastele **CTRL** sau **SHIFT**.
         Dacă nu ați selectat nicio regulă, Kaspersky Endpoint Security va exporta toate regulile.
      2. Faceți clic pe linkul **Exportă**.
      3. În fereastra care se deschide, specificați numele fișierului XML în care doriți să exporți lista de reguli și selectați directorul în care doriți să salvați acest fișier.
      4. Salvați fișierul.
         Kaspersky Endpoint Security exportă lista de reguli în fișierul XML.
   c. Pentru a importa o listă de reguli Monitorizare în timp real a integrității sistemului:
      1. Faceți clic pe linkul **Importă**.
         În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de reguli.
      2. Deschideți fișierul.
         În cazul în care computerul are deja o listă de reguli, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul XML.

5. Pentru a exporta sau a importa reguli *Verificare integritate sistem*:

   a. În secțiunea **Verificare integritate sistem**, selectați **Setări personalizate**.

   b. Fă clic pe **Setări**.

   c. Pentru a exporta lista de reguli Verificare integritate sistem:

      1. Selectați regulile pe care doriți să le exportați. Pentru a selecta mai multe porturi, utilizați tastele **CTRL** sau **SHIFT**.

         Dacă nu ați selectat nicio regulă, Kaspersky Endpoint Security va exporta toate regulile.

      2. Faceți clic pe linkul **Exportă**.

      3. În fereastra care se deschide, specificați numele fișierului XML în care doriți să exporți lista de reguli și selectați directorul în care doriți să salvați acest fișier.

      4. Salvați fișierul.

      Kaspersky Endpoint Security exportă lista de reguli în fișierul XML.

   d. Pentru a importa lista de reguli Verificare integritate sistem:

      1. Faceți clic pe linkul **Importă**.

         În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de reguli.

      2. Deschideți fișierul.

      În cazul în care computerul are deja o listă de reguli, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul XML.

6. Salvați-vă modificările.

Cum se exportă și se importă o listă de reguli Monitorizare integritate sistem în Web Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **Security Controls** → **System Integrity Monitoring**.

5. Selectați fila **Windows**.

6. Pentru a exporta sau a importa reguli *Monitorizare în timp real a integrității sistemului*:

   a. În blocul **Real-Time System Integrity Monitoring**, faceți clic pe linkul **Rules**.

   b. Pentru a exporta o listă de reguli Monitorizare în timp real a integrității sistemului:

      1. Selectați regulile pe care doriți să le exportați.

      2. Fă clic pe butonul → **Export**.

         Kaspersky Endpoint Security exportă lista de reguli într-un fișier JSON în directorul de descărcări implicit.

   c. Pentru a importa o listă de reguli Monitorizare în timp real a integrității sistemului:

      1. Fă clic pe butonul → **Import**.

         În fereastra care se deschide, selectați fișierul JSON din care doriți să importați lista de adrese de încredere.

      2. Deschideți fișierul.

         În cazul în care computerul are deja o listă de reguli, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul JSON.

7. Pentru a exporta sau a importa reguli *Verificare integritate sistem*:

   a. În secțiunea **On-Demand System Integrity Check**, selectați **Custom settings**.

   b. Faceți clic pe linkul **Rules**.

   c. Pentru a exporta lista de reguli Verificare integritate sistem:

      1. Selectați regulile pe care doriți să le exportați.

      2. Fă clic pe butonul → **Export**.

         Kaspersky Endpoint Security exportă lista de reguli într-un fișier JSON în directorul de descărcări implicit.

   d. Pentru a importa lista de reguli Verificare integritate sistem:

      1. Fă clic pe butonul → **Import**.

         În fereastra care se deschide, selectați fișierul JSON din care doriți să importați lista de adrese de încredere.

      2. Deschideți fișierul.

         În cazul în care computerul are deja o listă de reguli, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul JSON.

8. Salvați-vă modificările.

Vizualizarea rapoartelor Monitorizare integritate sistem

Pentru a analiza performanța regulilor Monitorizare integritate sistem, puteți consulta rapoartele și evenimentele generate de aplicație. Kaspersky Endpoint Security generează următoarele rapoarte cu privire la componentă:

- În interfața aplicației:
  - Raportul Monitorizare integritate sistem
  - Raportul Verificare integritate sistem
  - Raportul Actualizare linie de bază

  Raportul conține evenimente Monitorizare integritate sistem
- În Consola Kaspersky Security Center:
  - Raportul despre computerele pe care regulile de monitorizare au fost declanșate de cele mai multe ori
  - Raportul despre regulile de monitorizare declanșate cel mai frecvent

  În mod implicit, este creat un raport pentru ultimele 30 de zile, incluzând data la care este creat raportul.

  Cum se vizualizează rapoartele Monitorizare integritate sistem în Consola de administrare (MMC)

  1. Deschide Consolă de administrare a Kaspersky Security Center.
  2. În nodul **Administration Server** din arborele consolei de administrare, selectați fila **Reports**.
  3. Fă clic pe **New report template**.

     Se lansează Expertul pentru șablon de raport nou.
  4. Urmează instrucțiunile din Expertul pentru șablon de raport. La pasul **Selecting the report template type**, selectați un raport Monitorizare integritate sistem (secțiunea **Other**):
     - **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**.

     După ce ai finalizat Expertul pentru șablon de raport nou, un nou șablon de raport apare în tabelul din fila **Reports**.
  5. Deschide raportul făcând dublu clic pe acesta.

  Începe procesul de generare a raportului. Raportul este afișat într-o fereastră nouă.

Cum se vizualizează rapoartele Monitorizare integritate sistem în Web Console

1. În fereastra principală a Web Console, selectați **Monitoring → Reports**.
2. Fă clic pe **Add**.

   Se lansează Expertul pentru șablon de raport nou.
3. În **Template type**, în secțiunea **Other**, selectați un raport Monitorizare integritate sistem:

   - **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**.

   După ce ai finalizat Expertul Șablon raport nou, un nou șablon de raport apare în tabel.
4. Selectați și executați raportul.

Începe procesul de generare a raportului. Raportul este afișat într-o fereastră nouă.

Pentru a vizualiza evenimentele generate de aplicație, puteți utiliza și selecțiile de evenimente din consola Kaspersky Security Center.

Resetarea stării de integritate a sistemului

Computerele din consola Kaspersky Security Center au una dintre următoarele stări: *OK*, *Warning* sau *Critical*. Dacă Monitorizare integritate sistem detectează modificarea fișierelor sau a cheilor de registry în domeniul de monitorizare, starea computerului se schimbă în *Warning* sau *Critical*. Starea atribuită de Monitorizare integritate sistem se numește *starea integrității sistemului*. Puteți reseta starea integrității sistemului, de exemplu, dacă analiza v-a convins că modificarea detectată a obiectelor nu afectează securitatea computerului.

Cum se resetează starea integrității sistemului în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Tasks**.

   Lista activităților se deschide.
2. Fă clic pe **New task**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Selectarea tipului activității

Selectați **Kaspersky Endpoint Security for Windows (14.1) → Resetarea stării de integritate a sistemului**.

Pasul 2. Selectarea dispozitivelor cărora le va fi atribuită activitatea

Selectați computerele pe care se va efectua activitatea. Sunt disponibile următoarele opțiuni:

- Atribuirea activității unui grup de administrare. În acest caz, activitatea este atribuită computerelor incluse într-un grup de administrare creat anterior.
- Selectare computere detectate în rețea de Serverul de administrare: *dispozitive neatribuite*. Dispozitivele specifice pot include dispozitive din grupuri de administrare, precum și dispozitive neatribuite.
- Specificarea manuală a adreselor computerelor sau importarea adreselor dintr-o listă. Poți specifica nume NetBIOS, adrese IP și subrețele IP ale dispozitivelor cărora dorești să le atribui activitatea.

Pasul 3. Configurarea unei planificări de pornire a activității

Configurează planificarea activității, de exemplu, manual.

Pasul 4. Definirea numelui activității

Introduceți numele activității, de exemplu, *Resetarea stării după modificarea domeniului de monitorizare*.

Pasul 5. Finalizarea creării activității

Ieșiți din Expert. Dacă este necesar, bifați caseta de selectare **Run the task after the wizard finishes**. Puteți monitoriza progresul activității în proprietățile activității.

Cum se resetează starea integrității sistemului în Web Console

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **Add**.

   Expertul de activitate pornește.

3. Configurați setările pentru activitate:

   a. În lista verticală **Application**, selectează **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. În lista verticală **Task type**, selectează **System integrity status reset**.

   c. În câmpul **Task name**, introduceți o scurtă descriere, de exemplu, *Resetarea stării după modificarea domeniului de monitorizare*.

   d. În blocul **Devices to which the task will be assigned**, selectați domeniul activității.

4. Selectați dispozitive în funcție de opțiunea selectată pentru domeniul activității. Mergeți la pasul următor.

5. Selectează un cont pentru a executa activitatea. În mod implicit, Kaspersky Endpoint Security începe activitatea cu drepturile unui cont de utilizator local.

6. Ieșiți din Expert.

   Se va afișa o activitate nouă în lista de activități.

7. Bifați caseta de selectare de lângă activitate.

8. Fă clic pe **Start**.

Ca rezultat, dacă starea computerului a fost schimbată în *Warning* sau *Critical* din cauza evenimentelor Monitorizare integritate sistem, starea computerului este resetată la *OK*. Dacă starea computerului a fost schimbată și din cauza altor evenimente, starea computerului rămâne neschimbată.

Cloud Discovery

Cloud Discovery gestionează accesul utilizatorilor la serviciile cloud. Serviciile cloud includ, de exemplu, Microsoft Teams, Salesforce și Microsoft Office 365. Serviciile cloud sunt grupate în categorii, de exemplu, *Partajare fișiere*, *Programe de mesagerie*, *E-mail*. Experții Kaspersky actualizează periodic categoriile Cloud Discovery și serviciile cloud clasificate în aceste categorii. Kaspersky Endpoint Security actualizează setul de categorii și servicii cloud cu bazele de date ale aplicațiilor. Acest lucru înseamnă că Cloud Discovery nu utilizează Kaspersky Security Network pentru clasificarea serviciilor cloud.

Cloud Discovery oferă următoarele funcționalități:

- Monitorizarea utilizării serviciilor cloud
- Blocarea accesului utilizatorilor la serviciile cloud

Cerințe de sistem

Cloud Discovery este disponibilă în cazul în care sunt îndeplinite următoarele condiții:

- Aplicația este instalată pe un computer care execută Windows pentru stații de lucru.

  Componenta nu este disponibilă pentru servere.

- Kaspersky Security Center versiunea 15.1 sau o versiune ulterioară.

  Componenta nu este disponibilă în Consola de administrare (MMC). Poți configura componenta Cloud Discovery în Kaspersky Security Center Web Console și Kaspersky Security Center Cloud Console.

- Licență Kaspersky Next.

Activează funcționalitatea aplicației pe care o necesită componenta Cloud Discovery:

1. **Scanează conexiunile criptate**. Acest lucru este necesar pentru monitorizarea traficului HTTPS. Poți gestiona această funcționalitate în secțiunea **Setări rețea**.

2. **Injectează segmente de script în traficul web pentru a interacționa cu paginile web**. Scriptul permite înregistrarea evenimentelor Cloud Discovery. Scriptul oferă, de asemenea, blocarea completă a accesului la serviciile cloud. Fără script, aplicația blochează accesul doar pentru domeniile de servicii cloud. Poți gestiona această funcționalitate în secțiunea **Setări rețea**.

De asemenea, puteți activa funcționalitatea **Înregistrați în jurnal deschiderea paginilor permise**. Funcționalitatea include gruparea evenimentelor atunci când un utilizator vizitează pagini web care aparțin aceluiași domeniu. În acest fel, atunci când un utilizator utilizează un serviciu cloud, Cloud Discovery înregistrează un singur eveniment în loc de mai multe evenimente pentru fiecare pagină web. Poți gestiona această funcționalitate în secțiunea **Control Web**.

Monitorizarea serviciilor cloud

Atunci când un utilizator începe să utilizeze un serviciu cloud, Kaspersky Endpoint Security înregistrează acest eveniment și creează o intrare în raport. Componenta Cloud Discovery controlează utilizarea serviciilor cloud în browser, precum și în aplicațiile corespunzătoare. Componenta Cloud Discovery controlează utilizarea serviciilor cloud prin HTTP și HTTPS.

Cum se activează monitorizarea serviciilor cloud în Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **Communication & Web Protection** → **Cloud Discovery**.

5. Duceți comutatorul **Cloud Discovery ENABLED** la poziția activat.

6. Salvați-vă modificările.

Ca urmare, aplicația transmite informații despre serviciile cloud utilizate către Kaspersky Security Center. Poți vizualiza informațiile privind utilizarea serviciilor cloud în rapoarte. Dacă este necesar, poți bloca accesul la serviciile în cloud.

Blocarea accesului utilizatorilor la serviciile cloud

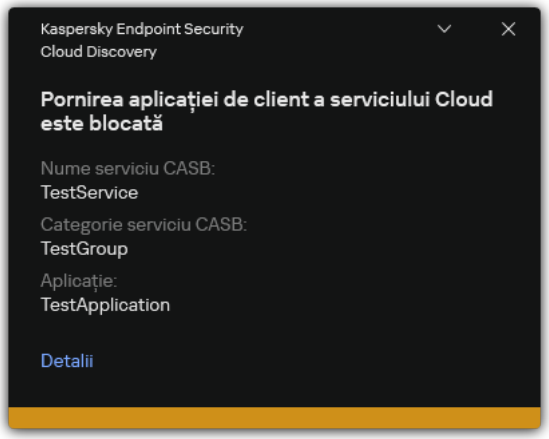
Blocarea accesului la serviciile în cloud este disponibilă numai pentru licența Kaspersky Next EDR Optimum și XDR Expert. Această caracteristică nu este disponibilă pentru licența Kaspersky Next EDR Foundations. Pentru o comparație între funcționalitățile aplicației în funcție de tipul de licență Kaspersky Next, consultați Ajutor Kaspersky Next.

Administratorul poate restricționa accesul utilizatorilor la categoriile Cloud Discovery sau la servicii cloud individuale. Astfel, administratorul poate permite numai servicii cloud sigure și poate evita scurgerile de date. *Informații privind nivelul de risc* este afișat pentru fiecare serviciu cloud în componenta Cloud Discovery. Nivelul de risc ajută la detectarea serviciilor care nu îndeplinesc cerințele de securitate ale organizației.

Nivelul de risc este o estimare și nu implică nicio declarație cu privire la calitatea serviciului cloud sau a furnizorului acestuia. Nivelul de risc este doar o recomandare a experților Kaspersky.

Nivelurile de risc ale serviciilor cloud sunt afișate în secțiunea **Cloud Discovery** a politicii în lista tuturor serviciilor cloud controlate.

Alte componente Kaspersky Endpoint Security asigură protecție împotriva amenințărilor și urmărirea activităților suspecte ale utilizatorilor atunci când folosesc servicii cloud.



Notificările Cloud Discovery

Componenta Cloud Discovery nu blochează aplicațiile cloud care au fost pornite înainte de Kaspersky Endpoint Security.

Cum se blochează accesul la serviciile în cloud în Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Communication & Web Protection** → **Cloud Discovery**.
5. Duceți comutatorul **Cloud Discovery ENABLED** la poziția activat.

   Se afișează o listă cu toate serviciile cloud. Serviciile cloud sunt grupate în categorii, de exemplu, *File sharing*, *Messengers*, *Email*. Experții Kaspersky actualizează periodic categoriile Cloud Discovery și serviciile cloud clasificate în aceste categorii. Kaspersky Endpoint Security actualizează setul de categorii și servicii cloud cu bazele de date ale aplicațiilor.
6. Utilizează comutatorul din coloana **Access** pentru a configura accesul la serviciile cloud.
7. Salvați-vă modificările.

Drept rezultat, aplicația controlează utilizarea serviciilor cloud în browser, precum și în aplicațiile corespunzătoare.

Zonă de încredere

O *zonă de încredere* este o listă de obiecte și aplicații configurate de administratorul de sistem, pe care Kaspersky Endpoint Security nu le monitorizează când este activ.

Administratorul formează zona de încredere independent, luând în considerare caracteristicile obiectelor gestionate și aplicațiile instalate pe computer. Este posibil să fie necesară includerea obiectelor și aplicațiilor în zona de încredere când Kaspersky Endpoint Security blochează accesul la un anumit obiect sau la o anumită aplicație, dacă ești sigur că obiectul sau aplicația respectivă este inofensivă. Un administrator poate permite, de asemenea, unui utilizator să își creeze propria zonă de încredere locală pentru un anumit computer. În acest fel, utilizatorii își pot crea propriile liste locale de excluderi și aplicații de încredere, pe lângă zona generală de încredere dintr-o politică.

Începând cu Kaspersky Endpoint Security 12.5 for Windows, poți adăuga telemetrie EDR în zona de încredere. Acest lucru permite optimizarea datelor pe care aplicația le trimite către serverul de colectare a telemetriei pentru soluția Kaspersky Anti Targeted Attack Platform (EDR).

Începând cu Kaspersky Endpoint Security 12.6 for Windows, excluderile de scanare și aplicații de încredere sunt adăugate la zona de încredere. Excluderile de la scanare și aplicațiile de încredere predefinite ajută la configurarea rapidă a Kaspersky Endpoint Security pe serverele SQL, serverele Microsoft Exchange și System Center Configuration Manager. Aceasta înseamnă că nu trebuie să configurați manual o zonă de încredere pentru aplicație pe servere.

Începând cu Kaspersky Endpoint Security 12.8 for Windows, poți instala aplicația în modul Light Agent pentru a proteja mediile virtuale. Excluderile de la scanare predefinite și aplicațiile de încredere te pot ajuta să configurezi rapid Kaspersky Endpoint Security în mediile virtuale Citrix și VMware.

Crearea unei excluderi de la scanare

O *excludere de la scanare* este un set de condiții care trebuie să fie îndeplinite pentru ca aplicația Kaspersky Endpoint Security să nu scaneze un anumit obiect pentru viruși și alte amenințări. Excluderile de la scanare fac posibilă utilizarea în siguranță a software-urilor legitime care pot fi exploatate de infractori pentru a aduce daune computerului sau datelor utilizatorului. Cu toate că nu au funcții rău intenționate, astfel de aplicații pot fi exploatate de intruși. Pentru detalii despre software-urile legitime care pot fi utilizate de intruși pentru a aduce daune computerului sau datelor personale, consultă site-ul web Enciclopedia IT Kaspersky.

Este posibil ca programul Kaspersky Endpoint Security să blocheze astfel de aplicații. Pentru a împiedica blocarea lor, poți configura excluderi de la scanare pentru aplicațiile în uz. În acest scop, adaugă numele sau masca de nume listată în Enciclopedia IT a Kaspersky la zona de încredere. De exemplu, utilizezi frecvent aplicația Radmin pentru administrarea de la distanță a computerelor. Kaspersky Endpoint Security privește această activitate ca suspectă și este posibil să o blocheze. Pentru a împiedica blocarea aplicației, creează o excludere de la scanare cu numele sau masca de nume listată în Enciclopedia IT a Kaspersky.

Dacă o aplicație care colectează informații și le trimite spre procesare este instalată pe computerul dvs., Kaspersky Endpoint Security poate clasifica această aplicație ca malware. Pentru a evita acest lucru, poți exclude aplicația de la scanare configurând Kaspersky Endpoint Security așa cum este descris în acest document.

Excluderile de la scanare pot fi utilizate de următoarele componente și acțiuni ale aplicației, care sunt configurate de către administratorul de sistem:

- Behavior Detection
- Exploit Prevention
- Host Intrusion Prevention
- File Threat Protection
- Web Threat Protection
- Mail Threat Protection
- Activitatea *Scanare malware*

Kaspersky Endpoint Security nu scanează un obiect dacă unitatea sau directorul care conține acel obiect este inclus(ă) în domeniul de scanare la începutul uneia dintre activitățile de scanare. Cu toate acestea, excluderea de la scanare nu se aplică atunci când se pornește o activitate de scanare particularizată pentru acest obiect particular.

Modificarea listei de excluderi de la scanare poate fi blocată de proprietățile politicii principale. Pentru a modifica lista, trebuie să permiteți modificarea setărilor zonei de încredere în Web Console („lacătul" trebuie să fie deblocat).

Zonele de încredere sunt grupate diferit în Consola de administrare (MMC) și în Web Console. De asemenea, modul în care se împiedică modificarea parametrilor zonei de încredere este diferit („lacăte" diferite). Vă recomandăm să utilizați exclusiv Web Console pentru gestionarea aplicației. În cazul în care configurați zona de încredere pe console diferite, este posibil ca plug-inul de gestionare să reseteze „lacătul" la starea implicită.

Cum se creează o excludere de la scanare în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Setări generale → Excluderi și tipuri de obiecte**.
4. În blocul **Excluderi de la scanare și aplicații de încredere → Excluderi de la scanare**, fă clic pe butonul **Setări**.
   Acest lucru va deschide o fereastră care conține lista excluderilor.
5. Bifați caseta de selectare **Îmbină valorile în momentul moștenirii** dacă doriți să creați o listă consolidată a excluderilor pentru toate computerele companiei. Listele excluderilor din politicile principale și secundare vor fi îmbinate. Listele vor fi îmbinate dacă funcția de îmbinare a valorilor în momentul moștenirii este activată. Excluderile de la din politica principală sunt afișate în politicile secundare într-o vizualizare numai citire. Nu este posibilă modificarea sau ștergerea excluderilor din politica principală.

6. Bifați caseta de selectare **Permite utilizarea excluderilor locale** dacă doriți să permiteți utilizatorului să creeze o listă locală de excluderi. În acest fel, un utilizator își poate crea propria listă locală de excluderi pe lângă lista generală de excluderi generate în politică. Un administrator poate utiliza Kaspersky Security Center pentru a vizualiza, adăuga, edita sau șterge elemente de listă din proprietățile computerului.

   În cazul în care caseta de selectare este debifată, utilizatorul poate accesa doar lista generală a excluderilor generate în politică. De asemenea, dacă această casetă de selectare este debifată, Kaspersky Endpoint Security ascunde lista consolidată a excluderilor de la scanare în interfața de utilizator a aplicației.

7. Faceți clic pe **Adaugă** și selectați o acțiune:

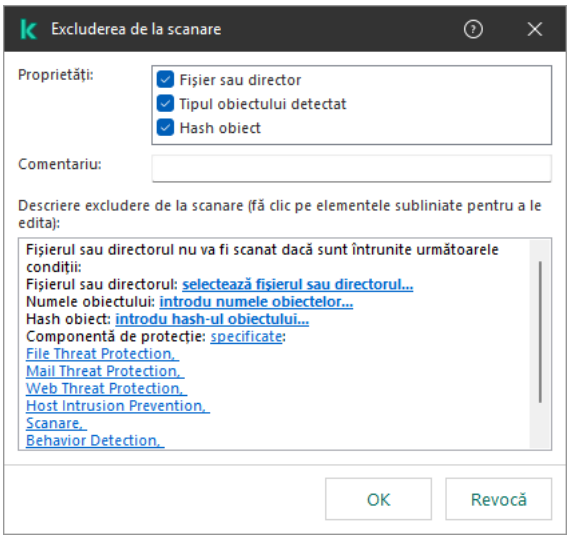
   - **Categorie**. Puteți grupa excluderile de la scanare în categorii separate. Pentru a crea o categorie nouă, introduceți numele categoriei și adăugați cel puțin o excludere de la scanare la categorie.

   - **Excludere nouă**. Kaspersky Endpoint Security adaugă o nouă excludere de la scanare la rădăcina listei.

   - **Selectează excluderea din listă**. Pentru a configura rapid Kaspersky Endpoint Security pe serverele SQL, serverele Microsoft Exchange și System Center Configuration Manager, aplicația include *excluderi de la scanare predefinite*. De asemenea, au fost adăugate excluderi de la scanare predefinite pentru a sprijini configurarea aplicațiilor în mediile virtuale Citrix și VMware. Trebuie să selectați excluderile de la scanare predefinite, în funcție de scopul serverului protejat.

   - **Excludere nouă în categoria selectată**. Pentru a adăuga o nouă excludere de la scanare la o anumită categorie, selectați o categorie.

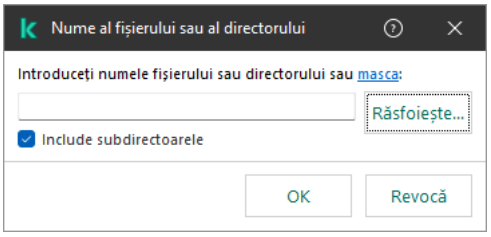
8. Pentru a exclude un fișier sau un director de la scanare:



Setări excluderi

a. În blocul **Proprietăți**, bifați caseta de selectare **Fișier sau director**.

b. Fă clic pe linkul din blocul de mai jos pentru a deschide fereastra **Nume al fișierului sau al directorului**.



Selectare fișier sau director

a. Introdu numele fișierului sau al directorului sau masca de nume pentru fișier sau director sau selectați fișierul sau directorul în arborele de directoare făcând clic pe **Răsfoiește**.

Folosiți măști:

- Caracterul `*` (asterisc) ține locul oricărui set de caractere, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\*\*.txt` va include toate căile către fișierele cu extensia TXT din directoarele de pe unitatea C:, dar nu și din subdirectoare.

- Două caractere `*` consecutive țin locul oricărui set de caractere (inclusiv un set gol) din numele de fișier sau director, inclusiv caracterele `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\**\*.txt` va include toate căile către fișierele cu extensia TXT localizată în directoarele imbricate în `Folder`, cu excepția `Folder` în sine. Masca trebuie să includă cel puțin un nivel de imbricare. Masca `C:\**\*.txt` nu este o mască validă.

- `?` (semn de întrebare) ține locul oricărui caracter individual, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\???.txt` va include căi pentru toate fișierele din directorul denumit `Folder` care au extensia TXT și un nume format din trei caractere.

Puteți utiliza măști la începutul, la mijlocul sau la sfârșitul căii fișierului. De exemplu, dacă doriți să adăugați un director pentru toți utilizatorii la excluderi, introduceți masca `?:\Users\*\Folder\`.

Kaspersky Endpoint Security acceptă variabile de mediu

Poți exclude directoarele de rețea. Pentru aceasta, introdu manual calea către directorul de rețea (de exemplu, `\\Network Share\*`).

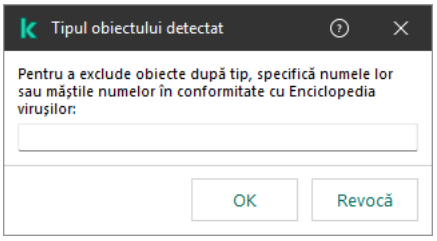
> Kaspersky Endpoint Security nu acceptă variabila de mediu `%userprofile%` atunci când se generează o listă de excluderi în consola Kaspersky Security Center. Pentru a aplica intrarea tuturor conturilor de utilizatori, puteți utiliza caracterul `*` (de exemplu, `C:\Users\*\Documents\File.exe`). Ori de câte ori adăugați o variabilă de mediu, trebuie să reporniți aplicația.

b. Salvați-vă modificările.

9. Pentru a exclude de la scanare obiecte cu un anumit nume:

a. În blocul **Proprietăți**, bifați caseta de selectare **Tipul obiectului detectat**.

b. Fă clic pe linkul din blocul de mai jos pentru a deschide fereastra **Tipul obiectului detectat**.



Selectare obiect

a. Introduceți numele tipului obiectului conform clasificării din Enciclopedia Kaspersky (de exemplu, `Email-Worm`, `Rootkit` sau `RemoteAdmin`).

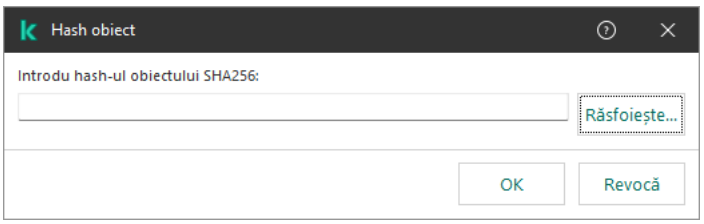
Puteți folosi măști cu caracterul `?` (înlocuiește orice caracter unic) și caracterul `*` (înlocuiește orice număr de caractere). De exemplu, dacă este specificată masca `Client*`, Kaspersky Endpoint Security exclude obiectele `Client-IRC`, `Client-P2P` și `Client-SMTP` de la scanări.

b. Salvați-vă modificările.

10. Dacă doriți să excludeți un fișier individual din scanări:

a. În blocul **Proprietăți**, bifați caseta de selectare **Hash obiect**.

b. Fă clic pe linkul din blocul de mai jos pentru a deschide fereastra **Hash obiect**.



Selectare fișier

a. Introdu hash-ul fișierului sau selectează fișierul făcând clic pe butonul **Răsfoiește**.

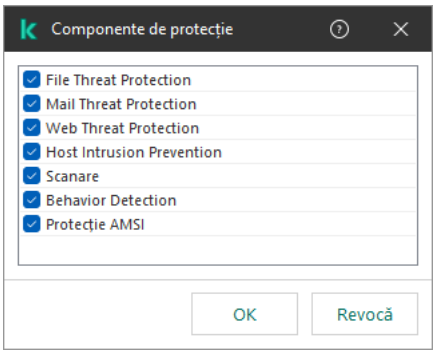
Dacă fișierul este modificat, va fi modificat și hash-ul fișierului. Dacă se întâmplă acest lucru, fișierul modificat nu va fi adăugat la excluderi.

b. Salvați-vă modificările.

11. Dacă este necesar, în câmpul **Comentariu**, introdu o descriere succintă a excluderii de la scanare pe care o creezi.

12. Specifică apoi componentele aplicației Kaspersky Endpoint Security care trebuie să utilizeze excluderea de la scanare:

    a. Fă clic pe linkul din blocul de mai jos pentru a deschide fereastra **Componente de protecție**.



Selectare componente de protecție

    a. Bifați casetele de selectare de lângă componentele pentru care trebuie aplicată excluderea de la scanare.

    În cazul în care componentele sunt specificate în setările pentru excluderea de la scanare, această excludere se aplică numai pentru scanarea de către aceste componente ale aplicației Kaspersky Endpoint Security.

    În cazul în care componentele nu sunt specificate în setările excluderii de la scanare, această excludere se aplică pentru scanarea de către toate componentele aplicației Kaspersky Endpoint Security.

13. Fă clic pe **OK**.

    Noua excludere va fi adăugată în listă. Puteți dezactiva excluderea oricând folosind caseta de selectare de lângă obiect.

14. Salvați-vă modificările.

Cum se creează o excludere de la scanare în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesează secțiunea **Trusted Zone**.

5. În fereastra care se deschide, fă clic pe linkul **Malware Scan exclusions**.

6. Bifați caseta de selectare **Merge values when inheriting** dacă doriți să creați o listă consolidată a excluderilor pentru toate computerele companiei. Listele excluderilor din politicile principale și secundare vor fi îmbinate. Listele vor fi îmbinate dacă funcția de îmbinare a valorilor în momentul moștenirii este activată. Excluderile de la din politica principală sunt afișate în politicile secundare într-o vizualizare numai citire. Nu este posibilă modificarea sau ștergerea excluderilor din politica principală.

7. Bifați caseta de selectare **Allow use of local exclusions** dacă doriți să permiteți utilizatorului să creeze o listă locală de excluderi. În acest fel, un utilizator își poate crea propria listă locală de excluderi pe lângă lista generală de excluderi generate în politică. Un administrator poate utiliza Kaspersky Security Center pentru a vizualiza, adăuga, edita sau șterge elemente de listă din proprietățile computerului.

   În cazul în care caseta de selectare este debifată, utilizatorul poate accesa doar lista generală a excluderilor generate în politică. De asemenea, dacă această casetă de selectare este debifată, Kaspersky Endpoint Security ascunde lista consolidată a excluderilor de la scanare în interfața de utilizator a aplicației.

8. Faceți clic pe **Add** și selectați o acțiune:

   - **Category**. Puteți grupa excluderile de la scanare în categorii separate. Pentru a crea o categorie nouă, introduceți numele categoriei și adăugați cel puțin o excludere de la scanare la categorie.
   - **New exclusion**. Kaspersky Endpoint Security adaugă o nouă excludere de la scanare la rădăcina listei.
   - **Select exclusion from list**. Pentru a configura rapid Kaspersky Endpoint Security pe serverele SQL, serverele Microsoft Exchange și System Center Configuration Manager, aplicația include *excluderi de la scanare predefinite*. De asemenea, au fost adăugate excluderi de la scanare predefinite pentru a sprijini configurarea aplicațiilor în mediile virtuale Citrix și VMware. Trebuie să selectați excluderile de la scanare predefinite, în funcție de scopul serverului protejat.

   Pentru a adăuga o nouă excludere de la scanare la o anumită categorie, bifați caseta de selectare de lângă categoria respectivă și selectați opțiunea **New exclusion**.

9. Selectați modul în care doriți să adăugați excluderea: **Path to the file or folder**, **Object type** sau **Object hash**.

10. Pentru a exclude un fișier sau un director de la scanare, introduceți calea manual. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști.

    - Caracterul `*` (asterisc) ține locul oricărui set de caractere, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\*\*.txt` va include toate căile către fișierele cu extensia TXT din directoarele de pe unitatea C:, dar nu și din subdirectoare.
    - Două caractere `*` consecutive țin locul oricărui set de caractere (inclusiv un set gol) din numele de fișier sau director, inclusiv caracterele `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\**\*.txt` va include toate căile către fișierele cu extensia TXT localizată în directoarele imbricate în `Folder`, cu excepția `Folder` în sine. Masca trebuie să includă cel puțin un nivel de imbricare. Masca `C:\**\*.txt` nu este o mască validă.
    - `?` (semn de întrebare) ține locul oricărui caracter individual, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\???.txt` va include căi pentru toate fișierele din directorul denumit `Folder` care au extensia TXT și un nume format din trei caractere.

      Puteți utiliza măști la începutul, la mijlocul sau la sfârșitul căii fișierului. De exemplu, dacă doriți să adăugați un director pentru toți utilizatorii la excluderi, introduceți masca `?:\Users\*\Folder\`.

      Poți exclude directoarele de rețea. Pentru aceasta, introdu manual calea către directorul de rețea (de exemplu, `\\Network Share\*`).

11. Dacă doriți să excludeți un anumit tip de obiect din scanări, în câmpul **Object type** introduceți numele tipului de obiect conform clasificării din Enciclopedia Kaspersky (de exemplu, `Email-Worm`, `Rootkit` sau `RemoteAdmin`).

    Puteți folosi măști cu caracterul `?` (înlocuiește orice caracter unic) și caracterul `*` (înlocuiește orice număr de caractere). De exemplu, dacă este specificată masca `Client*`, Kaspersky Endpoint Security exclude obiectele `Client-IRC`, `Client-P2P` și `Client-SMTP` de la scanări.

12. Dacă doriți să excludeți un fișier individual de la scanări, introduceți hash-ul fișierului în câmpul **Object hash**.

    Dacă fișierul este modificat, va fi modificat și hash-ul fișierului. Dacă se întâmplă acest lucru, fișierul modificat nu va fi adăugat la excluderi.

13. În blocul **Apply exclusion to**, selectați componentele la care doriți să se aplice excluderea scanării.

14. Dacă este necesar, în câmpul **Comment**, introdu o descriere succintă a excluderii de la scanare pe care o creezi.

15. Fă clic pe **OK**.

    Noua excludere va fi adăugată în listă. Puteți utiliza comutatorul pentru a stop an exclusion în orice moment.

16. Salvați-vă modificările.

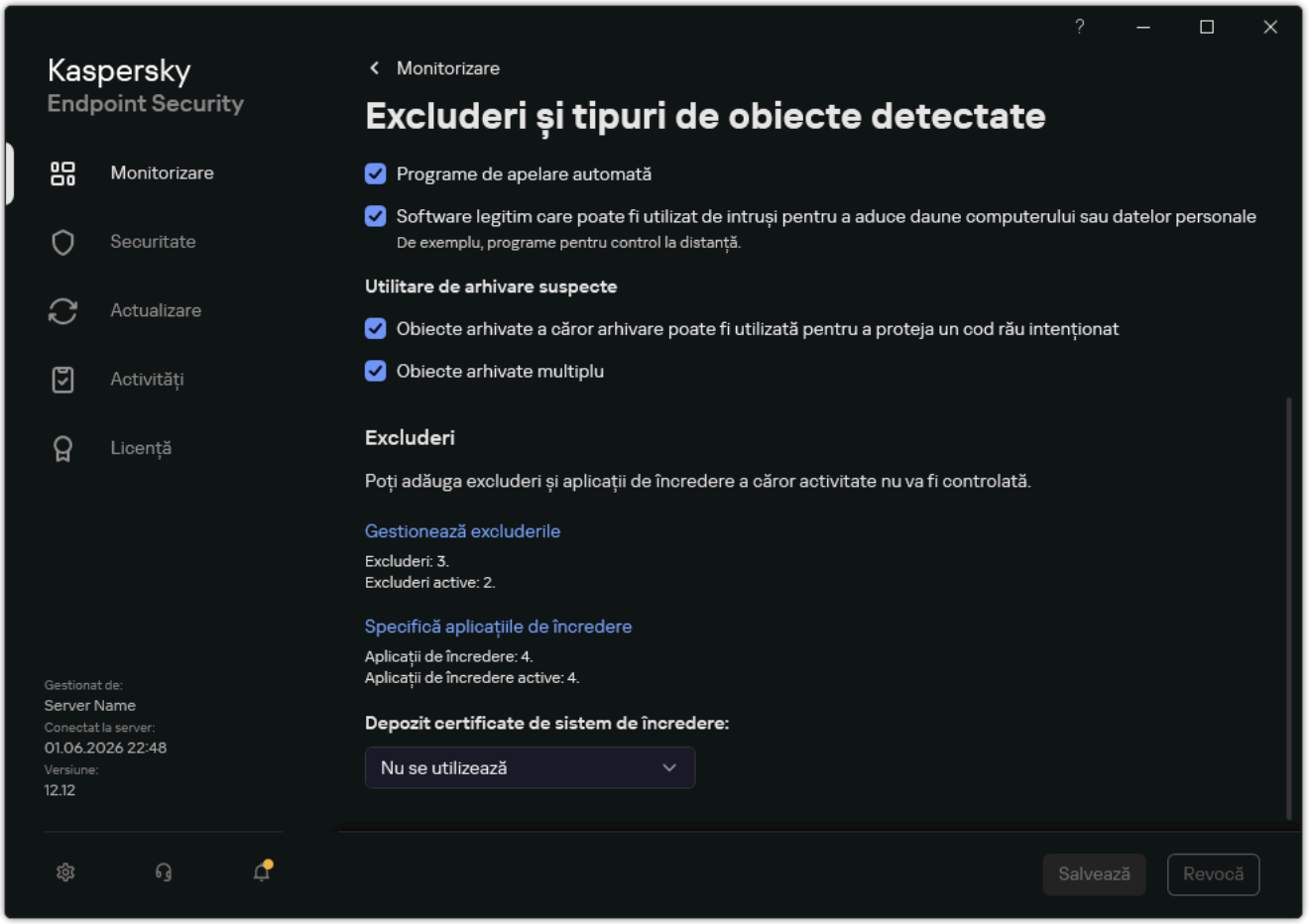
Cum se creează o excludere de scanare în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Setări generale** → **Excluderi și tipuri de obiecte detectate**.

3. În blocul **Excluderi**, faceți clic pe linkul **Gestionează excluderile**.

> Kaspersky Endpoint Security ascunde lista excluderilor de la scanare în interfața de utilizator a aplicației dacă configurarea excluderilor de la scanare este blocată de administrator în consolă (simbolul „lacăt închis") și excluderile de la scanare locale sunt interzise (caseta de selectare **Permite utilizarea excluderilor locale** este debifată).



Setări pentru excluderi

4. Faceți clic pe **Adaugă** și selectați o acțiune:

   - **Categorie**. Puteți grupa excluderile de la scanare în categorii separate. Pentru a crea o categorie nouă, introduceți numele categoriei și adăugați cel puțin o excludere de la scanare la categorie.
   - **Excludere nouă**. Kaspersky Endpoint Security adaugă o nouă excludere de la scanare la rădăcina listei.
   - **Selectează excluderea din listă**. Pentru a configura rapid Kaspersky Endpoint Security pe serverele SQL, serverele Microsoft Exchange și System Center Configuration Manager, aplicația include *excluderi de la scanare predefinite*. De asemenea, au fost adăugate excluderi de la scanare predefinite pentru a sprijini configurarea aplicațiilor în mediile virtuale Citrix și VMware. Trebuie să selectați excluderile de la scanare predefinite, în funcție de scopul serverului protejat.

   Pentru a adăuga o nouă excludere de la scanare la o anumită categorie, bifați caseta de selectare de lângă categoria respectivă și selectați opțiunea **Excludere nouă**.

5. Dacă doriți să excludeți un fișier sau director din scanări, selectați fișierul sau directorul făcând clic pe butonul **Răsfoiește**.

   De asemenea, puteți introduce calea manual. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști.

   - Caracterul `*` (asterisc) ține locul oricărui set de caractere, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\*\*.txt` va include toate căile către fișierele cu extensia TXT din directoarele de pe unitatea C:, dar nu și din subdirectoare.
   - Două caractere `*` consecutive țin locul oricărui set de caractere (inclusiv un set gol) din numele de fișier sau director, inclusiv caracterele `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\**\*.txt` va include toate căile către fișierele cu extensia TXT localizată în directoarele imbricate în `Folder`, cu excepția `Folder` în sine. Masca trebuie să includă cel puțin un nivel de imbricare. Masca `C:\**\*.txt` nu este o mască validă.
   - `?` (semn de întrebare) ține locul oricărui caracter individual, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\???.txt` va include căi pentru toate fișierele din directorul denumit `Folder` care au extensia TXT și un nume format din trei caractere.

     Puteți utiliza măști la începutul, la mijlocul sau la sfârșitul căii fișierului. De exemplu, dacă doriți să adăugați un director pentru toți utilizatorii la excluderi, introduceți masca `?:\Users\*\Folder\`.

     Poți exclude directoarele de rețea. Pentru aceasta, introdu manual calea către directorul de rețea (de exemplu, `\\Network Share\*`).

6. Dacă doriți să excludeți un anumit tip de obiect din scanări, în câmpul **Tipul obiectului detectat** introduceți numele tipului de obiect conform clasificării din Enciclopedia Kaspersky (de exemplu, `Email-Worm`, `Rootkit` sau `RemoteAdmin`).

   Puteți folosi măști cu caracterul `?` (înlocuiește orice caracter unic) și caracterul `*` (înlocuiește orice număr de caractere). De exemplu, dacă este specificată masca `Client*`, Kaspersky Endpoint Security exclude obiectele `Client-IRC`, `Client-P2P` și `Client-SMTP` de la scanări.

7. Dacă doriți să excludeți un fișier individual de la scanări, introduceți hash-ul fișierului în câmpul **Hash obiect**.

   Dacă fișierul este modificat, va fi modificat și hash-ul fișierului. Dacă se întâmplă acest lucru, fișierul modificat nu va fi adăugat la excluderi.

8. În blocul **Componente de protecție**, selectați componentele la care doriți să se aplice excluderea scanării.

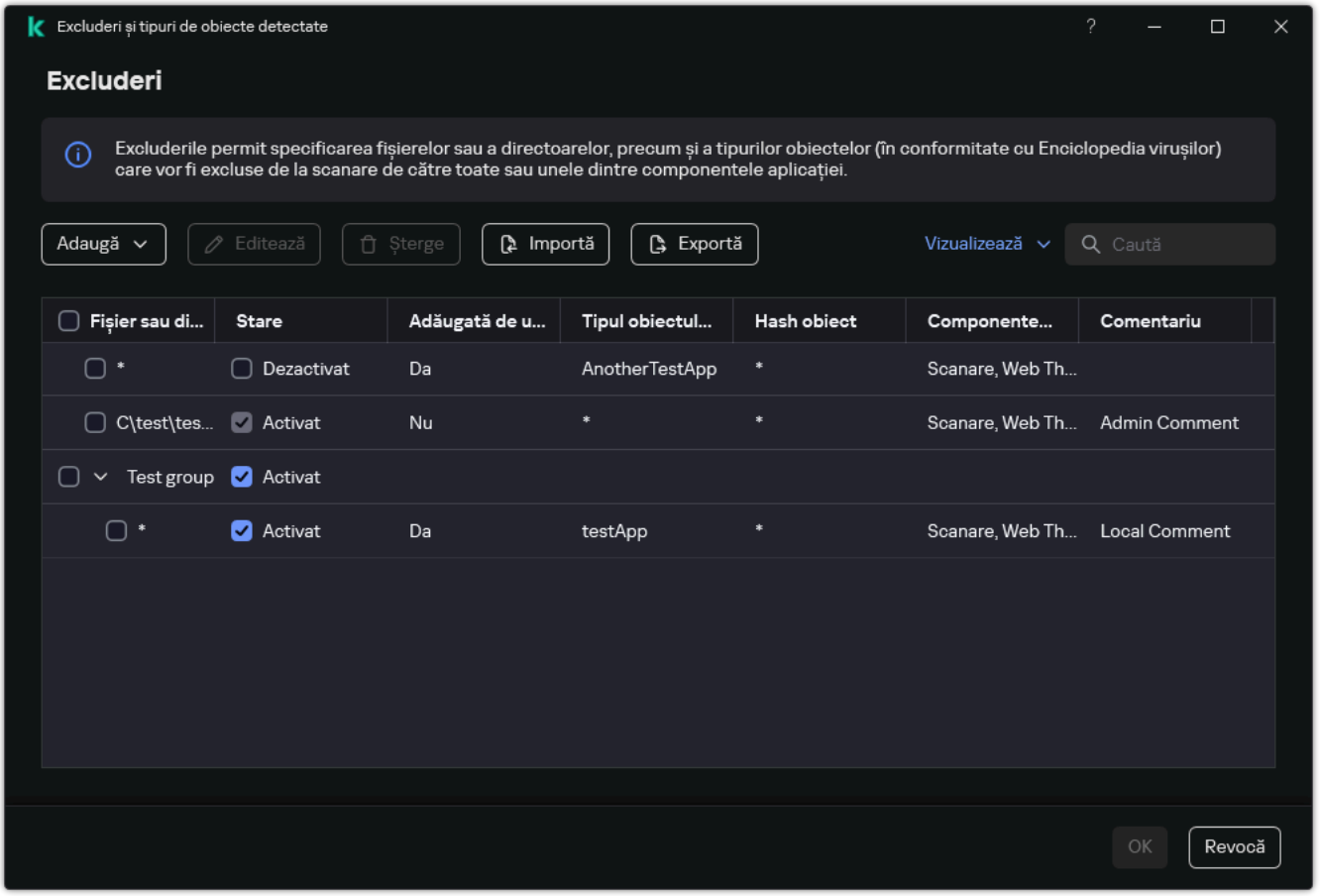
9. Dacă este necesar, în câmpul **Comentariu**, introdu o descriere succintă a excluderii de la scanare pe care o creezi.

10. Selectați starea **Activă** pentru excludere.

11. Fă clic pe **Adaugă**.

    Noua excludere va fi adăugată în listă. Puteți dezactiva excluderea oricând folosind caseta de selectare din coloana **Stare**.

12. Salvați-vă modificările.



Listă de excluderi

Exemple de mască de cale:

Recomandăm specificarea unor căi relative în locul unor căi absolute. Acest lucru permite excluderea nu doar a obiectelor sistemului de fișiere, ci și a obiectelor fără fișiere. De exemplu, `*\Program Files (x86)\Folder\Subfolder`.

Căi către fișiere aflate în oricare dosar:

- Masca `*.exe` va include toate căile către fișierele care au extensia exe.
- Masca `example*` va include toate căile către fișierele denumite EXAMPLE.

Căi către fișiere aflate într-un dosar specificat:

- Masca `C:\dir\*.*` va include toate căile către fișierele aflate în directorul C:\dir\, însă nu în subdirectoarele din `C:\dir\`.
- Masca `C:\dir\*` va include toate căile către fișierele aflate în directorul `C:\dir\`, inclusiv în subdirectoare.
- Masca `C:\dir\` va include toate căile către fișierele aflate în directorul `C:\dir\`, inclusiv în subdirectoare.
- Masca `C:\dir\*.exe` va include toate căile către fișierele cu extensia EXE aflate în directorul `C:\dir\`, însă nu în subdirectoarele din `C:\dir\`.
- Masca `C:\dir\test` va include toate căile către fișierele denumite „test" aflate în directorul `C:\dir\`, însă nu în subdirectoarele din `C:\dir\`.
- Masca `C:\dir\*\test` va include toate căile către fișierele denumite „test" aflate în directorul `C:\dir\` și în subdirectoarele din `C:\dir\`.
- Masca `C:\dir1\*\dir3\` va include toate căile către fișierele din subdirectoarele dir3 la un nivel din directorul `C:\dir1\`.
- Masca `C:\dir1\**\dirN\` va include toate căile către fișierele din subdirectoarele dirN din directorul `C:\dir1\` la orice nivel.

Căi către fișiere aflate în toate dosarele cu un nume specificat:

- Masca `dir\*.*` va include toate căile către fișierele din directoarele denumite „dir", însă nu în subdirectoarele respectivelor directoare.
- Masca `dir\*` va include toate căile către fișierele din directoarele denumite „dir", însă nu în subdirectoarele respectivelor directoare.
- Masca `dir\` va include toate căile către fișierele din directoarele denumite „dir", însă nu în subdirectoarele respectivelor directoare.
- Masca `dir\*.exe` va include toate căile către fișierele cu extensia EXE din directoarele denumite „dir", însă nu în subdirectoarele respectivelor directoare.
- Masca `dir\test` va include toate căile către fișierele denumite „test" din directoarele denumite „dir", însă nu în subdirectoarele respectivelor directoare.

Crearea unei excluderi după tipul obiectelor detectate

Kaspersky Endpoint Security clasifică obiectele detectate după cum urmează:

- **Viruși și viermi**

  Subcategoria: Viruși și viermi (Viruses_and_Worms)

  Nivel de pericol: Ridicat

  Virușii și viermii clasici efectuează acțiuni care nu sunt autorizate de către utilizator. Ei pot crea copii care se pot înmulți singure.

  Virus clasic

  Când un virus clasic se infiltrează într-un computer, el infectează un fișier, se activează, efectuează acțiuni rău intenționate și adaugă copii ale sale la alte fișiere.

Un virus clasic se multiplică numai pe resursele locale ale computerului; el nu poate pătrunde singur pe alte computere. El poate fi transferat pe un alt computer numai dacă adaugă o copie a sa la un fișier care este stocat într-un director partajat sau pe un CD inserat sau dacă utilizatorul redirecționează un mesaj de e-mail cu un fișier infectat atașat.

Codul de virus clasic poate pătrunde în diferite zone ale computerelor, sistemelor de operare și aplicațiilor. În funcție de mediu, virușii se împart în *viruși de fișier*, *viruși de boot*, *viruși de script*, și *viruși macro*.

Virușii pot infecta fișiere folosind o varietate de tehnici. Virușii de tip *Overwriting* își scriu codul peste o parte din codul fișierului infectat, ștergând astfel conținutul fișierului. Fișierul infectat nu mai funcționează și nu poate fi restaurat. Virușii de tip *Parasitic* modifică fișierele, lăsându-le complet sau parțial funcționale. Virușii de tip *Companion* nu modifică fișiere, dar, în schimb, creează duplicate. Atunci când un fișier infectat este deschis, este pornit un duplicat al acestuia (care este în realitate un virus). De asemenea, sunt întâlnite și următoarele tipuri de viruși: *Viruși de tip Link*, *viruși OBJ*, *viruși LIB*, viruși *cod sursă* și mulți alții.

Vierme

La fel ca în cazul unui virus clasic, codul unui vierme se activează și efectuează acțiuni rău intenționate după ce se infiltrează într-un computer. Virușii se numesc astfel datorită capacității lor de a se „târî" de la un computer la altul și de a răspândi copii ale lor prin numeroase canale de date, fără permisiunea utilizatorului.

Modul în care viermii se răspândesc este principala caracteristică permițând diferențierea între diferitele tipuri de viermi. Tabelul următor conține o prezentare generală a diferitelor tipuri de viermi, clasificați după modul în care se răspândesc.

Moduri în care se răspândesc viermii

Tip	Name	Descriere
Vierme de e-mail	Vierme e-mail	Ei se răspândesc prin e-mail. Un mesaj de e-mail infectat conține un fișier infectat cu o copie a unui vierme sau un link către un fișier care este încărcat pe un site Web care este posibil să fi fost modificat prin hacking sau creat exclusiv în acest scop. Atunci când deschizi fișierul atașat, viermele este activat. Atunci când faci clic pe link, descarci sau deschizi fișierul, viermele începe să execute acțiunile sale rău intenționate. După aceea, el continuă să răspândească alte copii ale sale, căutând alte adrese de e-mail și trimițându-le mesaje infectate.
Vierme de MI	Viermi de client MI	Se răspândesc prin intermediul clienților de mesagerie instantanee. De obicei, acești viermi trimit mesaje care conțin un link către un fișier care conține o copie a viermelui pe un site Web, utilizând listele de contact ale utilizatorului. Atunci când utilizatorul descarcă și deschide fișierul, viermele se activează.
Vierme de IRC	Viermi de chat pe Internet	Se răspândesc prin Internet Relay Chats, sisteme de servicii care permit comunicarea în timp real cu alte persoane de pe Internet. Acești viermi publică un fișier cu o copie a lor sau un link către un fișier într-un chat Internet. Atunci când utilizatorul descarcă și deschide fișierul, viermele se activează.
Vierme de rețea	Viermi de rețea	Acești viermi se răspândesc prin rețele de computere. Spre deosebire de alte tipuri de viermi, un vierme tipic de rețea se răspândește fără participarea utilizatorului. El scanează rețeaua locală pentru computere care conțin programe cu vulnerabilități. Pentru aceasta, trimite un pachet de rețea într-un format special (un „exploit") care conține codul viermelui sau o parte din acesta. Dacă în rețea se găsește un computer „vulnerabil", el primește un astfel de pachet de rețea. Atunci când viermele pătrunde complet pe computer, se activează.
Vierme P2P	Viermi pentru rețele de partajare a fișierele	Se răspândesc prin intermediul rețelelor peer-to-peer de partajare a fișierelor. Pentru a se infiltra într-o rețea P2P, viermele se copie într-un director de partajare de fișiere care este de regulă localizat pe computerul utilizatorului. Rețeaua P2P afișează informații despre acest fișier, astfel încât utilizatorul poate „găsi" fișierul infectat prin rețea, asemenea oricărui alt fișier, și îl poate apoi descărca și deschide. Viermii mai sofisticați emulează protocolul de rețea al unei rețele P2P specifice: ei returnează răspunsuri pozitive la interogări de căutare și oferă spre descărcare copii ale lor.

Tip	Name	Descriere
Vierme	Alte tipuri de viermi	Alte tipuri de viermi includ: • Viermi care se răspândesc prin resurse de rețea. Utilizând funcțiile sistemului de operare, ei scanează după directoare de rețea disponibile, se conectează la computere prin Internet și încearcă să obțină acces complet la unitățile lor de hard disk. Spre deosebire de tipurile de viermi descrise mai sus, alte tipuri de viermi nu se activează singuri, ci atunci când utilizatorul deschide un fișier care conține o copie a viermelui. • Viermi care nu folosesc niciuna dintre metodele descrise în tabelul anterior pentru a se răspândi (de exemplu, ceii care se răspândesc prin telefoanele celulare).

- **Troieni (inclusiv programe ransomware)**

  Subcategoria: Troieni

  Nivel de pericol: Ridicat

  Spre deosebire de viermi și de viruși, troienii nu se multiplică singuri. De exemplu, ei penetrează un computer prin e-mail sau printr-un browser, atunci când utilizatorul vizitează o pagină Web infectată. Troienii se lansează cu participarea utilizatorului. Ei încep să execute acțiunile rău intenționate imediat după ce sunt lansați.

  Diverși troieni au comportamente diferite pe computerele infectate. Principala funcție a troienilor constă în blocarea, modificarea sau distrugerea informațiilor și dezactivarea unor computere sau rețele. Troienii pot primi și trimite fișiere, le pot executa, pot afișa mesaje pe ecran, pot solicita pagini Web, pot descărca și instala programe și pot reporni computerul.

  Hacker-ii folosesc adesea „seturi" de troieni diferiți.

  Tipurile de comportament de troian sunt descrise în tabelul următor.

  Tipuri de comportament de troian pe un computer infectat

Tip	Name	Descriere
Trojan-ArcBomb	Troieni – „bombe de arhivă"	Atunci când sunt dezarhivați, aceste arhive cresc în dimensiuni, până când funcționarea computerului este afectată. Atunci când utilizatorul încearcă să dezarhiveze o astfel de arhivă, computerul poate fi încetinit sau se poate bloca; unitatea de hard disc se umple cu date „goale". „Bombele de arhivă" sunt periculoase în special pe serverele de fișiere și de e-mail. Dacă serverul folosește un sistem automat pentru procesarea informațiilor primite, o „bombă de arhivă" poate opri serverul.
Backdoor	Troieni pentru administrare la distanță	Sunt considerați tipul cel mai periculos de troieni. Prin funcțiile lor se aseamănă cu aplicațiile de administrare la distanță care sunt instalate pe computere. Aceste programe se instalează pe computer fără a fi observate de utilizator, permițând intrusului să gestioneze computerul de la distanță.
Troian	Troieni	Includ următoarele tipuri de aplicații rău intenționate: • **Troieni clasici**. Aceștia execută doar funcții de bază ale troienilor: blochează, modifică sau distrug informații și dezactivează computere sau rețele. Ei nu au funcționalități avansate, spre deosebire de alte tipuri de troieni descrișii în tabel. • **Troieni versatili**. Aceste programe au caracteristici avansate, tipice pentru anumite tipuri de troieni.
Trojan-Ransom	Troieni de recompensă	Ei țin „ostatice" informațiile utilizatorului, modificându-le sau blocându-le sau afectând funcționarea computerului, astfel încât utilizatorul pierde capacitatea de a utiliza informațiile. Intrusul solicită o recompensă din partea utilizatorului, promițând că va trimite o aplicație pentru restaurarea performanței computerului și a datelor care au fost stocate pe acesta.
Trojan-Clicker	Troieni de tip clicker	Ei accesează pagini Web de pe computerul utilizatorului, fie prin trimiterea de comenzi către un browser, pe cont propriu, fie prin modificarea adreselor Web care sunt specificate în fișierele sistemului de operare. Prin utilizarea acestor programe, intrușii execută atacuri de rețea și sporesc numărul de vizite pe un site Web, sporind numărul de reclame banner afișate.
Trojan-Downloader	Troieni programe de descărcare	Ei accesează pagina Web a intrusului, descarcă de pe ea alte aplicații rău intenționate și le instalează pe computerul utilizatorului. Ei pot conține numele fișierului aplicației rău intenționate de descărcat sau îl pot primi de pe pagina Web accesată.

Tip	Name	Descriere
Trojan-Dropper	Troieni de tip Dropper	Ei conțin alți troieni, pe care îi pot depune și apoi instala pe unitatea de hard disc. Intruşii pot folosi programe de tipul Trojan Dropper în următoarele scopuri: • Instalarea unei aplicații rău intenționate fără a fi observat de utilizator: Programele de tipul Trojan Dropper nu afișează mesaje sau afișează mesaje false care informează, de exemplu, că există o eroare într-o arhivă sau o versiune incompatibilă a sistemului de operare. • Protejarea altei aplicații rău intenționate cunoscute de la detecție: nu toate software-urile antivirus pot detecta o aplicație rău intenționată din interiorul altei aplicații de tip Trojan Dropper.
Trojan-Notifier	Troieni de notificare	Ei informează un intrus că este accesibil computerul infectat, trimițând intrusului informații despre computer: adresa IP, numărul portului deschis sau adresa de e-mail. Ei comunică cu introdusul prin e-mail, FTP, accesând pagina Web a intrusului sau într-un alt mod. Programele de tip Trojan Notifier sunt folosite adesea în seturi care conțin mai mulți troieni. Ei îl notifică pe intrus că alți troieni s-au instalat cu succes pe computerul utilizatorului.
Trojan-Proxy	Proxyuri de troieni	Ei permit intrusului să acceseze anonim pagini Web folosind computerul utilizatorului; sunt adesea folosiți pentru a trimite spam.
Trojan-PSW	Programe dedicate sustragerii de parole	Programele care sustrag parole sunt un tip de troieni care fură conturi de utilizator, de exemplu date de înregistrare software. Acești troieni găsesc date confidențiale în fișierele de sistem și în registru și le trimit „atacatorului" prin e-mail, FTP, accesând pagina web a intrusului sau într-un alt mod. Unii dintre acești troieni sunt încadrați în tipuri separate descrise în acest tabel. Aceștia sunt Troieni care fură conturi bancare (Trojan-Banker), date de la utilizatori de clienți de mesagerie instantanee (Trojan-IM) și informații de la utilizatori de jocuri online (Trojan-GameThief).
Trojan-Spy	Spioni troieni	Ei îl spionează pe utilizator, colectând informații despre acțiunile pe efectuate de utilizator în timp ce acesta lucrează la computer. Ei pot intercepta date pe care utilizatorul le introduce de la tastatură, pot face copii de ecran sau pot colecta liste de aplicații active. După ce primesc informațiile, le transferă intrusului prin e-mail, FTP, accesând pagina Web a intrusului sau într-un alt mod.
Trojan-DDoS	Troieni atacatori de rețea	Ei trimit numeroase cereri de pe computerul utilizatorului către un server la distanță. Serverul nu dispune de resurse pentru a procesa toate cererile, astfel că nu mai funcționează (DoS sau Refuzare serviciu) Hackerii infectează adesea multe computere cu aceste programe, astfel încât pot utiliza computerele pentru a ataca simultan un singur server. Programe de tip Refuzare serviciu execută un atac de pe un singur computer, cu cunoștința utilizatorului. Programele de tip DDoS (Refuzare distribuită serviciu) execută atacuri distribuite din mai multe computere, fără a fi observate de utilizatorul computerului infectat.
Trojan-IM	Troieni care fură informații de la utilizatorii clienților de mesagerie instantanee	Fură numere de cont și parole ale utilizatorilor de clienți de mesagerie instantanee. Ei transferă datele intrusului prin e-mail, FTP, accesând pagina Web a intrusului sau într-un alt mod.
Rootkit	Rootkituri	Ei maschează alte aplicații rău intenționate și activitatea acestora, prelungind astfel persistența programelor rău intenționate în sistemul de operare. Ei pot, de asemenea, să ascundă fișiere, procese din memoria unui computer infectat sau chei de registru care execută aplicații rău intenționate. Rootkiturile pot masca schimbul de date între aplicații de pe computerul utilizatorului și alte computere din rețea.
Trojan-SMS	Troieni sub formă de mesaje SMS	Ele infectează telefoane celulare, trimițând mesaje SMS către numere de telefon cu tarif premium.
Trojan-GameThief	Troieni care fură informații de la utilizatorii de jocuri online	Ei fură acreditări de cont de la utilizatorii de jocuri online, după care trimit datele intrusului pe e-mail, prin FTP, accesând pagina Web a intrusului sau într-un alt mod.
Trojan-Banker	Troieni care furcă conturi bancare	Aceștia fură datele conturilor bancare sau datele pentru sistemele de plată electronică; trimit datele hackerului prin e-mail, FTP, accesând pagina web a hackerului sau folosind altă metodă.
Trojan-Mailfinder	Troieni care colectează adrese de e-mail	Ei colectează adrese de e-mail stocate pe iun computer și le trimit intrusului prin e-mail, FTP, accesând pagina Web a intrusului sau într-un alt mod. Intruşii pot trimite spam către adresele pe care le-au colectat.

- **Instrumente rău intenționate**

  Subcategoria: Instrumente periculoase

  Nivel de pericol: Mediu

Spre deosebire de alte tipuri de malware, instrumentele periculoase nu își execută acțiunile imediat după ce sunt pornite. Ele pot fi stocate în siguranță și pornite pe computerul utilizatorului. Intrușii folosesc adesea caracteristicile acestor programe pentru a crea viruși, viermi și troieni, să execute atacuri de rețea pe servere la distanță, să compromită computere sau să execute alte acțiuni rău intenționate.

Diverse caracteristici ale instrumentelor periculoase sunt grupate după tipurile descrise în tabelul următor.

Caracteristici ale instrumentelor periculoase

Tip	Name	Descriere
Constructor	Constructori	Permit crearea de noi viruși, viermi și troieni. Unele programe constructor dispun de o interfață bazată pe o fereastră standard în care utilizatorul poate selecta tipul aplicației rău intenționate de creat, modul de contracarare a depanatoarelor și alte caracteristici.
Dos	Atacuri de rețea	Ei trimit numeroase cereri de pe computerul utilizatorului către un server la distanță. Serverul nu dispune de resurse pentru a procesa toate cererile, astfel că nu mai funcționează (DoS sau Refuzare serviciu)
Exploit	Exploituri	Un *exploit* este un set de date sau un cod de program care folosește vulnerabilitățile aplicației în care este procesat, executând o acțiune rău intenționată pe un computer. De exemplu, un exploit poate scrie sau citi fișiere sau poate solicita pagini Web infectate. Diferite exploituri folosesc vulnerabilități ale diferitelor aplicații sau servicii de rețea. Deghizat ca pachet de rețea, un exploit este transmis prin rețea către numeroase computere, căutând computere cu servicii de rețea vulnerabile. Un exploit într-un fișier DOC folosește vulnerabilitățile editorului text. Atunci când utilizatorul deschide fișierul infectat, exploitul poate începe să execute acțiuni care sunt pre-programate de către hacker Un exploit care este încorporat într-un mesaj de e-mail caută vulnerabilități în orice client de e-mail. El poate începe să execute o acțiune rău intenționată imediat ce utilizatorul deschide mesajul infectat în clientul de e-mail respectiv. Viermii de rețea se răspândesc prin rețele, folosind exploituri. Exploiturile de tip Nuker sunt pachete de rețea care dezactivează computerele.
FileCryptor	Programe de criptare	Ele criptează alte aplicații rău intenționate, pentru a le ascunde de aplicația antivirus.
Flooder	Programe pentru „contaminarea" rețelelor.	Ele trimit numeroase mesaje prin canale de rețea. Acest tip de instrumente include, de exemplu, instrumente care contaminează camerele Internet Relay Chats. Instrumentele de tip flooder nu includ programe care „contaminează" canale care sunt folosite de clienți de e-mail, de mesagerie instantanee și de sisteme de comunicații mobile. Aceste programe se disting ca tipuri separate care sunt deschise în tabel (Email-Flooder, IM-Flooder și SMS-Flooder).
HackTool	Instrumente de hacking	Ele fac posibilă deturnarea computerului pe care sunt instalate sau atacarea altui computer (de exemplu, prin adăugarea de noi conturi de sistem fără permisiunea utilizatorului sau prin ștergerea jurnalelor de sistem pentru a ascunde urme ale prezenței în sistemul de operare). Acest tip de instrumente include unele sniffere care prezintă funcții rău intenționate, cum ar fi interceptarea parolelor. Snifferele sunt programe care permit vizionarea traficului de rețea.
Hoax	Hoaxuri	Ele îl alarmează pe utilizator cu mesaje care seamănă cu cele pentru viruși: ele pot să „detecteze un virus" într-un fișier care de fapt nu este infectat sau să îl notifice pe utilizator că discul a fost formatat, deși acest lucru nu s-a întâmplat în realitate.
Spoofer	Instrumente de contrafacere	Ele trimit mesaje și cereri de rețea cu o adresă a expeditorului falsă. Intrușii folosesc instrumente de tip Spoofer pentru a se deghiza în expeditori reali de mesaje, de exemplu.
VirTool	Instrumente care modifică aplicații rău intenționate	Ele permit modificarea altor programe malware, ascunzându-le de aplicațiile antivirus.
Email-Flooder	Programe care „contaminează" adrese de e-mail	Ele trimit numeroase mesaje către diferite adrese de e-mail, „contaminându-le" astfel. Un volum mare de mesaje primite îi împiedică pe utilizatori să vizualizeze mesaje utile din inboxurile lor.
IM-Flooder	Programe care „contaminează" traficul clienților de mesagerie instantanee	Ele îi inundă cu mesaje pe clienții aplicațiilor de mesagerie instantanee. Un volum mare de mesaje îi împiedică pe utilizatori să vizualizeze mesaje utile.
SMS-Flooder	Programe care „contaminează" traficul cu mesaje SMS	Ele trimit numeroase mesaje SMS către telefoane celulare.

- Adware

  Subcategoria: Software de advertising (Adware)

Nivel de pericol: Mediu

Programele adware afișează informații publicitare utilizatorului. Programele adware afișează reclame banner în interfețele altor programe și redirecționează interogările de căutare către pagini Web de publicitate. Unele dintre ele colectează informații de marketing despre utilizator și le trimit dezvoltatorului. Aceste informații pot include numele site-urilor Web care sunt vizitate de utilizator sau conținutul interogărilor de căutare ale utilizatorului. Spre deosebire de programele de tip Trojan-Spy, programele adware trimit aceste informații dezvoltatorului, cu permisiunea utilizatorului.

- **Programe de apelare automată**

  Subcategoria: Programe de apelare automată (Program de apelare).

  Nivel de pericol: Mediu

  Programele de apelare automată pot stabili în secret conexiuni telefonice folosind un modem.

- **Software legitim care poate fi utilizat de intruși pentru a aduce daune computerului sau datelor personale**

  Subcategoria: software legitim care poate fi utilizat de intruși pentru a aduce daune computerului sau datelor personale.

  Nivel de pericol: Mediu

  Majoritatea acestor aplicații sunt utile, astfel că mulți utilizatori le execută. Aceste aplicații includ clienți IRC, programe de apelare automată, programe de descărcare a fișierelor, programe de monitorizare a activității sistemului, utilitare de parolă și servere de Internet pentru FTP, HTTP și Telnet.

  Cu toate acestea, dacă intrușii obțin acces la aceste programe sau dacă le instalează pe computerul utilizatorului, unele dintre caracteristicile aplicației pot fi utilizate pentru a încălca securitatea.

  Aceste aplicații diferă după funcția lor; tipurile lor sunt descrise în tabelul următor.

Tip	Name	Descriere
Client-IRC	Clienți de chat Internet	Utilizatorii instalează aceste programe pentru a vorbi cu alte persoane în camere Internet Relay Chats. Intrușii îi folosesc pentru a răspândi malware.
Downloader	Programe pentru descărcare	Ele pot descărca fișiere din pagini Web în mod ascuns.
Monitor	Programe pentru monitorizare	Ele permit monitorizarea activității pe computerul pe care sunt instalate (urmărind ce aplicații sunt active și modul în care se modifică date cu aplicațiile care sunt instalate pe alte computere).
PSWTool	Programe de restaurare a parolelor	Ele permit vizualizarea și restaurarea parolelor uitate. Intrușii le instalează în mod secret pe computerele utilizatorilor, în același scop.
RemoteAdmin	Programe de administrare la distanță	Sunt folosite pe scară largă de administratorii de sistem. Aceste programe permit obținerea accesului la interfața unui computer la distanță pentru a o monitoriza și a o gestiona. Intrușii le instalează în mod secret pe computerele utilizatorilor, în același scop: acela de a monitoriza și a gestiona computere la distanță. Programele legitime de administrare la distanță diferă de troienii de tip Backdoor pentru administrare la distanță. Troienii au capacitatea de a penetra în sistemul de operare independent și de a se instala; programele legale nu pot face acest lucru.
Server-FTP	Servere FTP	Ele funcționează ca servere FTP. Intrușii le instalează pe computerul utilizatorului pentru a deschide accesul la distanță prin FTP.
Server-Proxy	Proxy server	Ele funcționează ca servere proxy. Intrușii le instalează pe computerul utilizatorului pentru a trimite spam în numele utilizatorului.
Server-Telnet	Servere Telnet	Ele funcționează ca servere Telnet. Intrușii le instalează pe computerul utilizatorului pentru a deschide accesul la distanță prin Telnet.

Tip	Name	Descriere
Server-Web	Servere Web	Ele funcționează ca servere Web. Intrușii le instalează pe computerul utilizatorului pentru a deschide accesul la distanță prin HTTP.
RiskTool	Instrumente pentru a lucra pe un computer local	Ele oferă utilizatorului opțiuni suplimentare atunci când lucrează pe propriul computer. Instrumentele permit utilizatorului să ascundă fișiere sau ferestre ale aplicațiilor active și să termine procese active.
NetTool	Instrumente de rețea	Ele oferă utilizatorului opțiuni suplimentare atunci când lucrează cu alte computere din rețea. Aceste instrumente permit repornirea computerelor, detectarea porturilor deschise și pornirea aplicațiilor instalate pe computere.
Client-P2P	Clienți de rețea P2P	Ei permit lucrul în rețele peer-to-peer. Ei pot fi folosite de intruși pentru a răspândi malware.
Client-SMTP	Clienți SMTP	Trimite mesaje e-mail fără știrea utilizatorului. Intrușii le instalează pe computerul utilizatorului pentru a trimite spam în numele utilizatorului.
WebToolbar	Bare de instrumente Web	Ele adaugă bare de instrumente la interfețele altor aplicații pentru a utiliza motoare de căutare.
FraudTool	Pseudo-programe	Ele se deghizează în alte tipuri de programe. De exemplu, există programe pseudo-antivirus care afișează mesaje despre detectarea de malware. Cu toate acestea, în realitate ele nu găsesc și nu dezinfectează nimic.

- **Obiecte arhivate a căror arhivare poate fi utilizată pentru a proteja un cod rău intenționat**

  Subcategoria: Fișiere arhivate care pot provoca daune.

  Nivel de pericol: Mediu.

  Fișierul este împachetat folosind un program de arhivare special, care este utilizat pentru arhivarea programelor malware: viruși, viermi, troieni. Kaspersky Endpoint Security scanează modulul de dezarhivare din arhive SFX (cu autoextragere).

  Pentru a ascunde malware-ul de la detectarea de către un antivirus, hackerii îl arhivează folosind programe de arhivare speciale. Experții Kaspersky au identificat programele de arhivare care sunt cele mai populare în rândul hackerilor.

- **Obiecte arhivate multiplu**

  Subcategoria: Fișiere arhivate multiplu.

  Nivel de pericol: Mediu.

  Fișierul este arhivat cu unul sau mai multe programe de arhivare de trei sau mai multe ori.

  Pentru a ascunde malware-ul de la detectarea de către un antivirus, hackerii pot arhiva un fișier de mai multe ori. Kaspersky Endpoint Security scanează fișierele arhivate.

În mod implicit, Kaspersky Endpoint Security detectează toate tipurile de obiecte. Recomandăm ca detectarea tuturor tipurilor de obiecte să fie păstrată activată pentru a îmbunătăți securitatea computerului. Dacă utilizezi utilitare interne pe care aplicația le detectează ca fiind rău intenționate, adaugă aceste utilitare la o listă de excludere, dar nu dezactiva detectarea întregului tip de obiecte.

Cum se selectează tipurile de obiecte detectate în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați **Policies**.
3. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

4. În fereastra politicii, selectați **Setări generale** → **Excluderi și tipuri de obiecte**.

5. În blocul **Tipuri de obiecte detectate**, fă clic pe butonul **Setări**.

6. În fereastra care se deschide, bifează casetele de selectare din dreptul tipurilor de obiecte pe care dorești să le detecteze Kaspersky Endpoint Security.

7. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se selectează tipurile de obiecte detectabile în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați fila **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **General Settings** → **Detection Settings**.

5. În blocul **Detection of other types of objects**, bifează casetele de selectare din dreptul tipurilor de obiecte pe care dorești să le detecteze Kaspersky Endpoint Security.

6. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

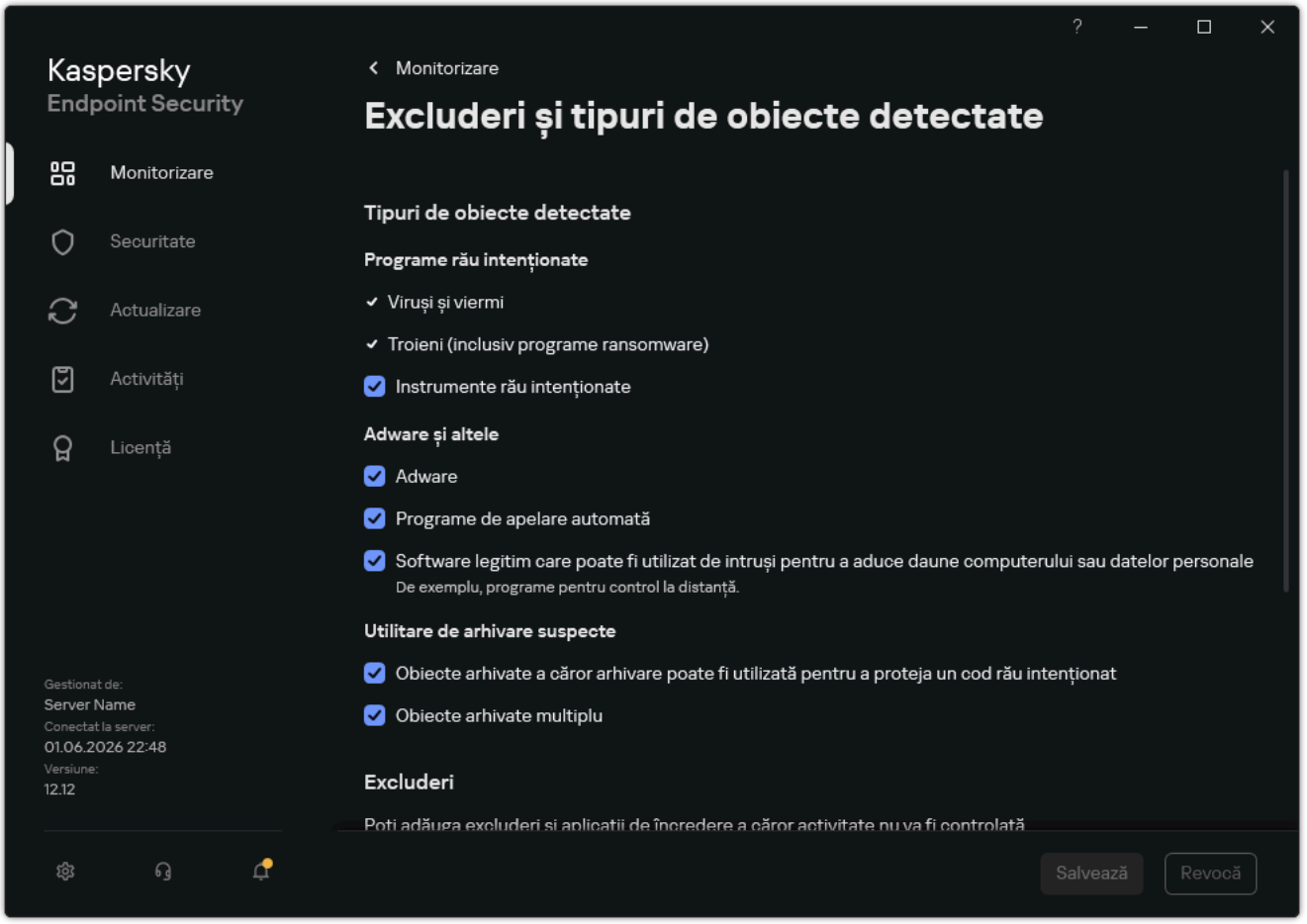
Cum se selectează tipurile de obiecte detectabile în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Setări generale** → **Excluderi și tipuri de obiecte detectate**.

3. În blocul **Tipuri de obiecte detectate**, bifează casetele de selectare din dreptul tipurilor de obiecte pe care dorești să le detecteze Kaspersky Endpoint Security.

4. Salvați-vă modificările.



Tipuri de obiecte detectabile

Editarea listei de aplicații de încredere

Lista de aplicații de încredere este o listă de aplicații pentru care Kaspersky Endpoint Security nu monitorizează activitatea cu fișierele și activitatea în rețea (inclusiv activitatea rău intenționată) și nici accesul la registrul de sistem. În mod implicit, Kaspersky Endpoint Security monitorizează obiectele care sunt deschise, executate sau salvate de orice proces al unei aplicații și controlează activitatea tuturor aplicațiilor și traficul în rețea generat de acestea. După ce o aplicație este adăugată la lista de aplicații de încredere, Kaspersky Endpoint Security oprește monitorizarea activității aplicației.

Diferența dintre excluderile de la scanare și aplicațiile de încredere este că, pentru excluderi, Kaspersky Endpoint Security nu scanează fișierele, în timp ce pentru aplicațiile de încredere nu controlează procesele inițiate. Dacă o aplicație de încredere creează un fișier rău intenționat într-un director care nu este inclus în excluderile de la scanare, Kaspersky Endpoint Security va detecta fișierul și va elimina amenințarea. Dacă directorul este adăugat la excluderi, Kaspersky Endpoint Security va omite acest fișier.

De exemplu, dacă presupui obiectele utilizate de aplicația Microsoft Windows Notepad standard ca fiind sigure, ceea ce înseamnă că ai încredere în această aplicație, poți adăuga Microsoft Windows Notepad în lista de aplicații de încredere, astfel încât obiectele utilizate de această aplicație nu sunt monitorizate. Acest lucru va crește performanța computerului, ceea ce este deosebit de important atunci când utilizați aplicații de pe server.

În plus, anumite acțiuni care sunt clasificate de către Kaspersky Endpoint Security ca fiind suspecte este posibil să fie sigure în contextul operațional pentru o serie de aplicații. De exemplu, interceptarea textul introdus de la tastatură este un proces de rutină pentru programele de comutare automată a structurii tastaturii (cum ar fi Punto Switcher). Pentru a ține cont de caracteristicile specifice ale unor astfel de aplicații și pentru a exclude activitatea lor din monitorizare, îți recomandăm să adaugi aceste aplicații în lista de aplicații de încredere.

Aplicațiile de încredere ajută la evitarea problemelor de compatibilitate între Kaspersky Endpoint Security și alte aplicații (de exemplu, problema scanării duble a traficului de rețea al unui computer terț de către Kaspersky Endpoint Security și de către o altă aplicație antivirus).

În același timp, fișierul executabil și procesele aplicației de încredere sunt scanate în continuare după viruși și alte programe malware. O aplicație poate fi exclusă complet de la scanarea Kaspersky Endpoint Security cu ajutorul excluderilor de la scanare.

Modificarea listei de aplicații de încredere poate fi blocată de proprietățile politicii principale. Pentru a modifica lista, trebuie să permiteți modificarea setărilor zonei de încredere în Web Console („lacătul" trebuie să fie deblocat).

Zonele de încredere sunt grupate diferit în Consola de administrare (MMC) și în Web Console. De asemenea, modul în care se împiedică modificarea parametrilor zonei de încredere este diferit („lacăte" diferite). Vă recomandăm să utilizați exclusiv Web Console pentru gestionarea aplicației. În cazul în care configurați zona de încredere pe console diferite, este posibil ca plug-inul de gestionare să reseteze „lacătul" la starea implicită.

Cum se adaugă o aplicație în lista de încredere din Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Setări generale** → **Excluderi și tipuri de obiecte**.
4. În blocul **Excluderi de la scanare și aplicații de încredere** → **Aplicații de încredere**, fă clic pe butonul **Setări**.

   Acest lucru va deschide o fereastră care conține lista aplicațiilor de încredere.
5. Bifați caseta de selectare **Îmbină valorile în momentul moștenirii** dacă doriți să creați o listă consolidată de aplicații de încredere pentru toate computerele companiei. Listele de aplicații de încredere din politicile principale și secundare vor fi îmbinate. Listele vor fi îmbinate dacă funcția de îmbinare a valorilor în momentul moștenirii este activată. Aplicațiile de încredere din politica principală sunt afișate în politicile secundare într-o vizualizare numai citire. Nu este posibilă modificarea sau ștergerea aplicațiilor de încredere ale politicii principale.
6. Bifați caseta de selectare **Permite utilizarea aplicațiilor de încredere locale** dacă doriți să permiteți utilizatorului să creeze o listă locală de aplicații de încredere. În acest fel, un utilizator își poate crea propria listă locală de aplicații de încredere pe lângă lista generală a aplicațiilor de încredere generate în politică. Un administrator poate utiliza Kaspersky Security Center pentru a vizualiza, adăuga, edita sau șterge elemente de listă din proprietățile computerului.

   În cazul în care caseta de selectare este debifată, utilizatorul poate accesa doar lista generală a aplicațiilor de încredere generate în politică. De asemenea, dacă această casetă de selectare este debifată, Kaspersky Endpoint Security ascunde lista consolidată a aplicațiilor de încredere în interfața de utilizator a aplicației.

7. Faceți clic pe **Adaugă** și selectați o acțiune:

- **Categorie**. Puteți grupa aplicațiile de încredere în categorii separate. Pentru a crea o categorie nouă, introduceți numele categoriei și adăugați cel puțin o aplicație de încredere la categorie.
- **Excludere nouă**. Kaspersky Endpoint Security adaugă o nouă aplicație de încredere la rădăcina listei.
- **Selectează excluderea din listă**. Pentru a configura rapid Kaspersky Endpoint Security pe serverele SQL, serverele Microsoft Exchange și System Center Configuration Manager, aplicația include *aplicații de încredere predefinite*. De asemenea, au fost adăugate aplicații de încredere predefinite pentru a sprijini configurarea aplicațiilor în mediile virtuale Citrix și VMware. Trebuie să selectați aplicații de încredere predefinite, în funcție de scopul serverului protejat.
- **Excludere nouă în categoria selectată**. Pentru a adăuga o nouă aplicație de încredere la o anumită categorie, selectați o categorie.

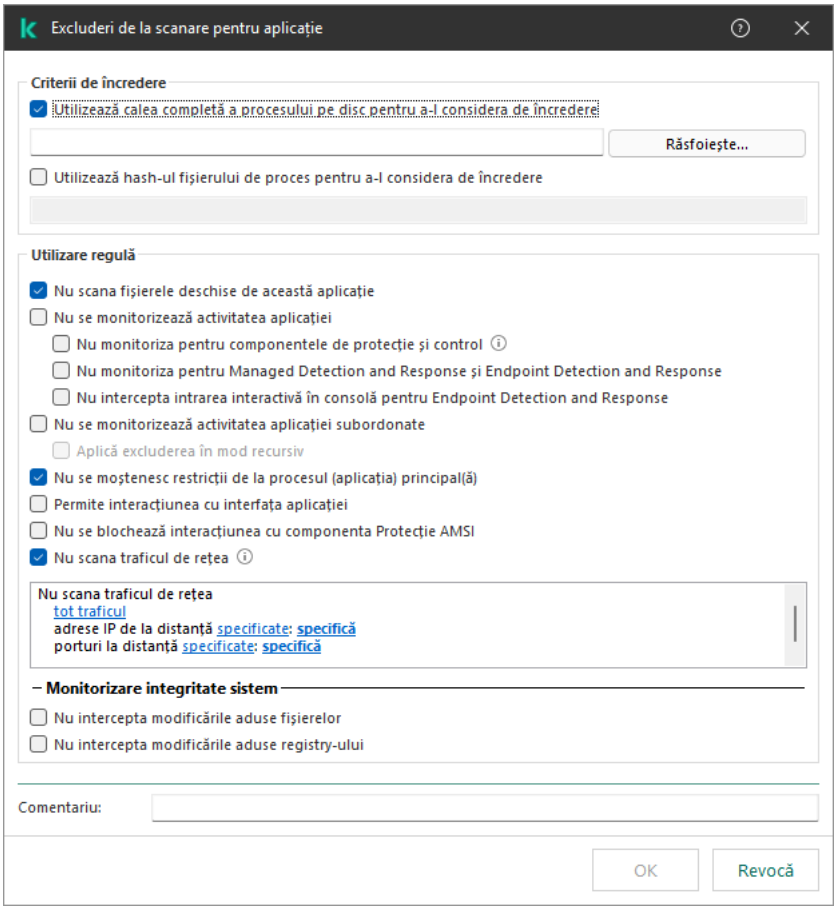
8. Selectează criteriile de încredere:

- **Utilizează calea completă a procesului pe disc pentru a-l considera de încredere**. Introdu calea către fișierul executabil al aplicației de încredere.

  Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști.

  Kaspersky Endpoint Security tratează numele fișierului unei aplicații de încredere ca fiind sensibil la majuscule și minuscule. Dacă numele fișierului pe care îl introduci conține majuscule sau minuscule care nu corespund, Kaspersky Endpoint Security nu va recunoaște aplicația de încredere.
- **Utilizează hash-ul fișierului de proces pentru a-l considera de încredere**.

Kaspersky Endpoint Security nu acceptă variabila de mediu `%userprofile%` atunci când se generează o listă de aplicații de încredere în consola Kaspersky Security Center. Pentru a aplica intrarea tuturor conturilor de utilizatori, puteți utiliza caracterul * (de exemplu, `C:\Users\*\Documents\File.exe`). Ori de câte ori adăugați o variabilă de mediu, trebuie să reporniți aplicația.



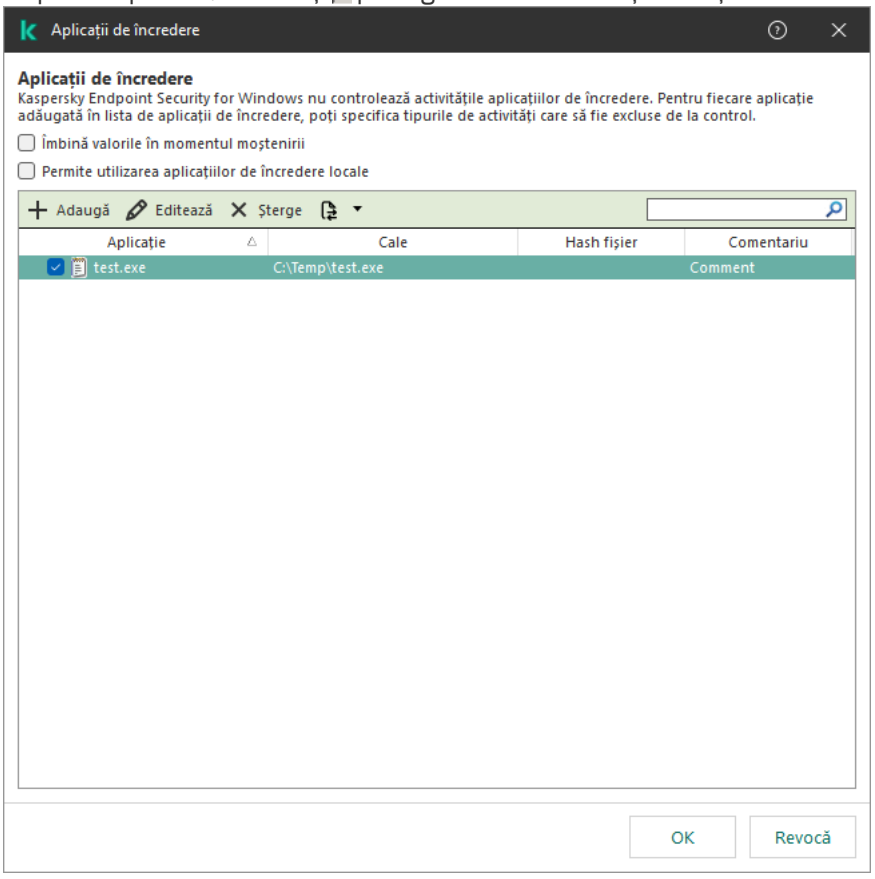
Setările aplicației de încredere

9. Configurați setările avansate pentru aplicația de încredere (consultați tabelul de mai jos).

10. Fă clic pe **OK**.

    Noua aplicație de încredere va fi adăugată în listă. Puteți exclude oricând o aplicație din zona de încredere folosind caseta de selectare de lângă obiect.

11. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.



Lista aplicațiilor de încredere

Cum se adaugă o aplicație în lista de încredere din Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesează secțiunea **Trusted Zone**.
5. În fereastra care se deschide, fă clic pe linkul **Applications**.

   Acest lucru va deschide o fereastră care conține lista aplicațiilor de încredere.
6. Bifați caseta de selectare **Merge values when inheriting** dacă doriți să creați o listă consolidată de aplicații de încredere pentru toate computerele companiei. Listele de aplicații de încredere din politicile principale și secundare vor fi îmbinate. Listele vor fi îmbinate dacă funcția de îmbinare a valorilor în momentul moștenirii este activată. Aplicațiile de încredere din politica principală sunt afișate în politicile secundare într-o vizualizare numai citire. Nu este posibilă modificarea sau ștergerea aplicațiilor de încredere ale politicii principale.
7. Bifați caseta de selectare **Allow use of local exclusions** dacă doriți să permiteți utilizatorului să creeze o listă locală de aplicații de încredere. În acest fel, un utilizator își poate crea propria listă locală de aplicații de încredere pe lângă lista generală a aplicațiilor de încredere generate în politică. Un administrator poate utiliza Kaspersky Security Center pentru a vizualiza, adăuga, edita sau șterge elemente de listă din proprietățile computerului.

   În cazul în care caseta de selectare este debifată, utilizatorul poate accesa doar lista generală a aplicațiilor de încredere generate în politică. De asemenea, dacă această casetă de selectare este debifată, Kaspersky Endpoint Security ascunde lista consolidată a aplicațiilor de încredere în interfața de utilizator a aplicației.

8. Faceți clic pe **Add** și selectați o acțiune:

   - **Category**. Puteți grupa aplicațiile de încredere în categorii separate. Pentru a crea o categorie nouă, introduceți numele categoriei și adăugați cel puțin o aplicație de încredere la categorie.
   - **New exclusion**. Kaspersky Endpoint Security adaugă o nouă aplicație de încredere la rădăcina listei.
   - **Select exclusion from list**. Pentru a configura rapid Kaspersky Endpoint Security pe serverele SQL, serverele Microsoft Exchange și System Center Configuration Manager, aplicația include *aplicații de încredere predefinite*. De asemenea, au fost adăugate aplicații de încredere predefinite pentru a sprijini configurarea aplicațiilor în mediile virtuale Citrix și VMware. Trebuie să selectați aplicații de încredere predefinite, în funcție de scopul serverului protejat.

   Pentru a adăuga o nouă aplicație de încredere la o anumită categorie, bifați caseta de selectare de lângă categoria respectivă și selectați opțiunea **New exclusion**.

9. Selectează criteriile de încredere:

   - **Path to the file or folder**. Introdu calea către fișierul executabil al aplicației de încredere.

     Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști.

     Kaspersky Endpoint Security tratează numele fișierului unei aplicații de încredere ca fiind sensibil la majuscule și minuscule. Dacă numele fișierului pe care îl introduci conține majuscule sau minuscule care nu corespund, Kaspersky Endpoint Security nu va recunoaște aplicația de încredere.

   - **Application hash**.

   > Kaspersky Endpoint Security nu acceptă variabila de mediu %userprofile% atunci când se generează o listă de aplicații de încredere în consola Kaspersky Security Center. Pentru a aplica intrarea tuturor conturilor de utilizatori, puteți utiliza caracterul `*` (de exemplu, `C:\Users\*\Documents\File.exe`). Ori de câte ori adăugați o variabilă de mediu, trebuie să reporniți aplicația.

10. Configurați setările avansate pentru aplicația de încredere (consultați tabelul de mai jos).

11. Fă clic pe **OK**.

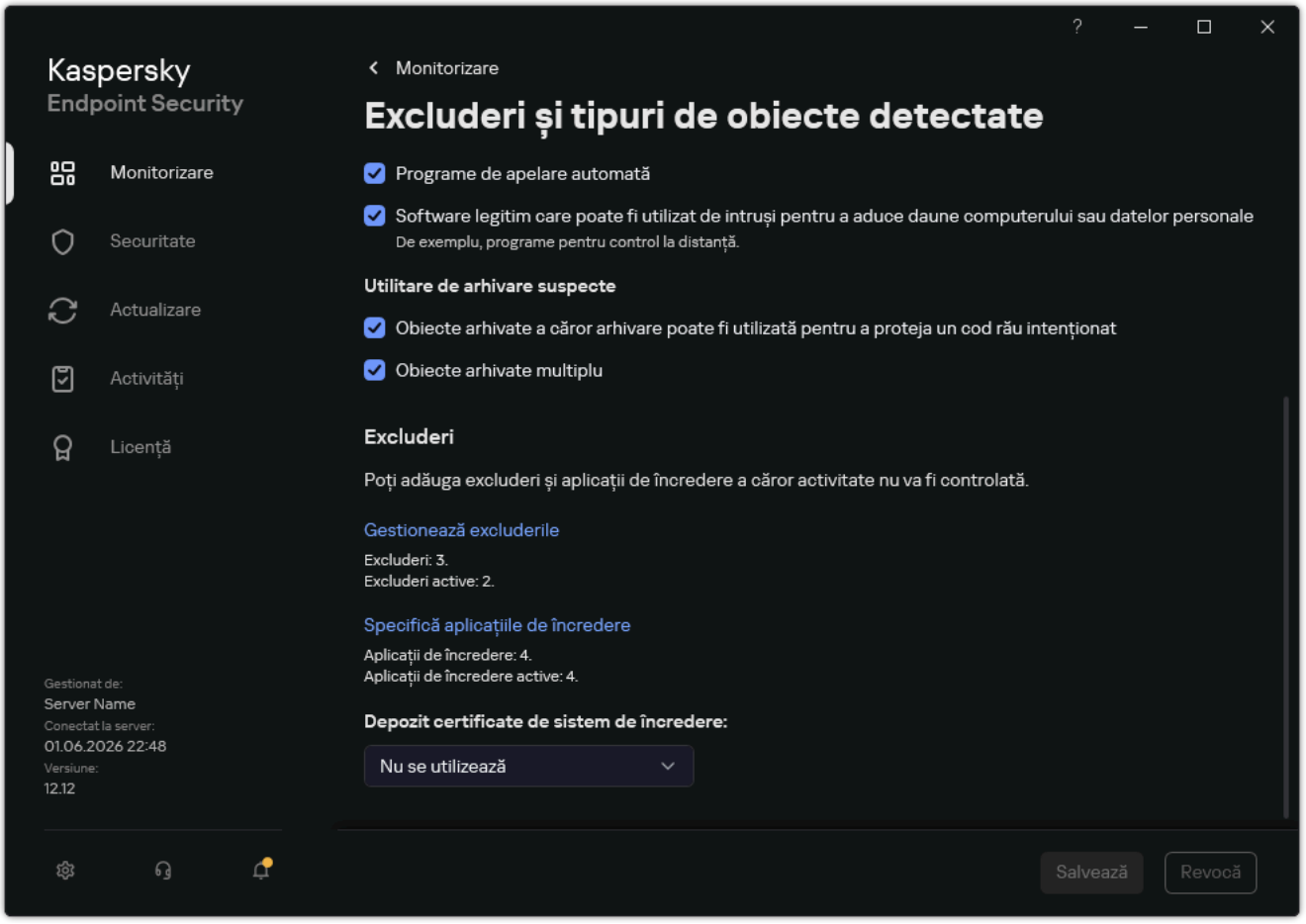
    Noua aplicație de încredere va fi adăugată în listă. Puteți exclude oricând o aplicație din zona de încredere folosind caseta de selectare din coloana **Status**.

12. Salvați-vă modificările.

Cum se adaugă o aplicație în lista de încredere din interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Setări generale → Excluderi și tipuri de obiecte detectate**.
3. În blocul **Excluderi**, faceți clic pe linkul **Specifică aplicațiile de încredere**.

Kaspersky Endpoint Security ascunde lista consolidată a aplicațiilor de încredere în interfața de utilizator a aplicației dacă configurarea aplicațiilor de încredere este blocată de administrator în consolă (simbolul „lăcăt închis") și aplicațiile locale de încredere sunt interzise (caseta de selectare **Permite utilizarea aplicațiilor de încredere locale** este debifată).



Setări pentru excluderi

4. Faceți clic pe **Adaugă** și selectați o acțiune:

   - **Categorie**. Puteți grupa aplicațiile de încredere în categorii separate. Pentru a crea o categorie nouă, introduceți numele categoriei și adăugați cel puțin o aplicație de încredere la categorie.
   - **Excludere nouă**. Kaspersky Endpoint Security adaugă o nouă aplicație de încredere la rădăcina listei.
   - **Selectează excluderea din listă**. Pentru a configura rapid Kaspersky Endpoint Security pe serverele SQL, serverele Microsoft Exchange și System Center Configuration Manager, aplicația include *aplicații de încredere predefinite*. De asemenea, au fost adăugate aplicații de încredere predefinite pentru a sprijini configurarea aplicațiilor în mediile virtuale Citrix și VMware. Trebuie să selectați aplicații de încredere predefinite, în funcție de scopul serverului protejat.

   Pentru a adăuga o nouă aplicație de încredere la o anumită categorie, bifați caseta de selectare de lângă categoria respectivă și selectați opțiunea **Excludere nouă**.

5. Selectează criteriile de încredere:

   - **Utilizează calea completă a procesului pe disc pentru a-l considera de încredere**. Introdu calea către fișierul executabil al aplicației de încredere.

     Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști.

Kaspersky Endpoint Security tratează numele fișierului unei aplicații de încredere ca fiind sensibil la majuscule și minuscule. Dacă numele fișierului pe care îl introduci conține majuscule sau minuscule care nu corespund, Kaspersky Endpoint Security nu va recunoaște aplicația de încredere.

- **Utilizează hash-ul fișierului de proces pentru a-l considera de încredere**.

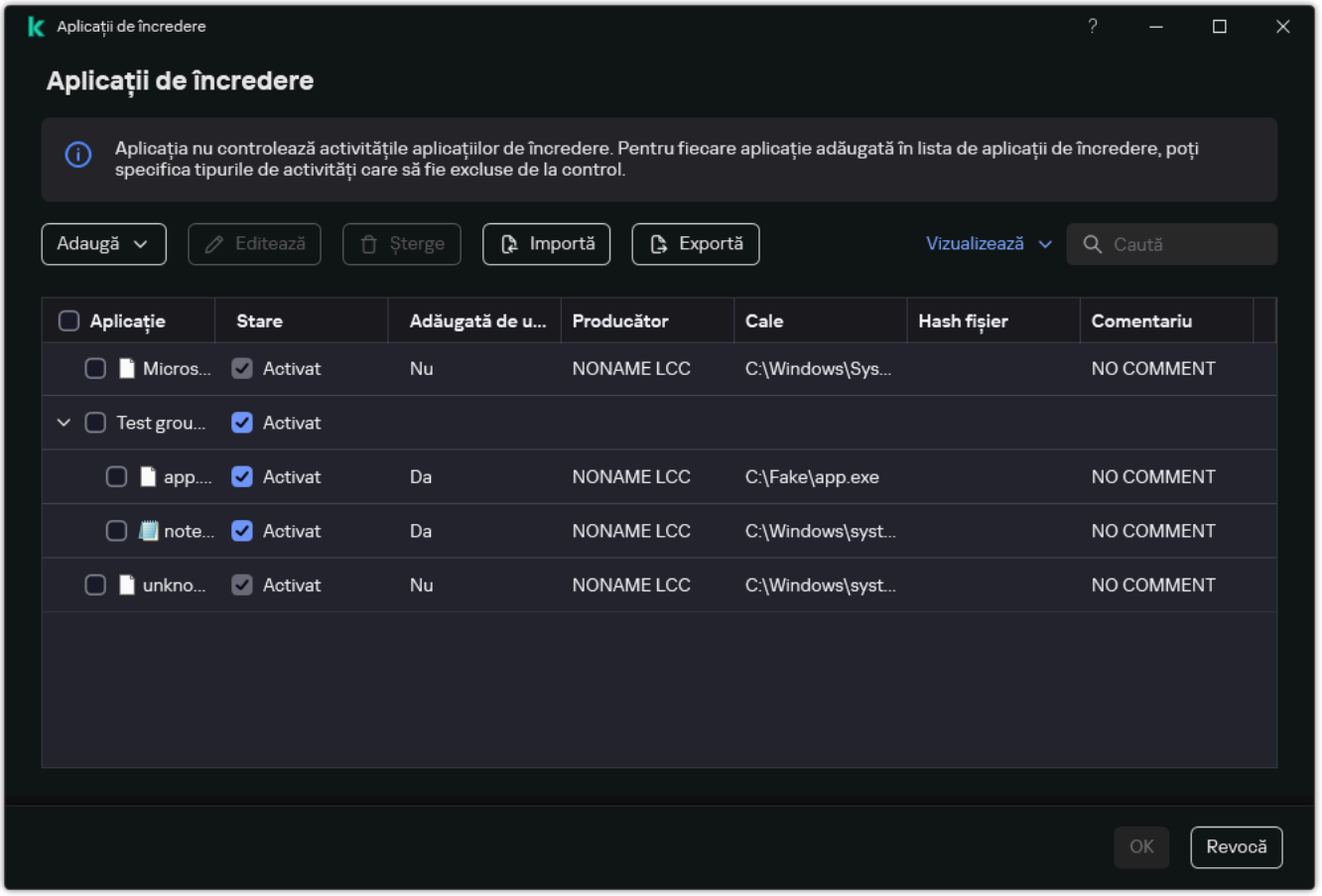
Kaspersky Endpoint Security acceptă variabilele de mediu și convertește calea din interfața locală a aplicației. Cu alte cuvinte, dacă introduceți calea fișierului `%userprofile%\Documents\File.exe`, se adaugă o înregistrate `C:\Users\Fred123\Documents\File.exe` în interfața locală a aplicației pentru utilizatorul Fred123. Astfel, Kaspersky Endpoint Security ignoră programul de încredere `File.exe` pentru ceilalți utilizatori. Pentru a aplica intrarea tuturor conturilor de utilizatori, puteți utiliza caracterul `*` (de exemplu, `C:\Users\*\Documents\File.exe`). Ori de câte ori adăugați o variabilă de mediu, trebuie să reporniți aplicația.

6. În fereastra de proprietăți a aplicației de încredere, configurați setările avansate.

7. Fă clic pe **OK**.

   Noua aplicație de încredere va fi adăugată în listă. Puteți exclude oricând o aplicație din zona de încredere folosind caseta de selectare din coloana **Stare**.

8. Salvați-vă modificările.



Lista aplicațiilor de încredere

Parametru	Descriere
Nu scana fișierele deschise de această aplicație	Toate fișierele deschise de aplicația de încredere sunt excluse de la scanări de Kaspersky Endpoint Security. De exemplu, dacă utilizați aplicații pentru copierea de rezervă a fișierelor, această caracteristică ajută la reducerea consumului de resurse de către Kaspersky Endpoint Security.
Nu monitoriza activitatea aplicației	Kaspersky Endpoint Security nu va monitoriza activitatea fișierelor și a rețelei aplicației în sistemul de operare. Poți configura monitorizarea activității aplicației pentru diferite componente ale Kaspersky Endpoint Security: • **Nu monitoriza pentru componentele de protecție și control**. Activitatea aplicației este monitorizată de următoarele componente: Behavior Detection, Exploit Prevention, Host Intrusion Prevention, Remediation Engine și Firewall. • **Nu monitoriza pentru Managed Detection and Response și Endpoint Detection and Response**. Activitatea aplicației este monitorizată de MDR Agent încorporat și EDR (KATA) Agent încorporat. • **Nu intercepta intrarea interactivă în consolă pentru Endpoint Detection and Response**. Kaspersky Endpoint Security nu trimite date de telemetrie despre gestionarea aplicației pe consolă. Datele de telemetrie sunt folosite de Kaspersky Anti Targeted Attack Platform (EDR).
Nu monitoriza activitatea aplicației subordonate	Kaspersky Endpoint Security nu va monitoriza activitatea fișierelor sau activitatea de rețea a aplicațiilor care sunt pornite de această aplicație. Poți aplica excluderea]n mod recursiv. Astfel ca aplicația să nu monitorizeze activitatea întregului lanț de aplicații secundare.
Nu moșteni restricții de la procesul principal (aplicația principală)	Restricțiile configurate pentru procesul părinte nu vor fi aplicate de Kaspersky Endpoint Security unui proces copil. Procesul părinte este inițiat de o aplicație pentru care sunt configurate drepturile aplicației (Host Intrusion Prevention) și regulile de rețea ale aplicației (Firewall).
Nu monitoriza activitatea aplicației subordonate	Kaspersky Endpoint Security nu va monitoriza activitatea fișierelor sau activitatea de rețea a aplicațiilor care sunt pornite de această aplicație. Poți aplica excluderea]n mod recursiv. Astfel ca aplicația să nu monitorizeze activitatea întregului lanț de aplicații secundare.
Permite interacțiunea cu interfața aplicației	Autoprotecția Kaspersky Endpoint Security blochează toate încercările de a gestiona serviciile aplicațiilor de pe un computer la distanță. Dacă această casetă de selectare este bifată, aplicația cu acces la distanță are permisiunea de a gestiona setările Kaspersky Endpoint Security prin interfața Kaspersky Endpoint Security.
Nu bloca interacțiunea cu componenta Protecție AMSI	Kaspersky Endpoint Security nu va monitoriza cererile aplicației de încredere pentru ca obiectele să fie scanate de componenta de protecție AMSI.
Nu scana traficul de rețea	Traficul de rețea inițiat de aplicație va fi exclus din scanări de Kaspersky Endpoint Security. Puteți exclude de la scanări fie traficul, fie doar traficul criptat. De asemenea, puteți exclude adresele IP și numerele de port individuale din scanări. Kaspersky Endpoint Security versiunea 14.0 sau o versiune anterioară nu acceptă excluderea traficului de rețea dacă este specificat un hash pentru o aplicație de încredere în loc de o cale.
Nu intercepta modificările aduse fișierelor *(disponibil numai în consola Kaspersky Security Center)*	Kaspersky Endpoint Security nu monitorizează modificările fișierelor din domeniul de aplicare al monitorizării pentru Monitorizare integritate sistem. Aplicația aplică excluderea tuturor modurilor opțiunii Monitorizare integritate sistem: Monitorizare în timp real a integrității sistemului și Verificare la cerere a integrității sistemului.
Nu intercepta modificările aduse registry-ului *(disponibil numai în consola Kaspersky Security Center)*	Kaspersky Endpoint Security nu monitorizează modificările cheilor de registry din domeniul de aplicare al monitorizării pentru Monitorizare integritate sistem. Aplicația aplică excluderea tuturor modurilor opțiunii Monitorizare integritate sistem: Monitorizare în timp real a integrității sistemului și Verificare la cerere a integrității sistemului.
Comentariu	Dacă este necesar, puteți oferi un scurt comentariu pentru aplicația de încredere. Comentariile simplifică căutările și sortarea aplicațiilor de încredere.
Stare	Starea aplicației de încredere: • Starea **Activă** înseamnă că aplicația este în zona de încredere. • Starea **Inactivă** înseamnă că aplicația este exclusă din zona de încredere.

Crearea unei zone de încredere locale

Utilizatorul își poate crea acum propria zonă de încredere locală pentru un anumit computer. În acest fel, utilizatorul își poate crea propriile liste locale de excluderi și aplicații de încredere, pe lângă zona de încredere generală dintr-o politică. Un administrator poate permite sau bloca utilizarea excluderilor locale sau a aplicațiilor locale de încredere în setările politicii. Pentru a face acest lucru, utilizați casetele de selectare **Permite utilizarea excluderilor locale** și **Permite utilizarea aplicațiilor de încredere locale** din secțiunea **Excluderi** a politicii.

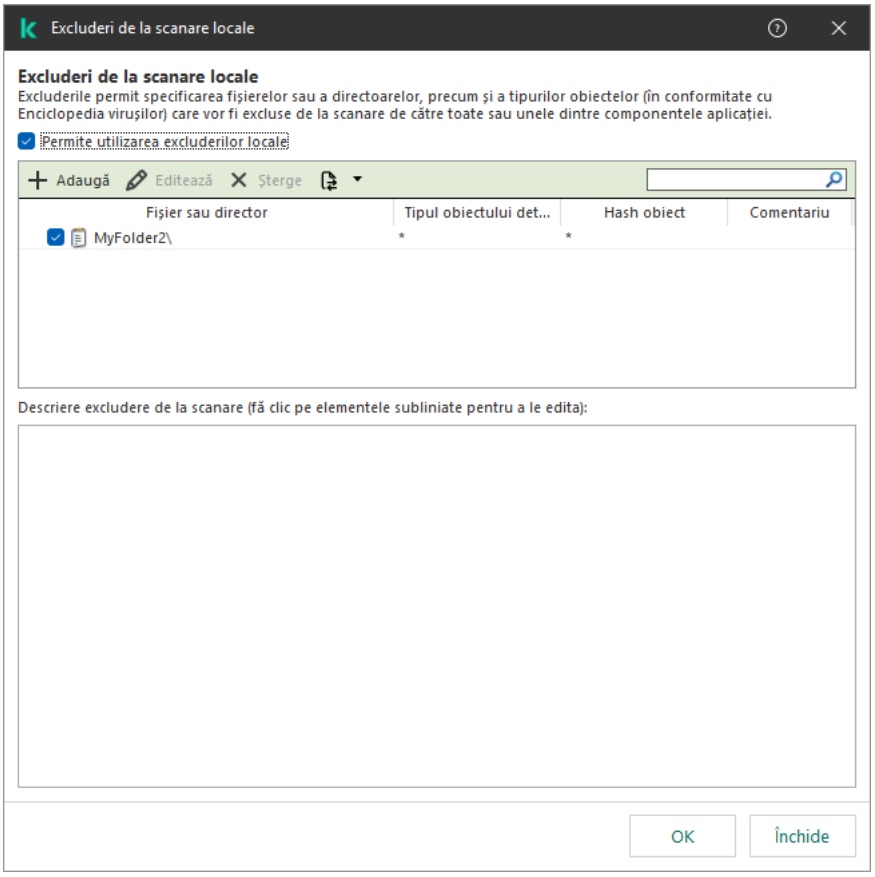
Dacă crearea unei zone de încredere locale este permisă de un administrator, utilizatorul poate adaugă propriile excluderi de la scanare și aplicații de încredere în interfața cu utilizatorul a aplicației. În același timp, utilizatorul nu are permisiuni de modificare sau ștergere a obiectelor din zona de încredere configurată în politică. De asemenea, administratorul poate vizualiza, adăuga, modifica sau șterge elemente din listă în consola Kaspersky Security Center dacă trebuie adăugate excluderi pentru un computer individual.

Kaspersky Endpoint Security ascunde listele cu excluderile de la scanare și cu aplicațiile de încredere în interfața de utilizator a aplicației dacă configurarea zonei de încredere este blocată de administrator în consolă (simbol (simbolul „lacăt închis") și excluderile de la scanare locale și aplicațiile de încredere sunt interzise.

Cum se adaugă un obiect în lista de încredere din Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Managed devices** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectează fila **Devices**.
4. Fă dublu clic pentru a deschide fereastra cu proprietățile computerului.
5. În fereastra cu proprietățile computerului, selectează secțiunea **Applications**.
6. În lista de aplicații Kaspersky instalate pe computer, selectează **Kaspersky Endpoint Security for Windows (14.1)** și fă dublu clic pentru a deschide proprietățile aplicației.
7. În fereastra cu setările aplicației, selectați **Setări generale → Excluderi și tipuri de obiecte**.
8. În blocul **Excluderi de la scanare și aplicații de încredere → Excluderi de la scanare locale**, fă clic pe butonul **Setări**.

Acest lucru va deschide o fereastră care conține lista excluderilor locale.



Setări zonă de încredere

9. Faceți o listă cu excluderile de la scanare locale.

   Regulile pentru crearea excluderilor de la scanare locale sunt aceleași ca și pentru excluderile generale. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele * și ? la introducerea unei măști.

10. În blocul **Excluderi de la scanare și aplicații de încredere** → **Aplicații de încredere locale**, fă clic pe butonul **Setări**.

    Acest lucru va deschide o fereastră care conține o listă cu aplicațiile de încredere locale.

11. Faceți o listă cu aplicațiile de încredere locale.

    Regulile pentru adăugarea aplicațiilor la lista de aplicații de încredere locale sunt aceleași cu regulile pentru adăugarea acestora la lista generală. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele * și ? la introducerea unei măști.

12. Salvați-vă modificările.

Cum se adaugă un obiect în zona de încredere locală din Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Assets (Devices)**.
2. Fă clic pe numele computerului pe care dorești să permiți unui utilizator să efectueze o acțiune blocată.
3. Selectați fila **Applications**.
4. Fă clic pe **Kaspersky Endpoint Security for Windows**.

   Se vor deschide setările locale pentru aplicație.

5. Selectați fila **Application settings**.

6. În fereastra cu setările aplicației, selectați **General settings** → **Exclusions and types of detected objects**.
7. În blocul **Scan exclusions and trusted applications**, faceți clic pe linkul **Local scan exclusions**.
8. Faceți o listă cu excluderile de la scanare locale.

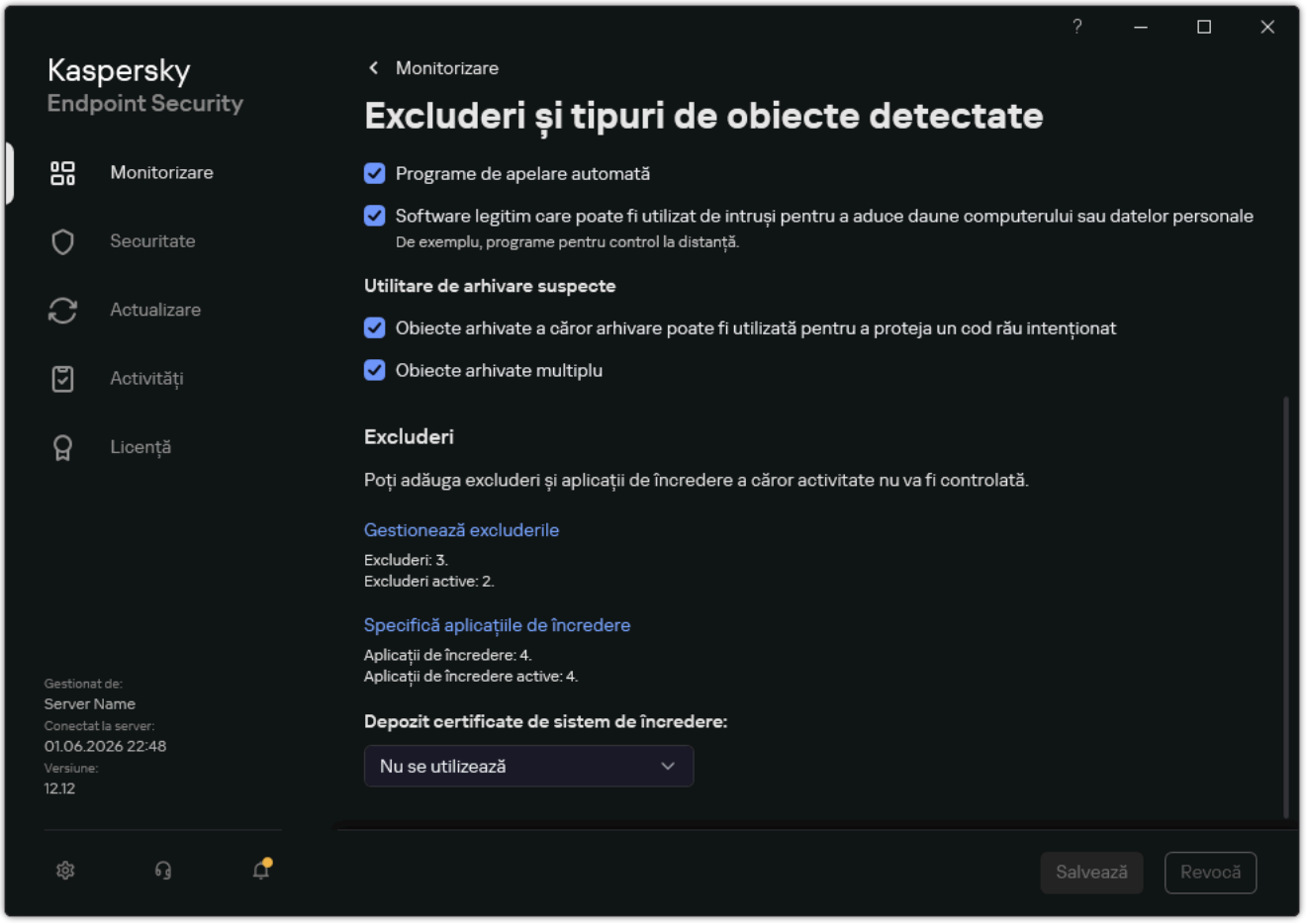
   Regulile pentru crearea excluderilor locale sunt aceleași cu regulile pentru crearea excluderilor generale. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele * și ? la introducerea unei măști.
9. În blocul **Scan exclusions and trusted applications**, faceți clic pe linkul **Local trusted applications**.
10. Faceți o listă cu aplicațiile de încredere locale.

    Regulile pentru adăugarea aplicațiilor la lista de aplicații de încredere locale sunt aceleași cu regulile pentru adăugarea acestora la lista generală. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele * și ? la introducerea unei măști.
11. Salvați-vă modificările.

Cum se creează o excludere de la scanare locală în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Setări generale** → **Excluderi și tipuri de obiecte detectate**.
3. În blocul **Excluderi**, faceți clic pe linkul **Gestionează excluderile**.

Kaspersky Endpoint Security ascunde lista excluderilor de la scanare în interfața de utilizator a aplicației dacă configurarea excluderilor de la scanare este blocată de administrator în consolă (simbolul „lacăt închis") și excluderile de la scanare locale sunt interzise (caseta de selectare **Permite utilizarea excluderilor locale** este debifată).



Setări pentru excluderi

4. Faceți clic pe **Adaugă** și selectați o acțiune:

   - **Categorie**. Puteți grupa excluderile de la scanare în categorii separate. Pentru a crea o categorie nouă, introduceți numele categoriei și adăugați cel puțin o excludere de la scanare la categorie.
   - **Excludere nouă**. Kaspersky Endpoint Security adaugă o nouă excludere de la scanare la rădăcina listei.
   - **Selectează excluderea din listă**. Pentru a configura rapid Kaspersky Endpoint Security pe serverele SQL, serverele Microsoft Exchange și System Center Configuration Manager, aplicația include *excluderi de la scanare predefinite*. De asemenea, au fost adăugate excluderi de la scanare predefinite pentru a sprijini configurarea aplicațiilor în mediile virtuale Citrix și VMware. Trebuie să selectați excluderile de la scanare predefinite, în funcție de scopul serverului protejat.

   Pentru a adăuga o nouă excludere de la scanare la o anumită categorie, bifați caseta de selectare de lângă categoria respectivă și selectați opțiunea **Excludere nouă**.

5. Dacă doriți să excludeți un fișier sau director din scanări, selectați fișierul sau directorul făcând clic pe butonul **Răsfoiește**.

De asemenea, puteți introduce calea manual. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști.

- Caracterul `*` (asterisc) ține locul oricărui set de caractere, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\*\*.txt` va include toate căile către fișierele cu extensia TXT din directoarele de pe unitatea C:, dar nu și din subdirectoare.

- Două caractere `*` consecutive țin locul oricărui set de caractere (inclusiv un set gol) din numele de fișier sau director, inclusiv caracterele `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\**\*.txt` va include toate căile către fișierele cu extensia TXT localizată în directoarele imbricate în `Folder`, cu excepția `Folder` în sine. Masca trebuie să includă cel puțin un nivel de imbricare. Masca `C:\**\*.txt` nu este o mască validă.

- `?` (semn de întrebare) ține locul oricărui caracter individual, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\???.txt` va include căi pentru toate fișierele din directorul denumit `Folder` care au extensia TXT și un nume format din trei caractere.

  Puteți utiliza măști la începutul, la mijlocul sau la sfârșitul căii fișierului. De exemplu, dacă doriți să adăugați un director pentru toți utilizatorii la excluderi, introduceți masca `?:\Users\*\Folder\`.

  Poți exclude directoarele de rețea. Pentru aceasta, introdu manual calea către directorul de rețea (de exemplu, `\\Network Share\*`).

6. Dacă doriți să excludeți un anumit tip de obiect din scanări, în câmpul **Tipul obiectului detectat** introduceți numele tipului de obiect conform clasificării din Enciclopedia Kaspersky (de exemplu, `Email-Worm`, `Rootkit` sau `RemoteAdmin`).

   Puteți folosi măști cu caracterul `?` (înlocuiește orice caracter unic) și caracterul `*` (înlocuiește orice număr de caractere). De exemplu, dacă este specificată masca `Client*`, Kaspersky Endpoint Security exclude obiectele `Client-IRC`, `Client-P2P` și `Client-SMTP` de la scanări.

7. Dacă doriți să excludeți un fișier individual de la scanări, introduceți hash-ul fișierului în câmpul **Hash obiect**.

   Dacă fișierul este modificat, va fi modificat și hash-ul fișierului. Dacă se întâmplă acest lucru, fișierul modificat nu va fi adăugat la excluderi.

8. În blocul **Componente de protecție**, selectați componentele la care doriți să se aplice excluderea scanării.

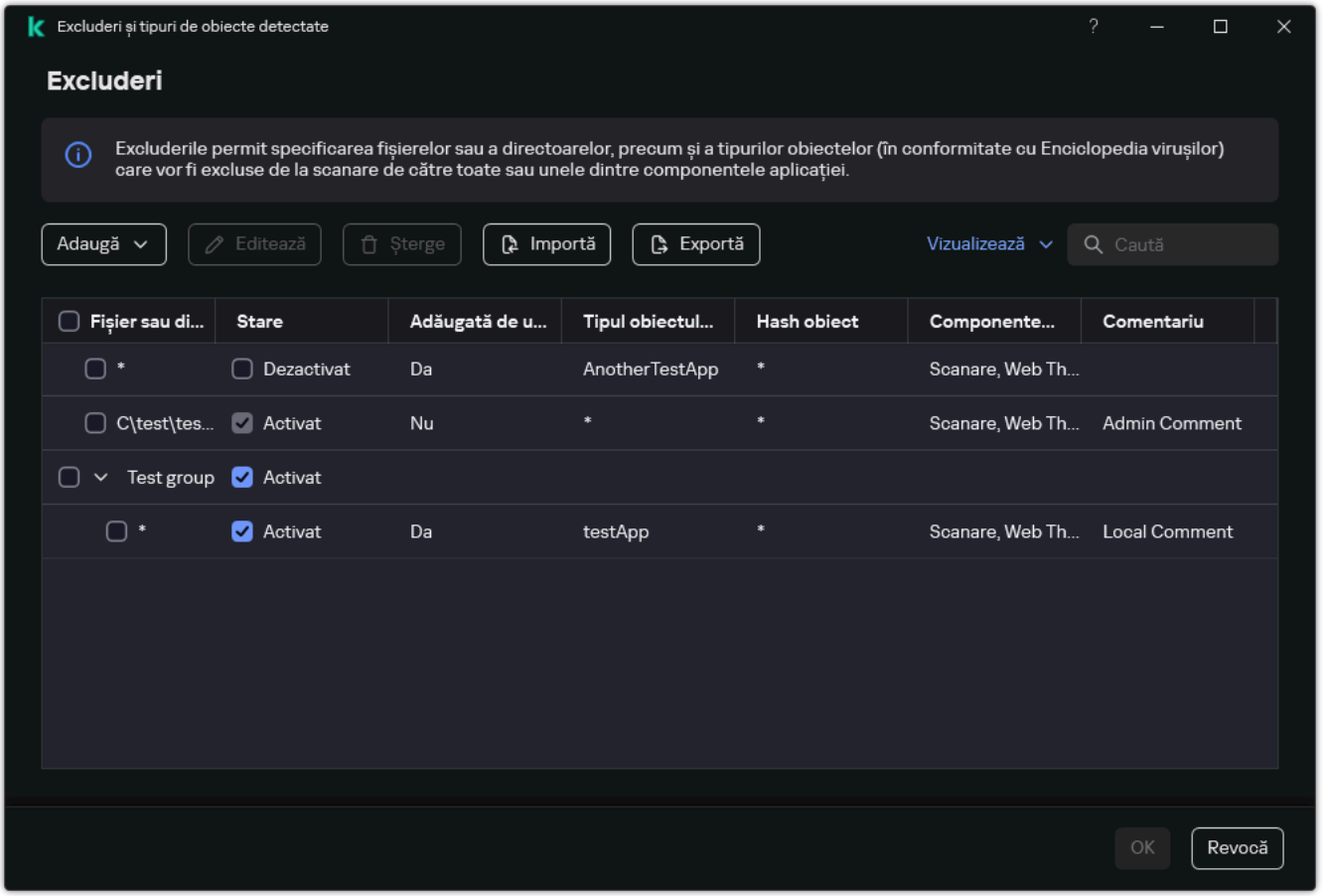
9. Dacă este necesar, în câmpul **Comentariu**, introdu o descriere succintă a excluderii de la scanare pe care o creezi.

10. Selectați starea **Activă** pentru excludere.

11. Fă clic pe **Adaugă**.

    Noua excludere va fi adăugată în listă. Puteți dezactiva excluderea oricând folosind caseta de selectare din coloana **Stare**.

12. Salvați-vă modificările.

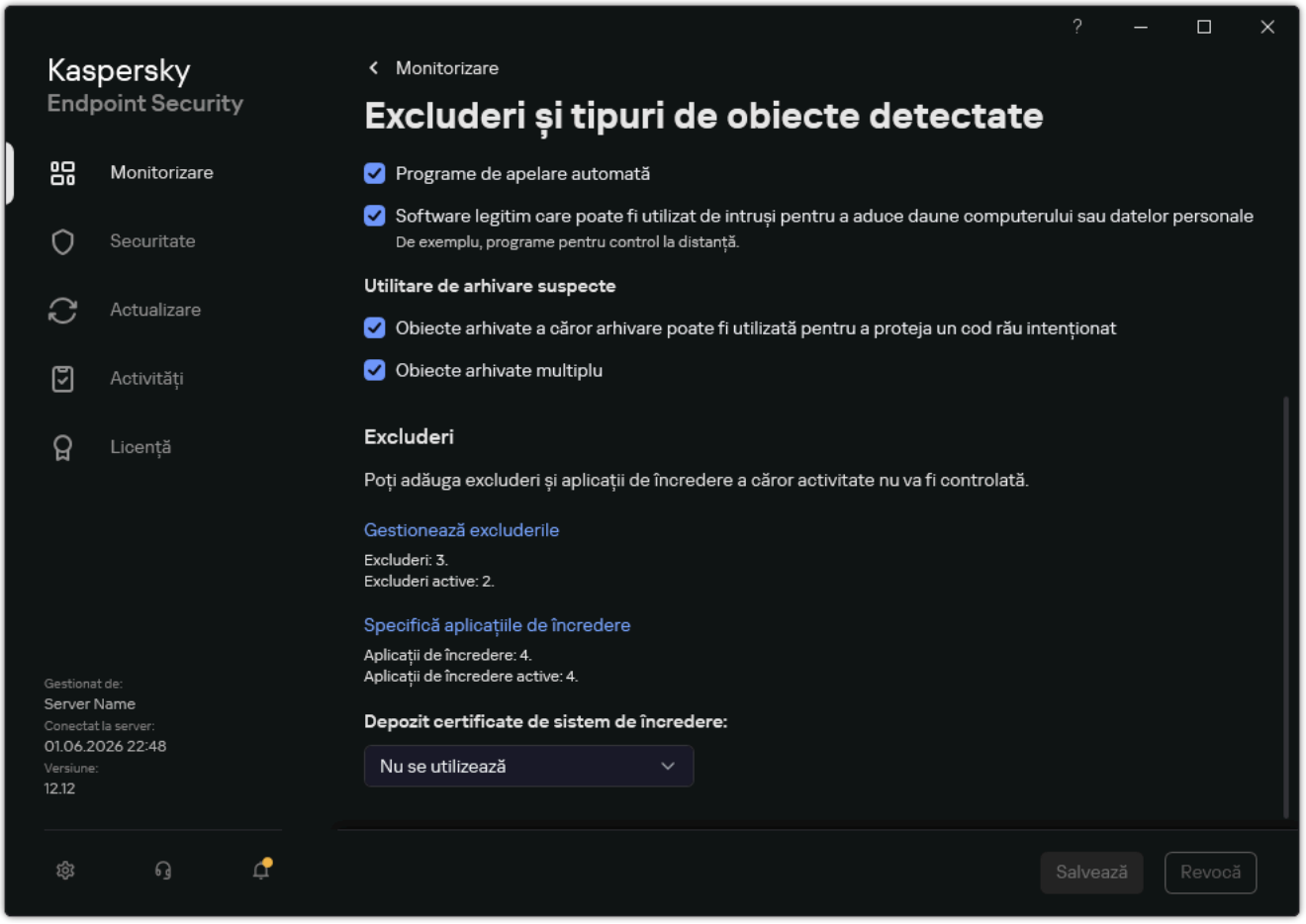


Listă de excluderi

Cum se adaugă o aplicație în lista aplicațiilor de încredere locale din interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Setări generale** → **Excluderi și tipuri de obiecte detectate**.
3. În blocul **Excluderi**, faceți clic pe linkul **Specifică aplicațiile de încredere**.

Kaspersky Endpoint Security ascunde lista consolidată a aplicațiilor de încredere în interfața de utilizator a aplicației dacă configurarea aplicațiilor de încredere este blocată de administrator în consolă (simbolul „lăcăt închis") și aplicațiile locale de încredere sunt interzise (caseta de selectare **Permite utilizarea aplicațiilor de încredere locale** este debifată).



Setări pentru excluderi

4. Faceți clic pe **Adaugă** și selectați o acțiune:

   - **Categorie**. Puteți grupa aplicațiile de încredere în categorii separate. Pentru a crea o categorie nouă, introduceți numele categoriei și adăugați cel puțin o aplicație de încredere la categorie.
   - **Excludere nouă**. Kaspersky Endpoint Security adaugă o nouă aplicație de încredere la rădăcina listei.
   - **Selectează excluderea din listă**. Pentru a configura rapid Kaspersky Endpoint Security pe serverele SQL, serverele Microsoft Exchange și System Center Configuration Manager, aplicația include *aplicații de încredere predefinite*. De asemenea, au fost adăugate aplicații de încredere predefinite pentru a sprijini configurarea aplicațiilor în mediile virtuale Citrix și VMware. Trebuie să selectați aplicații de încredere predefinite, în funcție de scopul serverului protejat.

   Pentru a adăuga o nouă aplicație de încredere la o anumită categorie, bifați caseta de selectare de lângă categoria respectivă și selectați opțiunea **Excludere nouă**.

5. Selectează criteriile de încredere:

   - **Utilizează calea completă a procesului pe disc pentru a-l considera de încredere**. Introdu calea către fișierul executabil al aplicației de încredere.

     Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști.

Kaspersky Endpoint Security tratează numele fișierului unei aplicații de încredere ca fiind sensibil la majuscule și minuscule. Dacă numele fișierului pe care îl introduci conține majuscule sau minuscule care nu corespund, Kaspersky Endpoint Security nu va recunoaște aplicația de încredere.

- **Utilizează hash-ul fișierului de proces pentru a-l considera de încredere**.

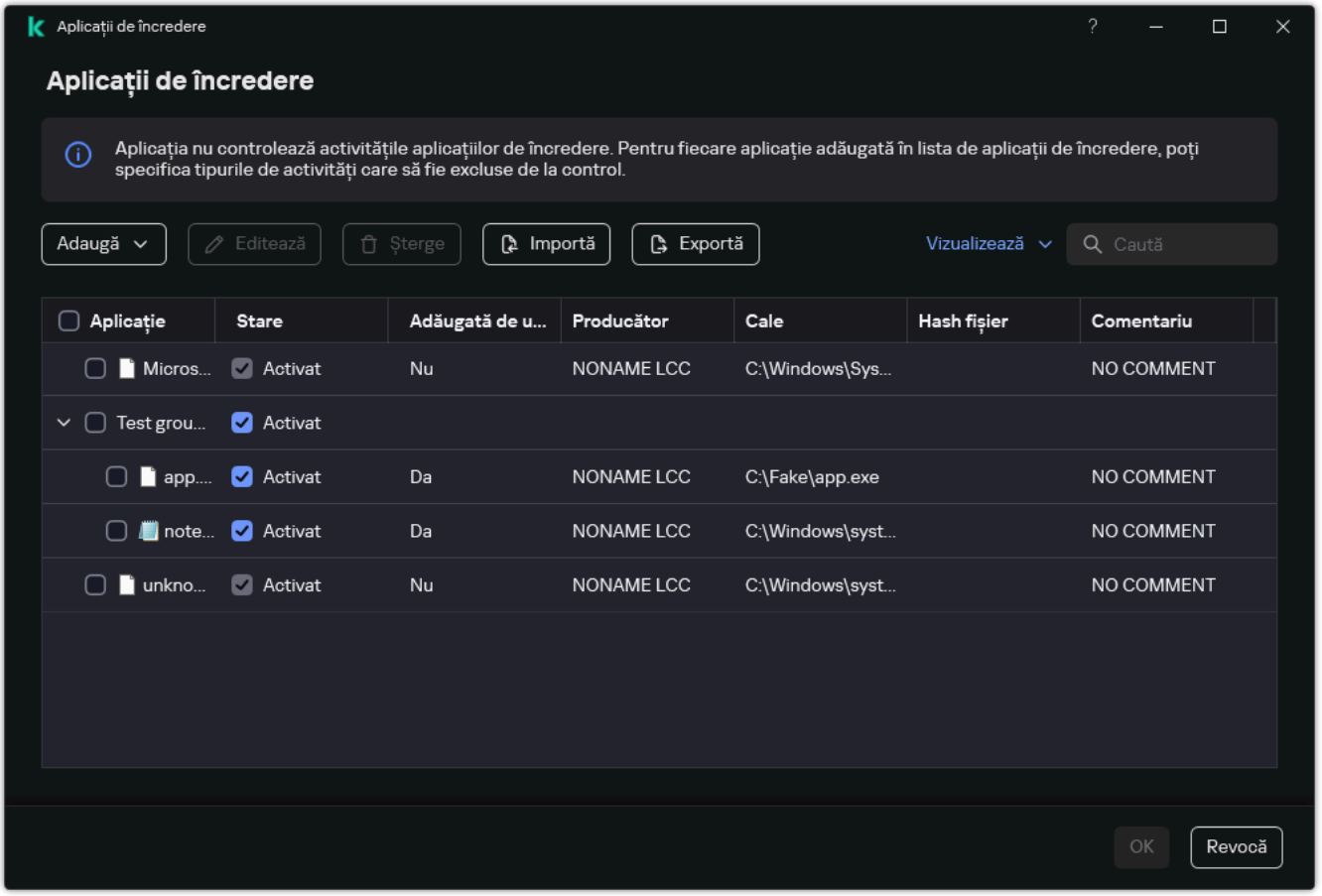
Kaspersky Endpoint Security acceptă variabilele de mediu și convertește calea din interfața locală a aplicației. Cu alte cuvinte, dacă introduceți calea fișierului `%userprofile%\Documents\File.exe`, se adaugă o înregistrate `C:\Users\Fred123\Documents\File.exe` în interfața locală a aplicației pentru utilizatorul Fred123. Astfel, Kaspersky Endpoint Security ignoră programul de încredere `File.exe` pentru ceilalți utilizatori. Pentru a aplica intrarea tuturor conturilor de utilizatori, puteți utiliza caracterul `*` (de exemplu, `C:\Users\*\Documents\File.exe`). Ori de câte ori adăugați o variabilă de mediu, trebuie să reporniți aplicația.

6. În fereastra de proprietăți a aplicației de încredere, configurați setările avansate.

7. Fă clic pe **OK**.

   Noua aplicație de încredere va fi adăugată în listă. Puteți exclude oricând o aplicație din zona de încredere folosind caseta de selectare din coloana **Stare**.

8. Salvați-vă modificările.



Lista aplicațiilor de încredere

Exportul și importul zonei de încredere

O *zonă de încredere* este o listă de obiecte și aplicații configurate de administratorul de sistem, pe care Kaspersky Endpoint Security nu le monitorizează când este activ. Zona de încredere conține următoarele liste: *excluderi de la scanare* și *aplicații de încredere*. Puteți exporta aceste liste în fișiere XML și în alte formate. Apoi puteți modifica fișierul pentru a adăuga, de exemplu, un număr mare de excluderi de același tip. De asemenea, puteți utiliza funcția de export/import pentru a face o copie de rezervă a listei de excluderi și a listei de aplicații de încredere sau pentru a migra lista pe un alt server.

Aplicația folosește următoarele formate pentru exportul și importul *listei de excluderi*:

- XML este disponibil în Consola de administrare (MMC), Web Console și Cloud Console.
- DAT este disponibil numai pentru import în Consola de administrare (MMC). Scopul acestui format este de a menține compatibilitatea cu versiunile mai vechi ale aplicației. Puteți converti un fișier DAT în XML în Consola de administrare (MMC) pentru a migra listele de excluderi în Web Console.
- CSV este disponibil doar în interfața locală a aplicației.

Kaspersky Endpoint Security folosește formatul XML pentru exportul și importul *listei de aplicații de încredere*.

Cum se exportă și se importă zona de încredere în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Setări generale** → **Excluderi și tipuri de obiecte**.
4. În **Excluderi de la scanare și aplicații de încredere**, selectează componenta zonei de încredere pe care dorești să o exporți sau să o imporți: **Excluderi de la scanare** sau **Aplicații de încredere**.
5. Fă clic pe **Setări**.
6. Pentru a exporta lista de reguli:
   a. Selectați excluderile pe care doriți să le exportați. Pentru a selecta mai multe porturi, utilizați tastele **CTRL** sau **SHIFT**.

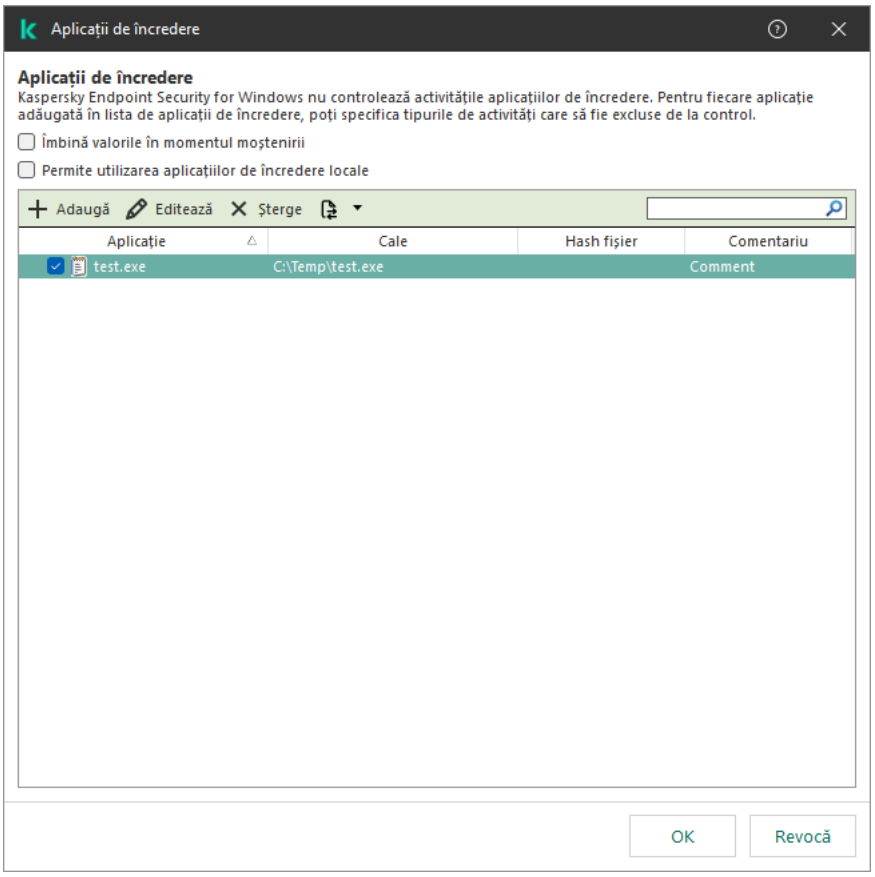
      Dacă nu ați selectat nicio excludere, Kaspersky Endpoint Security va exporta toate excluderile.

   b. Fă clic pe butonul → **Exportă**.

   c. În fereastra care se deschide, specificați numele fișierului XML în care doriți să exporți lista de excluderi și selectați directorul în care doriți să salvați acest fișier.

d. Salvați fișierul.

Kaspersky Endpoint Security exportă întreaga listă de excluderi în fișierul XML. Kaspersky Endpoint Security acceptă, de asemenea, exportul listei de excluderi într-un fișier DAT.



Lista aplicațiilor de încredere

7. Pentru a importa lista de excluderi:

a. Fă clic pe butonul → **Importă**.

b. În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de excluderi.

c. Deschideți fișierul.

În cazul în care computerul are deja o listă de excluderi, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul XML. Kaspersky Endpoint Security acceptă, de asemenea, importul unei liste de excluderi dintr-un fișier DAT.

8. Salvați-vă modificările.

Cum se exportă și se importă zona de încredere în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.
4. Accesează secțiunea **Trusted Zone**.

5. Pentru a exporta lista de reguli:

   a. Faceți clic pe linkul **Malware Scan exclusions**.

   b. Selectați excluderile pe care doriți să le exportați.

   c. Fă clic pe butonul → **Export**.

      Kaspersky Endpoint Security exportă lista de excluderi într-un fișier JSON în directorul pentru descărcări implicit.

6. Pentru a exporta lista cu aplicațiile de încredere:

   a. Selectați aplicațiile de încredere pe care doriți să le exportați.

   b. Fă clic pe butonul → **Export**.

      Kaspersky Endpoint Security exportă lista de aplicații de încredere într-un fișier JSON în directorul de descărcări implicit.

7. Pentru a importa lista de excluderi:

   a. Faceți clic pe linkul **Malware Scan exclusions**.

   b. Fă clic pe butonul → **Import**.

      În fereastra care se deschide, selectați fișierul JSON din care doriți să importați lista de excluderi.

   c. Deschideți fișierul.

      În cazul în care computerul are deja o listă de excluderi, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul JSON.

8. Pentru a importa o listă cu aplicațiile de încredere:

   a. Faceți clic pe linkul **Applications**.

   b. Fă clic pe butonul → **Import**.

      Astfel, se deschide o fereastră; în acea fereastră, selectați fișierul JSON din care doriți să importați lista cu aplicațiile de încredere.

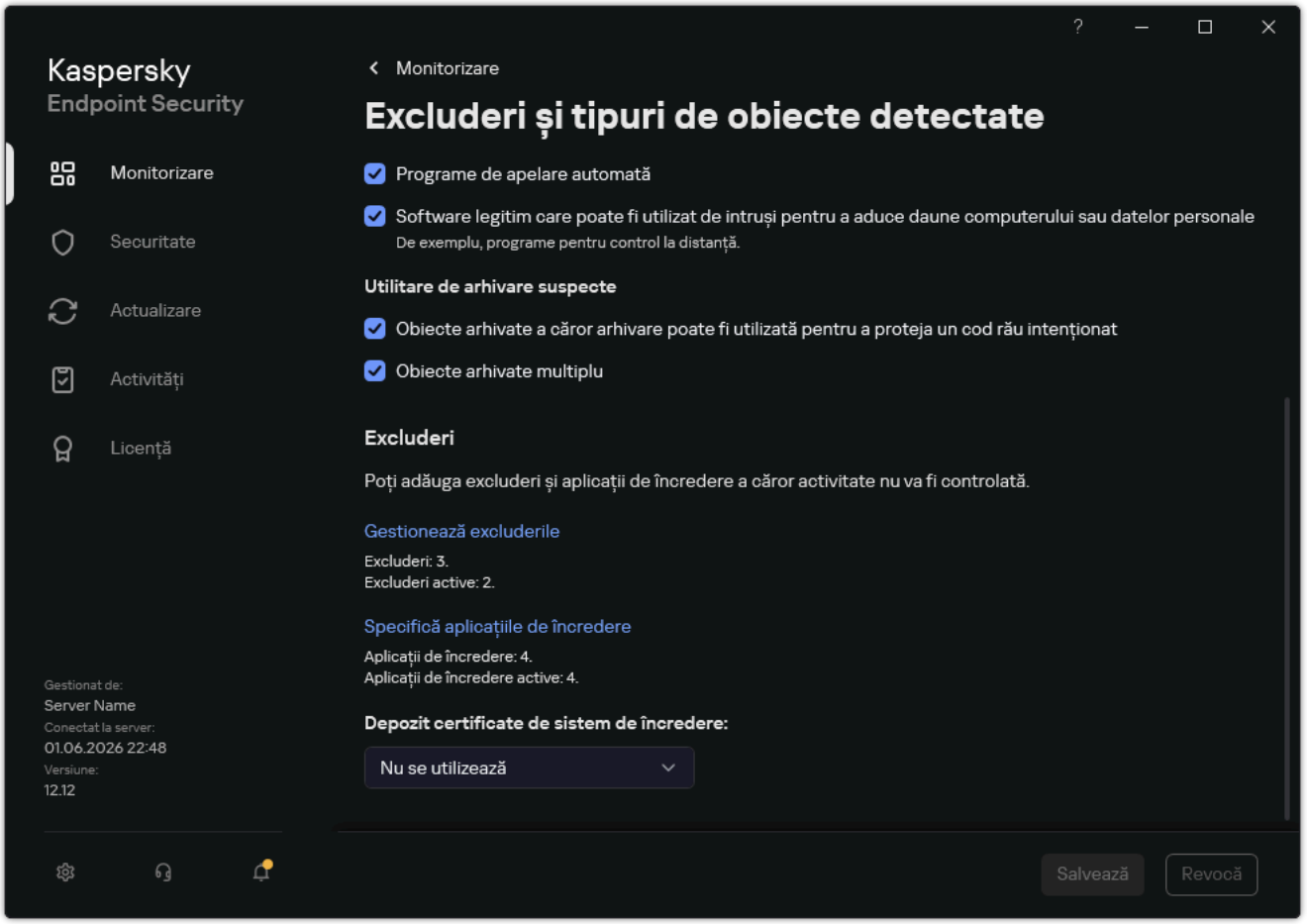
   c. Deschideți fișierul.

      În cazul în care computerul are deja o listă cu aplicații de încredere, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul JSON.

9. Salvați-vă modificările.

Cum se exportă și se importă zona de încredere în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul .
2. În fereastra cu setările aplicației, selectați **Setări generale** → **Excluderi și tipuri de obiecte detectate**.

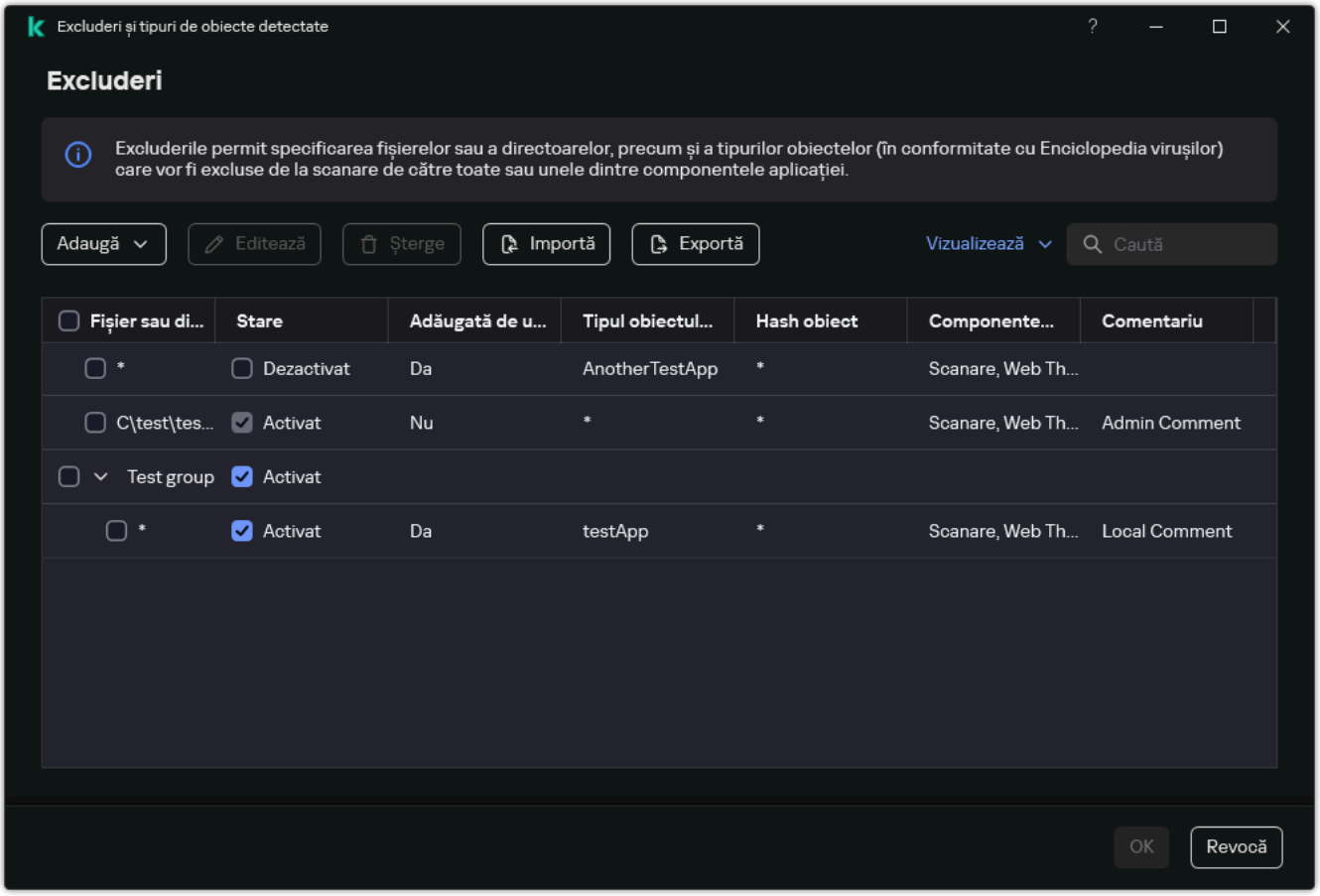


Setări pentru excluderi

3. Pentru a exporta lista de reguli:
   a. În blocul **Excluderi**, faceți clic pe linkul **Gestionează excluderile**.
   b. Selectați excluderile pe care doriți să le exportați.
   c. Fă clic pe **Exportă**.
   d. Confirmați că doriți să exportați numai excluderile selectate sau exportați întreaga listă de excluderi.
   e. În fereastra care se deschide, specificați numele fișierului CSV în care doriți să exporți lista de excluderi și selectați directorul în care doriți să salvați acest fișier.

f. Salvați fișierul.

Kaspersky Endpoint Security exportă întreaga listă de excluderi în fișierul CSV.



Listă de excluderi

4. Pentru a exporta lista cu aplicațiile de încredere:

a. În blocul **Excluderi**, faceți clic pe linkul **Specifică aplicațiile de încredere**.

b. Selectați aplicațiile de încredere pe care doriți să le exportați.

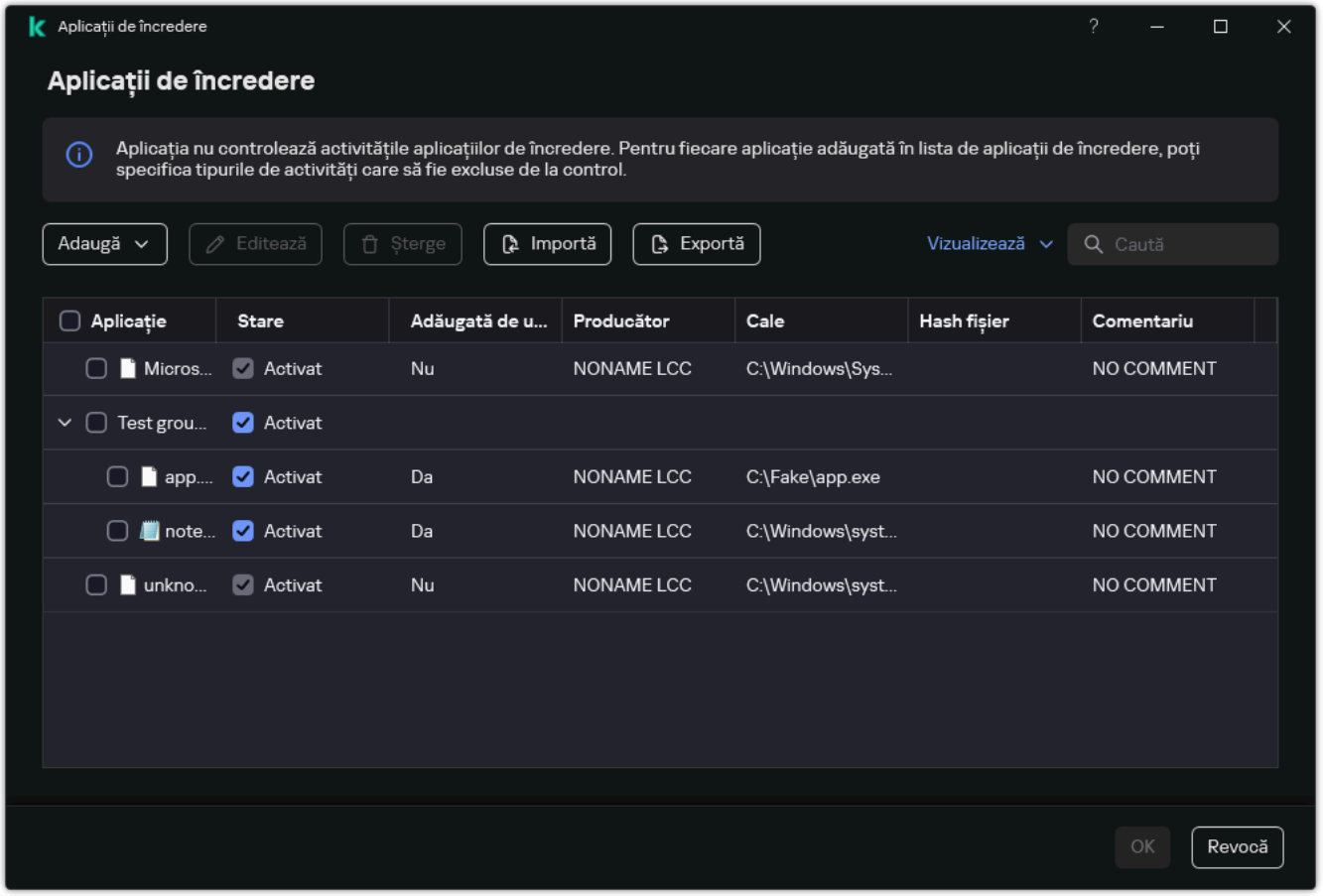
c. Fă clic pe **Exportă**.

d. Confirmați că doriți să exportați numai aplicațiile de încredere selectate sau să exportați întreaga listă.

e. Astfel, se deschide o fereastră; în acea fereastră, introdu numele fișierului XML în care dorești să exporți lista cu aplicațiile de încredere și selectează directorul în care dorești să salvezi acest fișier.

f. Salvați fișierul.

Kaspersky Endpoint Security exportă întreaga listă de aplicații de încredere în fișierul XML.



Lista aplicațiilor de încredere

5. Pentru a importa lista de excluderi:

a. În blocul **Excluderi**, faceți clic pe linkul **Gestionează excluderile**.

b. Fă clic pe **Importă**.

c. În fereastra care se deschide, selectați fișierul CSV din care doriți să importați lista de excluderi.

d. Deschideți fișierul.

În cazul în care computerul are deja o listă de excluderi, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul CSV.

6. Pentru a importa o listă cu aplicațiile de încredere:

a. În blocul **Excluderi**, faceți clic pe linkul **Specifică aplicațiile de încredere**.

b. Fă clic pe **Importă**.

c. Astfel, se deschide o fereastră; în acea fereastră, selectați fișierul XML din care doriți să importați lista cu aplicațiile de încredere.

d. Deschideți fișierul.

În cazul în care computerul are deja o listă cu aplicații de încredere, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul XML.

7. Salvați-vă modificările.

Gestionarea aplicațiilor cu o semnătură digitală de încredere

Folosirea depozitului de certificate de sistem de încredere îți permite să excluzi de la scanările de viruși aplicațiile semnate cu o semnătură digitală de încredere. Kaspersky Endpoint Security atribuie automat astfel de aplicații grupului *De încredere*.

Cum se începe utilizarea unui spațiu de stocare pentru certificate de sistem de încredere în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Setări generale** → **Excluderi și tipuri de obiecte**.
4. În blocul **Depozit certificate de sistem de încredere**, bifați caseta de selectare **Utilizează depozitul de certificate de sistem de încredere**.
5. În lista verticală, selectează depozitul sistemului pe care Kaspersky Endpoint Security trebuie să îl considere ca fiind de încredere.
6. Salvați-vă modificările.

Cum se începe utilizarea unui spațiu de stocare pentru certificate de sistem de încredere în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați fila **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesează secțiunea **Trusted Zone**.
5. În fereastra care se deschide, fă clic pe linkul **Root certificates**.
6. În fereastra care se deschide, bifați caseta de selectare **Use trusted system certificate store**.
7. Selectează depozitul sistemului pe care Kaspersky Endpoint Security trebuie să îl considere ca fiind de încredere.
8. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se începe utilizarea unui spațiu de stocare pentru certificate de sistem de încredere în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Setări generale** → **Excluderi și tipuri de obiecte detectate**.
3. În lista verticală **Depozit certificate de sistem de încredere**, selectați depozitul sistemului pe care Kaspersky Endpoint Security trebuie să îl considere ca fiind de încredere.
4. Salvați-vă modificările.

Appendix. Excluderi de la scanare și aplicații de încredere predefinite

Începând cu Kaspersky Endpoint Security 12.6 for Windows, excluderile de scanare și aplicații de încredere sunt adăugate la zona de încredere. Excluderile de la scanare și aplicațiile de încredere predefinite ajută la configurarea rapidă a Kaspersky Endpoint Security pe serverele SQL, serverele Microsoft Exchange și System Center Configuration Manager. Aceasta înseamnă că nu trebuie să configurați manual o zonă de încredere pentru aplicație pe servere. Începând cu Kaspersky Endpoint Security 12.8 for Windows, poți instala aplicația în modul Light Agent pentru a proteja mediile virtuale. Excluderile de la scanare predefinite și aplicațiile de încredere te pot ajuta să configurezi rapid Kaspersky Endpoint Security în mediile virtuale Citrix și VMware.

Poți selecta excluderi predefinite și aplicații de încredere în următoarele moduri:

- Instalarea aplicației.
  - Instalarea locală a aplicației folosind Expertul
  - Proprietăți a pachetului de instalare.
- Setarea politicii.
  - Asistent pentru politici noi
  - Proprietăți politici: excluderi de la scanare și aplicații de încredere

Server SQL

Când instalezi Kaspersky Endpoint Security pe un server SQL, trebuie să creezi o zonă de încredere din excluderi predefinite și aplicații de încredere pentru a te asigura că funcționarea serverului nu este afectată.

Excluderi de la scanare predefinite

Cale	Versiunea SQL
`%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA\*.mdf`	2012 2014 2016 2017 2019 2022
`%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?\*\Data\*.mdf`	2012

Cale	Versiunea SQL
%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

Server Microsoft Exchange

Când instalezi Kaspersky Endpoint Security pe un server Microsoft Exchange, trebuie să creezi o zonă de încredere din excluderi predefinite și aplicații de încredere pentru a te asigura că funcționarea serverului nu este afectată.

Excluderi de la scanare predefinite

Cale	Versiune Microsoft Exchange
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
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

Cale	Versiune Microsoft Exchange
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

Aplicații de încredere predefinite

Cale	Versiune Microsoft Exchange
%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

Excluderi de la scanare predefinite

Cale	Versiune System Center Configuration Manager
%ProgramFiles%\Microsoft Configuration Manager\Inboxes	2012 2012 R2

Citrix

Când instalezi Kaspersky Endpoint Security într-un mediu virtual Citrix, trebuie să creezi o zonă de încredere din excluderile predefinite și aplicațiile de încredere pentru a te asigura că funcționarea serverului nu este afectată.

Excluderi de la scanare predefinite

Cale
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName_log.ldf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName_log.ldf
%ProgramData%\Citrix\Broker\Cache
%SystemRoot%\System32\drivers\CtxUvi.sys

Cale
%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

Cale	Soluția Citrix
%ProgramFiles%\Citrix\Broker\Service\BrokerService.exe	Aplicații și desktopuri virtuale
%ProgramFiles%\Microsoft SQL Server\150\LocalDB\Binn\sqlservr.exe	Aplicații și desktopuri virtuale
%ProgramFiles%\Citrix\Broker\Service\HighAvailabilityService.exe	Aplicații și desktopuri virtuale
%ProgramFiles%\Citrix\ConfigSync\ConfigSyncService.exe	Aplicații și desktopuri virtuale
%ProgramFiles%\Citrix\User Profile Manager\UserProfileManager.exe	Aplicații și desktopuri virtuale
%ProgramFiles%\Citrix\Virtual Desktop Agent\BrokerAgent.exe	Aplicații și desktopuri virtuale
%SystemRoot%\System32\drivers\CVhdFilter.sys	Aplicații și desktopuri virtuale
%ProgramFiles(x86)%\Citrix\ICAService\CtxSvcHost.exe	Aplicații și desktopuri virtuale
%ProgramFiles%\Citrix\System32\ctxgfx.exe	Aplicații și desktopuri virtuale
%ProgramFiles%\Citrix\ICAService\picaSvc2.exe	Aplicații și desktopuri virtuale
%ProgramFiles%\Citrix\ICAService\CpSvc.exe	Aplicații și desktopuri virtuale
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Aplicații și desktopuri virtuale
%ProgramFiles%\Citrix\HDX\bin\CtxSvcHost.exe	Aplicații și desktopuri virtuale
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Aplicații și desktopuri virtuale
%ProgramFiles%\Citrix\HDX\bin\picaSvc2.exe	Aplicații și desktopuri virtuale
%ProgramFiles%\Citrix\HDX\bin\CpSvc.exe	Aplicații și desktopuri virtuale
%ProgramFiles(x86)%\Citrix\System32\WebSocketService.exe	Aplicații și desktopuri virtuale
%ProgramFiles%\Citrix\ICAService\WebSocketService.exe	Aplicații și desktopuri virtuale
%ProgramFiles(x86)%\Citrix\HDX\bin\WebSocketService.exe	Aplicații și desktopuri virtuale

Cale	Soluția Citrix
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\AudioTranscoder.exe	Aplicații și desktopuri virtuale
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngine.Net.Service.exe	Aplicații și desktopuri virtuale
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngineService.exe	Aplicații și desktopuri virtuale
%ProgramFiles(x86)%\Citrix\ICA Client\MediaEngineService.exe	Aplicația Spațiu de lucru
%ProgramFiles(x86)%\Citrix\ICA Client\CDViewer.exe	Aplicația Spațiu de lucru
%ProgramFiles(x86)%\Citrix\ICA Client\concentr.exe	Aplicația Spațiu de lucru
%ProgramFiles(x86)%\Citrix\ICA Client\wfica32.exe	Aplicația Spațiu de lucru
%ProgramFiles(x86)%\Citrix\ICA Client\bgblursvc.exe	Aplicația Spațiu de lucru
%ProgramFiles(x86)%\Citrix\ICA Client\AuthManager\AuthManSvr.exe	Aplicația Spațiu de lucru
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfService.exe	Aplicația Spațiu de lucru
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfServicePlugin.exe	Aplicația Spațiu de lucru
%ProgramFiles(x86)%\Citrix\ICA Client\HdxRtcEngine.exe	Aplicația Spațiu de lucru
%ProgramFiles(x86)%\Citrix\ICA Client\HdxTeams.exe	Aplicația Spațiu de lucru
%ProgramFiles%\Citrix\Provisioning Services\BNTFTP.EXE	Asigurare acces
%ProgramFiles%\Citrix\Provisioning Services\PVSTSB.EXE	Asigurare acces
%ProgramFiles%\Citrix\Provisioning Services\StreamService.exe	Asigurare acces
%ProgramFiles%\Citrix\Provisioning Services\StreamProcess.exe	Asigurare acces
%ProgramFiles%\Citrix\Provisioning Services\soapserver.exe	Asigurare acces
%ProgramFiles%\Citrix\Provisioning Services\Inventory.exe	Asigurare acces
%ProgramFiles%\Citrix\Provisioning Services\Notifier.exe	Asigurare acces
%ProgramFiles%\Citrix\Provisioning Services\MgmtDaemon.exe	Asigurare acces
%ProgramFiles%\Citrix\Provisioning Services\BNPXE.exe	Asigurare acces

Cale	Soluția Citrix
%ProgramFiles%\Citrix\Provisioning Services\CdfSvc.exe	Asigurare acces
%ProgramFiles%\Citrix\Provisioning Services\BNAbsService.exe	Asigurare acces
%SystemRoot%\System32\drivers\bnistack6.sys	Asigurare acces
%SystemRoot%\System32\drivers\CfsDep2.sys	Asigurare acces
%SystemRoot%\System32\drivers\cnicteam.sys	Asigurare acces
%ProgramFiles%\Citrix\Provisioning Services\BNDevice.exe	Asigurare acces
%ProgramFiles%\Citrix\Provisioning Services\drivers\BNIstack6.sys	Asigurare acces
%ProgramFiles%\Citrix\Provisioning Services\drivers\CNicTeam.sys	Asigurare acces
%ProgramFiles%\Citrix\Provisioning Services\drivers\CFsDep2.sys	Asigurare acces
%ProgramFiles%\Citrix\Provisioning Services\drivers\CVhdMp.sys	Asigurare acces
%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

Când instalezi Kaspersky Endpoint Security într-un mediu virtual VMware, trebuie să creezi o zonă de încredere din aplicațiile de încredere predefinite pentru a te asigura că funcționarea serverului nu este afectată.

Aplicații de încredere predefinite

Cale	Soluția VMware
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

Cale	Soluția VMware
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
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

Gestionarea copiilor de rezervă

Opțiunea *Copiere de rezervă* stochează copii de rezervă ale fișierelor care au fost șterse sau modificate în timpul dezinfectării. O *copie de rezervă* este copia unui fișier creată înainte ca fișierul să fie dezinfectat sau șters. Copiile de rezervă ale fișierelor sunt stocate într-un format special și nu reprezintă o amenințare.

Copiile de rezervă ale fișierelor sunt stocate în directorul `C:\ProgramData\Kaspersky Lab\KES.14.1\QB`.

Utilizatorii din grupul Administratori au permisiuni complete de a accesa acest director. Utilizatorul al cărui cont a fost utilizat pentru a instala Kaspersky Endpoint Security primește drepturi de acces limitate la acest director.

Kaspersky Endpoint Security nu permite configurarea permisiunilor de acces al utilizatorului la copiile de rezervă ale fișierelor.

Uneori nu este posibilă păstrarea integrității fișierelor în timpul dezinfectării. Dacă după dezinfectare pierzi parțial sau total accesul la informații importante dintr-un fișier dezinfectat, poți încerca să restabilești fișierul din copia de rezervă în directorul inițial.

Dacă Kaspersky Endpoint Security se execută sub administrarea Kaspersky Security Center, copiile de rezervă ale fișierelor ar putea să fie transmise către Serverul de administrare al Kaspersky Security Center. Pentru mai multe detalii despre gestionarea copiilor de rezervă ale fișierelor în Kaspersky Security Center, te rugăm să consulți sistemul de ajutor al Kaspersky Security Center.

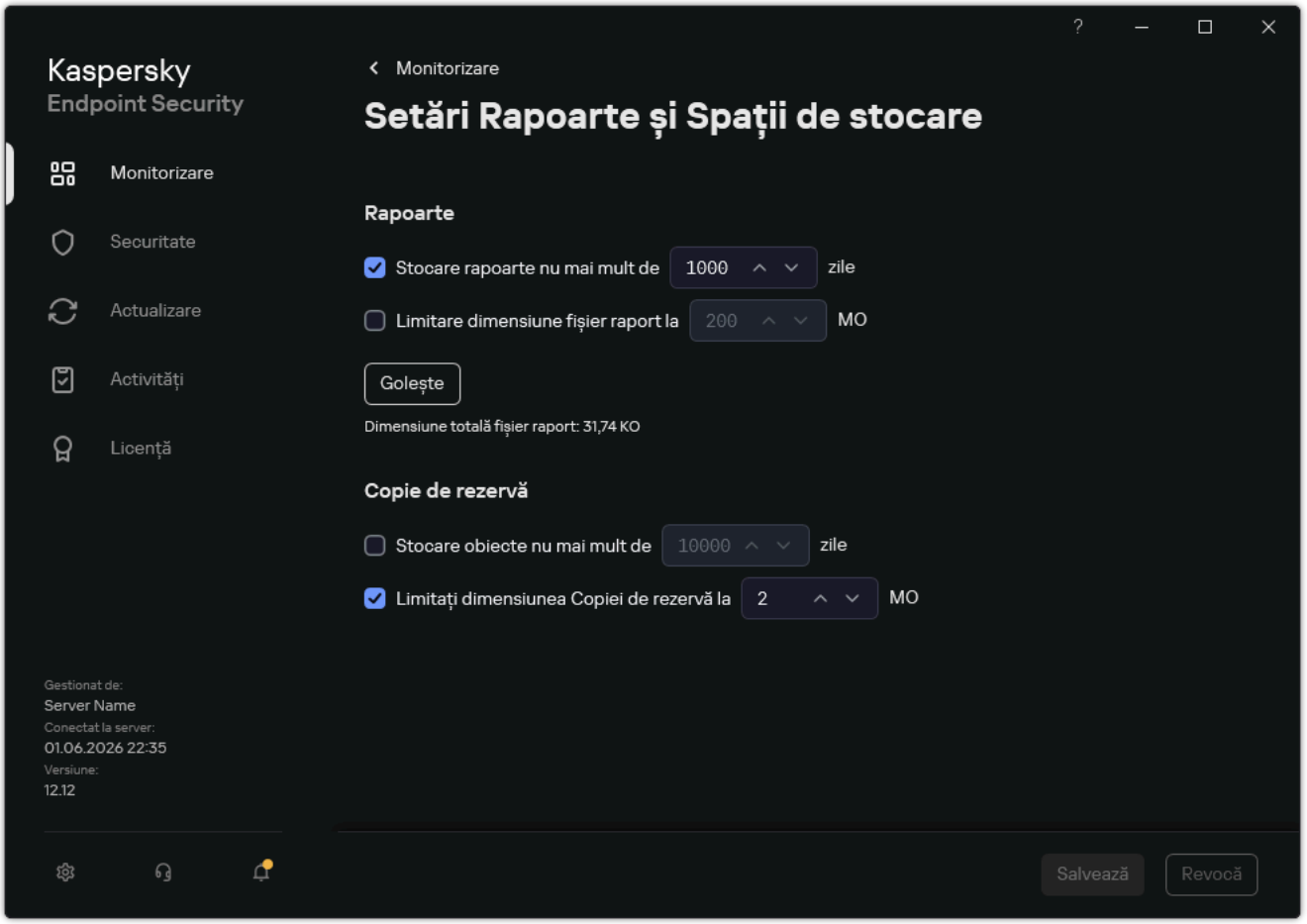
Configurarea perioadei maxime de stocare pentru fișierele din Copie de rezervă

Durata maximă implicită de stocare pentru copiile fișierelor din Copie de rezervă este de 30 de zile. După expirarea duratei maxime de stocare, Kaspersky Endpoint Security șterge fișierele cele mai vechi din Copie de rezervă.

Pentru a configura perioada maximă de stocare pentru fișierele din Copie de rezervă:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra de setări a aplicației, în **Setări generale** fă clic pe opțiunea **Rapoarte și Spații de stocare**.



Setări copiere de rezervă

3. Dacă doriți să limitați perioada de stocare pentru copiile fișierelor în Copie de rezervă, bifați caseta de selectare **Stocare obiecte nu mai mult de N zile** din blocul **Copie de rezervă**. Introduceți durata maximă de stocare pentru copiile de rezervă ale fișierelor în Copie de rezervă.

4. Salvați-vă modificările.

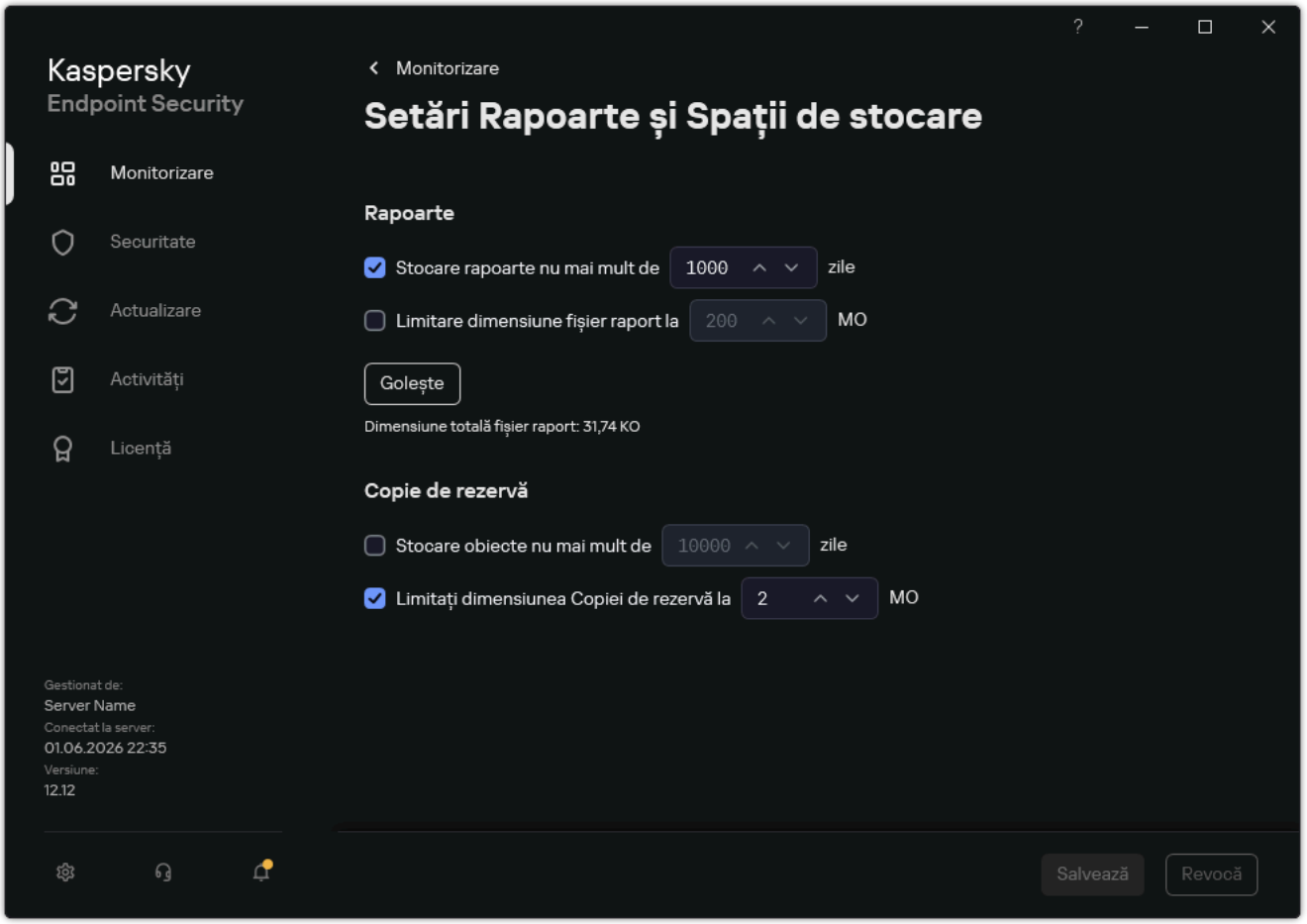
Configurarea dimensiunii maxime pentru Copie de rezervă

Puteți specifica dimensiunea maximă a copiei de rezervă. În mod implicit, dimensiunea pentru Copie de rezervă nu este limitată. După ce dimensiunea maximă este atinsă, Kaspersky Endpoint Security șterge automat fișierele cele mai vechi din Copie de rezervă.

Pentru a configura dimensiunea maximă pentru Copie de rezervă:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra de setări a aplicației, în **Setări generale** fă clic pe opțiunea **Rapoarte și Spații de stocare**.



Setări copiere de rezervă

3. În blocul **Copie de rezervă**, bifați caseta de selectare **Limitați dimensiunea Copiei de rezervă la N MO**. În cazul în care caseta de selectare este bifată, dimensiunea maximă de stocare este limitată la valoarea definită. În mod implicit, dimensiunea maximă este de 1024 MO. Pentru a evita depășirea dimensiunii maxime a de stocare, Kaspersky Endpoint Security șterge automat fișierele cele mai vechi din stocare atunci când este atinsă dimensiunea maximă de stocare.

4. Salvați-vă modificările.

Restaurarea fișierelor din Copie de rezervă

Dacă într-un fișier este detectat cod rău intenționat, Kaspersky Endpoint Security blochează fișierul, îi atribuie starea *Nedezinfectat*, plasează o copie a acestuia în Copie de rezervă și încearcă să-l dezinfecteze. Dacă dezinfectarea fișierului se face cu succes, starea copiei de rezervă a fișierului se modifică în *Dezinfectat*. Fișierul devine disponibil în directorul său original. Dacă un fișier nu poate fi dezinfectat, Kaspersky Endpoint Security îl șterge din directorul său original. Poți restaura fișierul din copia sa de rezervă în directorul său original.

Fișierele cu starea *Va și șterasă la repornirea computerului* nu pot fi restaurate. Reporniți computerul, iar starea fișierului se va schimba în *Dezinfectat* sau *Șters*. Puteți, de asemenea, restaura fișierul din copia sa de rezervă în directorul său original.

Atunci când detectează cod rău intenționat într-un fișier care face parte din aplicația Windows Store, Kaspersky Endpoint Security șterge imediat fișierul, fără a-l muta în Copie de rezervă. Poți restaura integritatea aplicației Windows Store folosind instrumentele adecvate ale sistemului de operare (consultă fișierele de ajutor Microsoft Windows pentru detalii referitoare la restaurarea aplicației Windows Store).

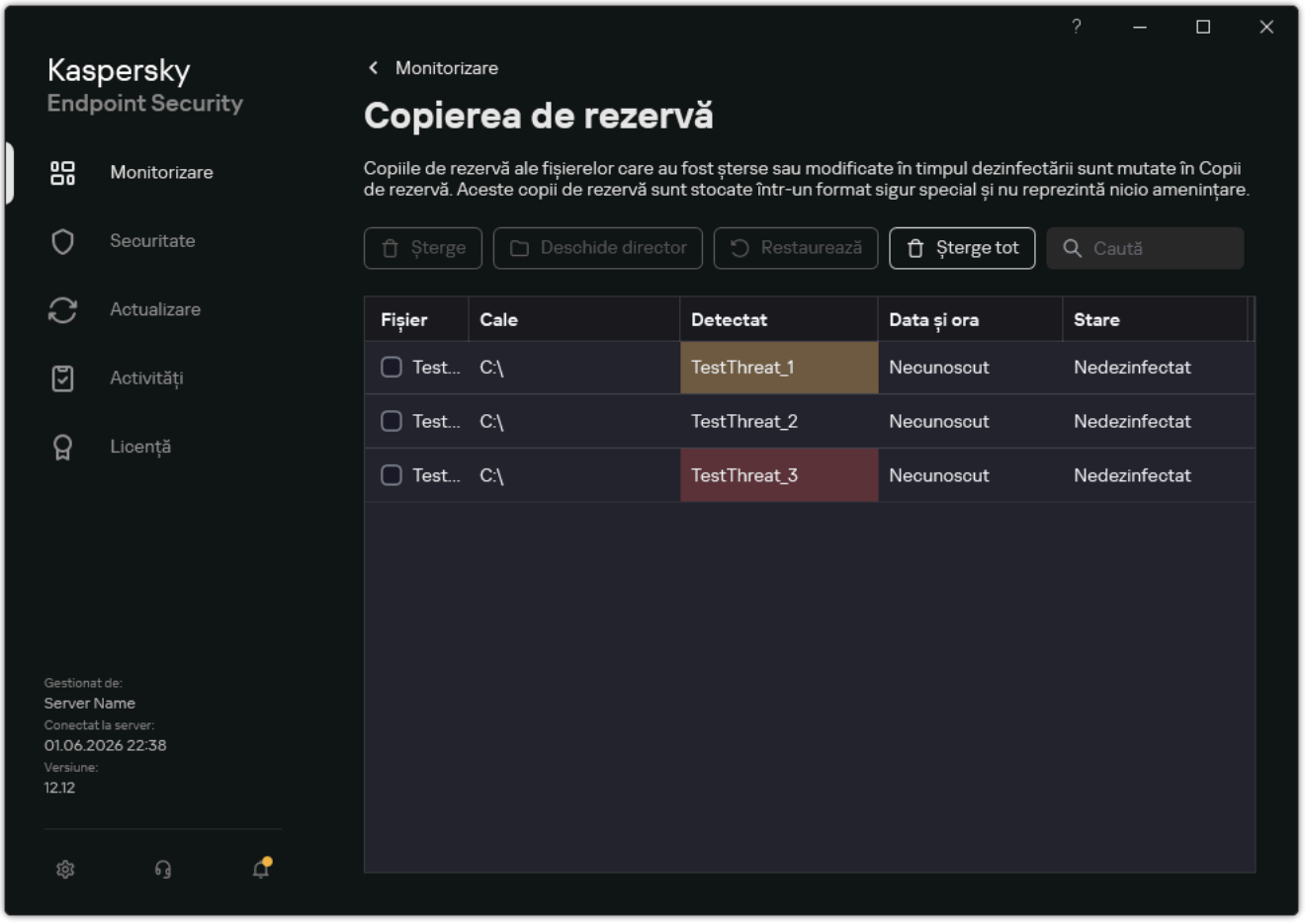
Setul de copii de rezervă ale fișierelor este prezentat sub formă de tabel. Se afișează calea către directorul inițial al fișierului pentru copia de rezervă a fișierului. Calea către directorul inițial al fișierului poate conține date personale.

Dacă mai multe fișiere cu nume identice și conținut diferit, amplasate în același director, sunt mutate în Copie de rezervă, va fi restaurat numai fișierul care a fost plasat ultimul în Copie de rezervă.

Pentru a restaura fișierele din Copie de rezervă:

1. În fereastra principală a aplicației, în secțiunea **Monitorizare**, faceți clic pe dala **Copiere de rezervă**.
2. Se deschide lista de fișiere din Copie de rezervă; în lista respectivă, selectați fișierele pe care doriți să le restaurați și faceți clic pe **Restaurează**.

Kaspersky Endpoint Security restaurează toate fișierele din copiile de rezervă selectate în directoarele lor inițiale.



Copie de rezervă

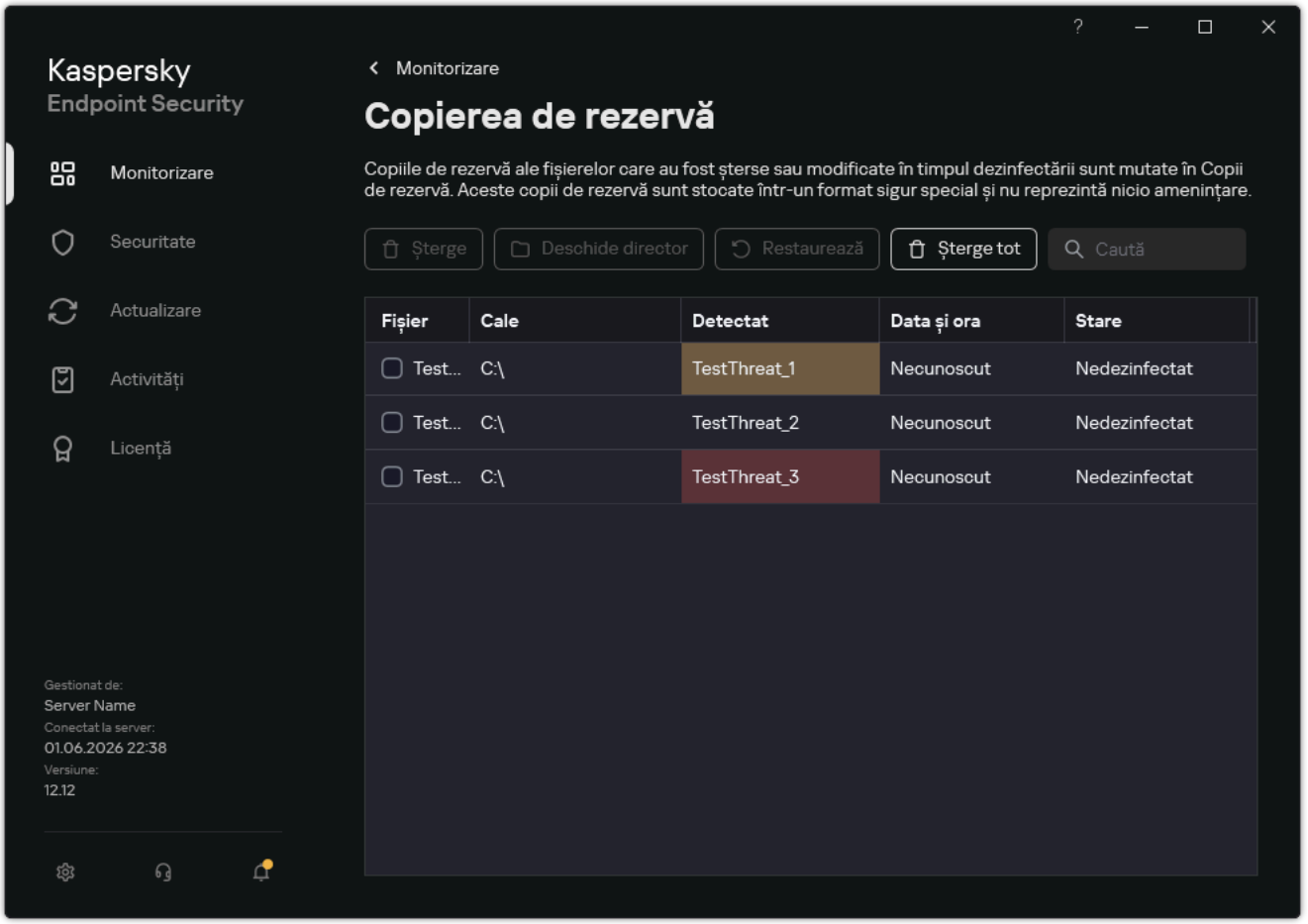
Ștergerea copiilor de rezervă ale fișierelor din Copie de rezervă

Kaspersky Endpoint Security șterge în mod automat copiile din Copie de rezervă ale fișierelor, indiferent de stare, după expirarea duratei de stocare care este configurată în setările aplicației. Poți, de asemenea, să ștergi manual orice copie a unui fișier din Copie de rezervă.

Pentru a șterge copiile de rezervă ale fișierelor din Copie de rezervă:

1. În fereastra principală a aplicației, în secțiunea **Monitorizare**, faceți clic pe dala **Copiere de rezervă**.
2. Se deschide lista de fișiere din Copie de rezervă; în lista respectivă, selectați fișierele pe care doriți să le ștergeți din Copie de rezervă și faceți clic pe **Șterge**.

Kaspersky Endpoint Security șterge copiile de rezervă selectate ale fișierelor din Copie de rezervă.



Copie de rezervă

Serviciul de notificare

În timpul funcționării Kaspersky Endpoint Security apar tot felul de evenimente. Notificările referitoare la aceste evenimente pot fi pur informative sau pot conține informații critice. De exemplu, notificările vă pot informa despre finalizarea cu succes a unei actualizări a bazei de date sau a unui modul al aplicației sau despre înregistrarea unor erori la componente care necesită remediere.

Kaspersky Endpoint Security acceptă înregistrarea în jurnal a informațiilor despre evenimente în funcționarea jurnalului de aplicații Microsoft Windows și/sau a jurnalului de evenimente Kaspersky Endpoint Security.

Kaspersky Endpoint Security furnizează notificări în următoarele moduri:

- utilizând notificări pop-up zona de notificare a barei de activități Microsoft Windows;
- prin e-mail.

Poți configura furnizarea notificărilor de evenimente. Metoda de furnizare a notificărilor este configurată pentru fiecare tip de eveniment.

Atunci când folosești tabelul de evenimente pentru a configura serviciul de notificări, poți executa următoarele acțiuni:

- Filtrează evenimentele serviciului de notificări după valorile coloanei sau utilizând condiții de filtrare particularizate.
- Utilizează funcția de căutare pentru evenimentele serviciului de notificări.
- Sortează evenimentele serviciului de notificări.
- Schimbă ordinea și setul de coloanele afișate în lista de evenimente ale serviciului de notificări.

Configurarea setărilor pentru jurnalul de evenimente

Pentru a configura setările jurnalului de evenimente:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Setări generale** → **Interfață**.
3. În blocul **Notificări**, fă clic pe butonul **Configurează notificările**.

   Componentele și activitățile aplicației Kaspersky Endpoint Security se afișează în partea stângă a ferestrei. În partea dreaptă a ferestrei sunt prezentate evenimentele generate pentru componenta sau activitatea selectată.

   Evenimentele pot conține următoarele date de utilizatorului:

   - Căile către fișierele scanate de Kaspersky Endpoint Security.
   - Căi către chei de registru modificate în timpul funcționării Kaspersky Endpoint Security.

- Numele de utilizator Microsoft Windows.
- Adresele paginilor Web deschide de utilizator.

4. În stânga ferestrei, selectați componenta sau activitatea pentru care dorești să configurezi setările jurnalului de evenimente.
5. Bifați casetele de selectare de lângă evenimentele relevante din coloanele **Salvează în raportul local** și **Salvează în Jurnal evenimente Windows**.

   Evenimentele ale căror casete de selectare sunt bifate în coloana **Salvează în raportul local** sunt afișate în jurnalele aplicației. Evenimentele ale căror casete de selectare sunt bifate în coloana **Salvează în Jurnal evenimente Windows** sunt afișate în jurnalele Windows în canalul `Application`.
6. Salvați-vă modificările.

Configurarea afișării și livrării notificărilor

Pentru a configura afișarea și livrarea notificărilor:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Setări generale** → **Interfață**.
3. În blocul **Notificări**, fă clic pe butonul **Configurează notificările**.

   Componentele și activitățile aplicației Kaspersky Endpoint Security se afișează în partea stângă a ferestrei. În partea dreaptă a ferestrei sunt prezentate evenimentele generate pentru componenta sau activitatea selectată.

   Evenimentele pot conține următoarele date de utilizatorului:
   - Căile către fișierele scanate de Kaspersky Endpoint Security.
   - Căi către chei de registru modificate în timpul funcționării Kaspersky Endpoint Security.
   - Numele de utilizator Microsoft Windows.
   - Adresele paginilor Web deschide de utilizator.
4. În stânga ferestrei, selectați componenta sau activitatea pentru care dorești să configurezi furnizarea notificărilor.
5. În coloana **Notifică pe ecran**, bifați casetele de selectare de lângă evenimentele relevante.

   Informațiile despre evenimentele selectate se vor afișa pe ecran ca mesaje pop-up în zona de notificare a barei de activități Microsoft Windows.
6. În coloana **Notifică prin e-mail**, bifați casetele de selectare de lângă evenimentele relevante.

   Informațiile despre evenimentele selectate sunt livrate prin e-mail, dacă setările de livrare a notificărilor prin e-mail sunt configurate.
7. Fă clic pe **OK**.

8. Dacă ați activat notificările prin e-mail, configurați setările pentru livrarea prin e-mail:

   a. Fă clic pe **Configurează notificările prin e-mail**.

   b. Bifați caseta de selectare **Notifică despre evenimente** pentru a activa furnizarea de informații despre evenimentele Kaspersky Endpoint Security selectate în coloana **Notifică prin e-mail**.

   c. Specifică setările de livrare a notificărilor prin e-mail.

   d. Fă clic pe **OK**.

9. Salvați-vă modificările.

Configurarea afișării avertizărilor despre starea aplicației în zona de notificare

Pentru a configura afișarea avertizărilor despre starea aplicației în zona de notificare:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Setări generale** → **Interfață**.

3. În blocul **Afișează starea aplicației în zona de notificări**, bifați casetele de selectare de lângă acele categorii de evenimente despre care doriți să vedeți notificări în zona de notificare din Microsoft Windows.

4. Salvați-vă modificările.

Atunci când apar evenimente din categoria selectată, pictograma aplicație din zona de notificare se modifică în sau în, în funcție de gravitatea avertizării.

Mesajele între utilizatori și administrator

Componentele Application Control, Control dispozitive și Web Control și Adaptive Anomaly Control permit utilizatorilor computerelor din rețeaua LAN pe care este instalat Kaspersky Endpoint Security să trimită mesaje către administrator.

Un utilizator poate trimite un mesaj administratorului rețelei locale în următoarele cazuri:

- Componenta Control dispozitive a blocat accesul la dispozitiv.

  Șablonul de mesaj pentru solicitarea accesului la un dispozitiv blocat este disponibil în interfața Kaspersky Endpoint Security, în secțiunea Device Contro.

- Componenta Application Control a blocat pornirea unei aplicații.

  Șablonul de mesaj pentru a solicita permiterea pornirii unei aplicații blocate este disponibil în interfața Kaspersky Endpoint Security, în secțiunea Application Control.

- Componenta Control Web a blocat accesul la o resursă Web.

  Șablonul de mesaj pentru a solicita accesul la o resursă Web blocată este disponibil în interfața Kaspersky Endpoint Security, în secțiunea Web Control.

Metoda folosită pentru trimiterea mesajelor și șablonul utilizat depinde de existența sau nu a unei politici active Kaspersky Security Center pe computerul pe care este instalată aplicația Kaspersky Endpoint Security și de existența sau nu a unei conexiuni cu serverul de administrare Kaspersky Security Center. Sunt posibile următoarele scenarii:

- Dacă nu se execută o politică a aplicației Kaspersky Security Center pe computerul pe care este instalat Kaspersky Endpoint Security, se trimite prin e-mail un mesaj al utilizatorului către administratorul rețelei locale.

  Câmpurile mesajului sunt populate din șablonul definit în interfața locală a Kaspersky Endpoint Security.

- Dacă se execută o politică a aplicației Kaspersky Security Center pe computerul pe care este instalat Kaspersky Endpoint Security, se trimite mesajul standard către Serverul de administrare Kaspersky Security Center.

  În acest caz, mesajele utilizatorului sunt disponibile spre vizualizare în spațiul de stocare pentru evenimente Kaspersky Security Center (consultați instrucțiunile de mai jos). Câmpurile mesajului sunt populate cu valori din câmpurile șablonului definit în politica aplicației Kaspersky Security Center.

- Dacă pe computerul pe care este instalată aplicația Kaspersky Endpoint Security este folosită o politică Absent de la birou a Kaspersky Security Center, metoda folosită pentru trimiterea mesajelor depinde de existența sau nu a unei conexiuni la Kaspersky Security Center.

  - Dacă a fost stabilită o conexiune cu aplicația Kaspersky Security Center, Kaspersky Endpoint Security trimite mesajul standard către serverul de administrare Kaspersky Security Center.

  - Dacă lipsește o conexiune cu Kaspersky Security Center, se trimite un mesaj al utilizatorului către administratorul rețelei locale, prin e-mail.

  În ambele cazuri, câmpurile mesajului sunt populate cu valori din câmpurile șablonului definit în politica aplicației Kaspersky Security Center.

Pentru a vizualiza un mesaj de la un utilizator în spațiul de stocare a evenimentelor din Kaspersky Security Center:

1. Deschide Consolă de administrare a Kaspersky Security Center.

2. În nodul **Administration Server** din arborele consolei de administrare, selectați fila **Events**.

   Spațiul de lucru Kaspersky Security Center afișează toate evenimentele apărute în cursul funcționării Kaspersky Endpoint Security, inclusiv mesaje primite de administrator de la utilizatorii rețelei LAN.

3. Pentru a configura filtrul de evenimente, în lista verticală **Event selections**, selectați **User requests**.

4. Selectați mesajul trimis către administrator.

5. Faceți clic butonul **Open event properties window** în partea dreaptă a spațiului de lucru Consolă de administrare.

Gestionarea rapoartelor

Informațiile despre funcționarea fiecărei componente Kaspersky Endpoint Security, evenimentele de criptare de date, performanțele fiecărei activități de scanare, de actualizare și de verificare a integrității, precum și funcționarea generală a aplicației sunt înregistrate în rapoarte.

Rapoartele sunt stocate în directorul `C:\ProgramData\Kaspersky Lab\KES.14.1\Report`.

Rapoartele pot conține următoarele date de utilizatorului:

- Căile către fișierele scanate de Kaspersky Endpoint Security.
- Căi către chei de registru modificate în timpul funcționării Kaspersky Endpoint Security.
- Numele de utilizator Microsoft Windows.
- Adresele paginilor Web deschide de utilizator.

Datele din raport sunt prezentate sub formă de tabel. Fiecare rând din tabel conține informații despre un eveniment separat. Atributele de eveniment sunt localizate în coloanele tabelului. Anumite coloane sunt compuse și conțin coloane imbricate, cu atribute suplimentare. Pentru a vizualiza atribute suplimentare, faceți clic pe butonul ⊞ de lângă numele coloanei. Evenimentele care sunt înregistrate în jurnal în timpul funcționării diferitelor componente sau în timpul derulării diferitelor activități au seturi diferite de atribute.

Sunt disponibile următoarele rapoarte:

- Raport **Auditare sistem**. Conține informații despre evenimente apărute în cursul interacțiunii dintre utilizator și aplicație și în cursul funcționării aplicației în general, care nu sunt legate de nicio componentă sau activitate particulară a Kaspersky Endpoint Security.
- Rapoarte cu privire la funcționarea componentelor Kaspersky Endpoint Security.
- Rapoarte ale activităților Kaspersky Endpoint Security.
- Raport **Criptare date**. Conține informații despre evenimente apărute în cursul criptării sau decriptării datelor.

Rapoartele folosesc următoarele nivele de importanță pentru evenimente:

ⓘ **Mesaje de informare**. Evenimentele de referință care nu conțin de regulă informații importante.

⚠ **Avertismente**. Evenimente care solicită atenție, deoarece ele reflectă situații importante în funcționarea Kaspersky Endpoint Security.

ⓘ **Evenimente critice**. Evenimente de importanță critică indicând probleme în funcționarea Kaspersky Endpoint Security sau vulnerabilități în protecția computerului utilizatorului.

Pentru o procesare convenabilă a rapoartelor, poți modifica prezentarea datelor pe ecran în modurile următoare:

- Filtrare listă de evenimente după diferite criterii.
- Utilizare funcție de căutare pentru a găsi un anumit eveniment.

- Vizualizare eveniment selectat într-o secțiune separată.
- Sortare listă de evenimente după fiecare coloană a raportului.
- Afișare și ascundere evenimente grupate de filtrul de evenimente utilizând butonul ⊞.
- Modificare ordine și aranjare coloane prezentate în raport.

Poți salva un raport generat într-un fișier text, dacă este necesar. De asemenea, poți șterge informații de raport privind componentele și activitățile Kaspersky Endpoint Security care sunt combinate în grupuri.

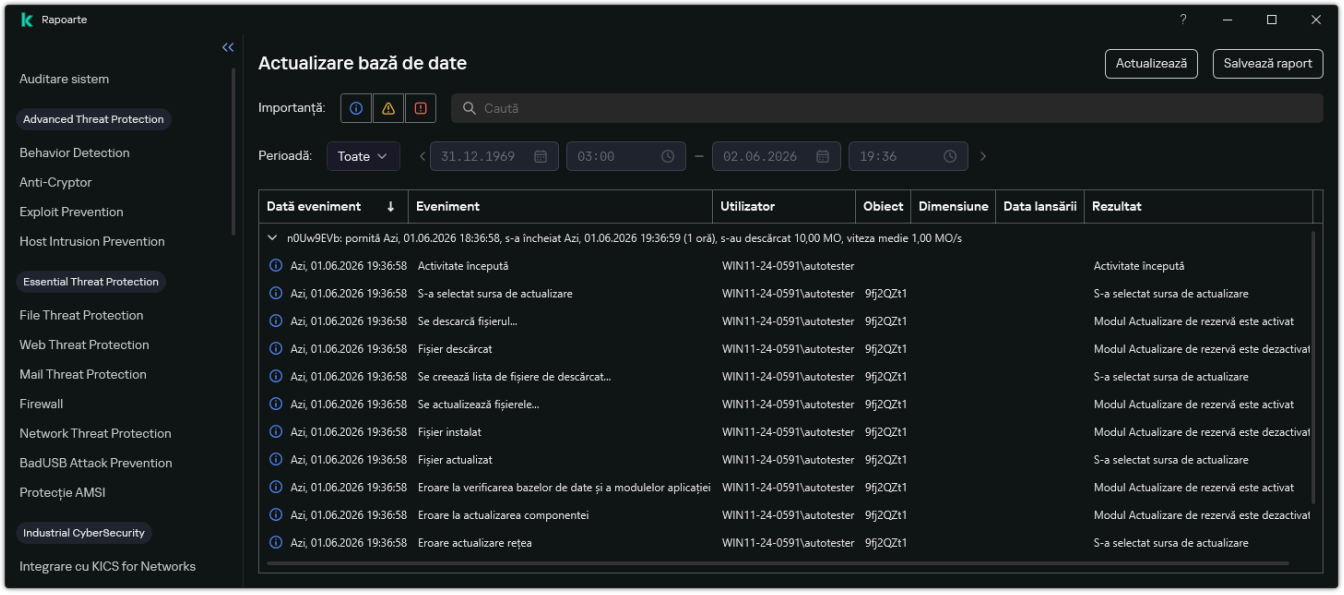
În cazul în care Kaspersky Endpoint Security se execută sub gestionarea Kaspersky Security Center, informațiile despre evenimente pot fi transmise către Kaspersky Security Center Administration Server(pentru mai multe detalii, consultați Ghidul de ajutor al Kaspersky Endpoint Security).

Vizualizarea rapoartelor

Dacă un utilizator poate vizualiza rapoartele, mai poate vizualiza toate evenimentele reflectate în rapoarte.

Pentru a vizualiza rapoarte:

1. În fereastra principală a aplicației, în secțiunea **Monitorizare**, faceți clic pe dala **Rapoarte**.



Rapoarte

2. În lista de componente și activități, selectează o componentă sau o activitate.

   Partea dreaptă a ferestrei afișează un raport care conține o listă de evenimente rezultate din funcționarea componentei selectate sau activității selectate a aplicației Kaspersky Endpoint Security. Poți sorta evenimente raport în funcție de valorile din celulele unei coloane.

3. Pentru a vizualiza informații detaliate despre un eveniment, selectați evenimentul în raport.

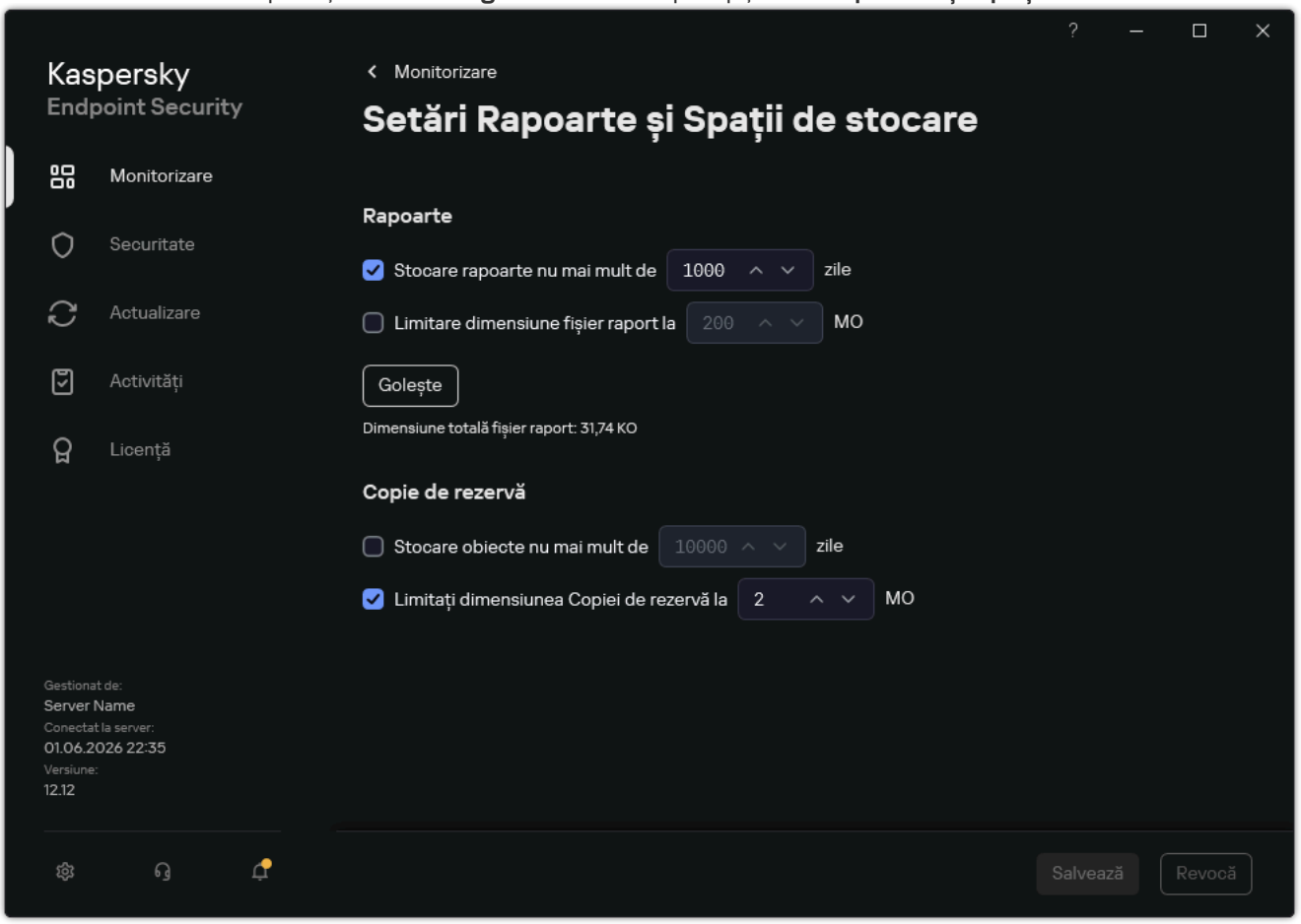
   În partea de jos a ferestrei este afișat un bloc cu sumarul evenimentului.

Configurarea duratei maxime de stocare a rapoartelor

Durata maximă implicită de stocare pentru rapoartele despre evenimentele înregistrate în jurnal de Kaspersky Endpoint Security este de 30 de zile. După această perioadă de timp, Kaspersky Endpoint Security șterge automat înregistrările cele mai vechi din fișierul de raport.

Pentru a modifica durata maximă de stocare a fișierelor:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra de setări a aplicației, în **Setări generale** fă clic pe opțiunea **Rapoarte și Spații de stocare**.



Setări rapoarte

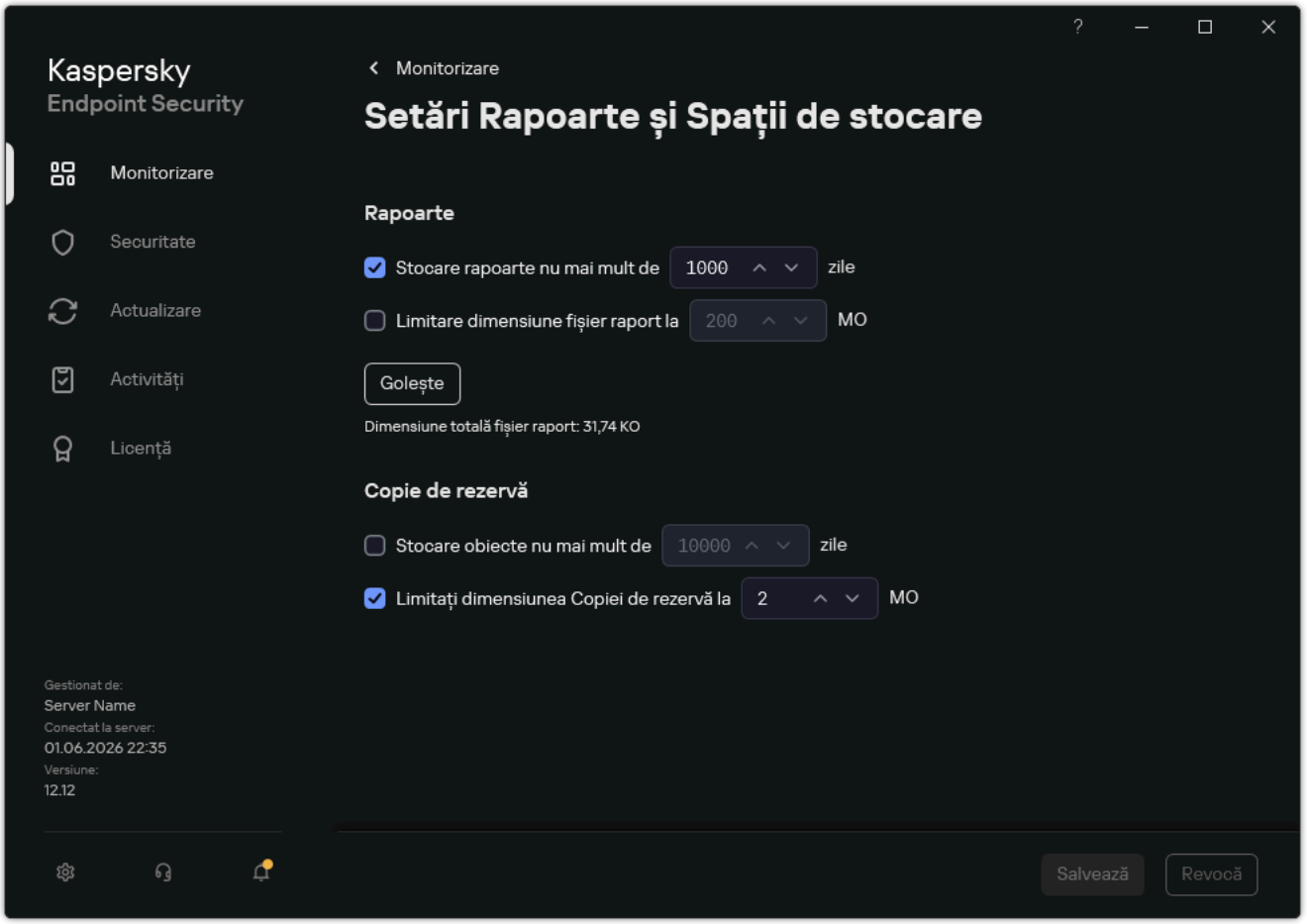
3. Dacă doriți să limitați termenul de stocare a raportului, bifați caseta de selectare **Stocare rapoarte nu mai mult de N zile** din blocul **Rapoarte**. Definiți durata maximă de stocare a rapoartelor.
4. Salvați-vă modificările.

Configurarea dimensiunii maxime a fișierului raport

Poți specifica dimensiunea maximă a fișierului care conține raportul. În mod implicit, dimensiunea maximă a fișierului raport este de 1.024 MB. Pentru a evita depășirea dimensiunii maxime a fișierului raport, Kaspersky Endpoint Security șterge automat înregistrările cele mai vechi din fișierul de raport atunci când este atinsă dimensiunea maximă a acestuia.

Pentru a configura dimensiunea maximă a fișierului raport:

1. În fereastra principală a aplicației, faceți clic pe butonul .
2. În fereastra de setări a aplicației, în **Setări generale** fă clic pe opțiunea **Rapoarte și Spații de stocare**.



Setări rapoarte

3. În blocul **Rapoarte**, bifați caseta de selectare **Limitare dimensiune fișier raport la N MO** dacă doriți să limitați dimensiunea unui fișier raport. Definiți dimensiunea maximă a fișierului raport.
4. Salvați-vă modificările.

Salvarea unui raport într-un fișier

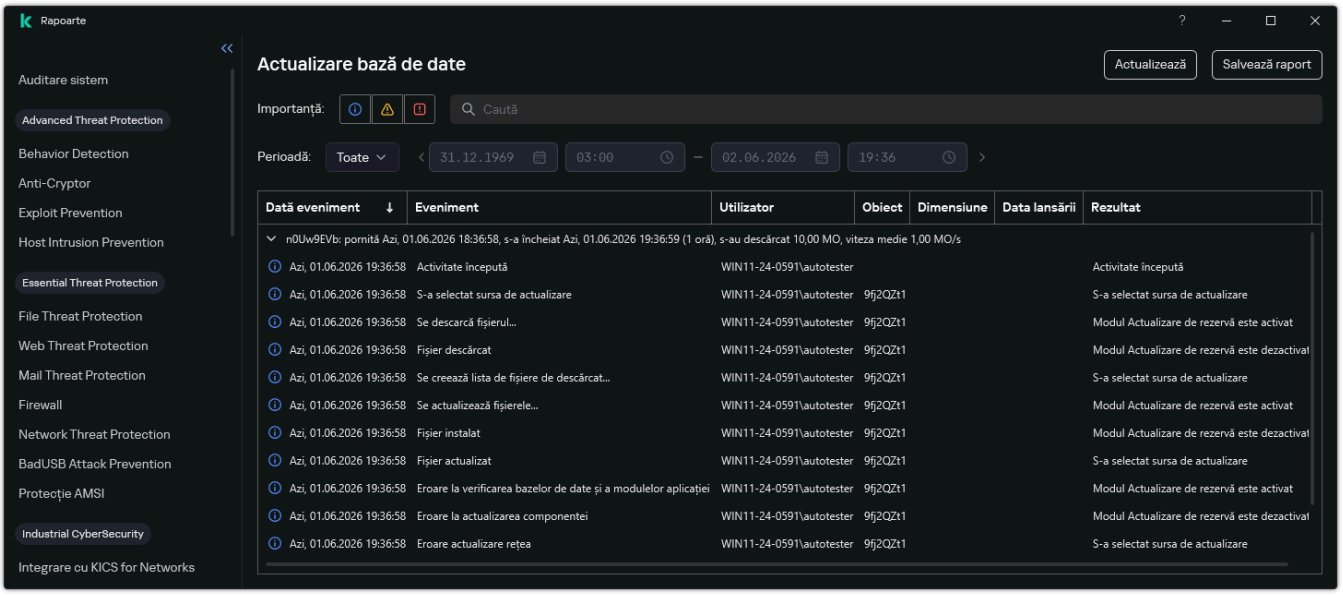
Utilizatorul răspunde personal pentru asigurarea securității informațiilor dintr-un raport salvat într-un fișier și, în special, pentru controlarea și restricționarea accesului la aceste informații.

Rapoartele pe care le generezi pot fi salvate în fișiere în format text (TXT) sau în fișiere CSV.

Kaspersky Endpoint Security înregistrează evenimentele în raport în același mod în care acestea sunt afișate pe ecran: cu alte cuvinte, cu același set și aceeași secvență de atribute de evenimente.

Pentru a salva un raport într-un fișier:

1. În fereastra principală a aplicației, în secțiunea **Monitorizare**, faceți clic pe dala **Rapoarte**.



Rapoarte

2. Se deschide o fereastră; în această fereastră, selectați componenta sau activitatea.

   Un raport se afișează în partea dreaptă a ferestrei și conține o listă de evenimente apărute în funcționarea componentei sau activității Kaspersky Endpoint Security selectate.

3. Dacă este necesar, poți modifica prezentarea datelor în raport:

   - Filtrând evenimentele
   - Executând o căutare de eveniment
   - Rearanjând coloanele
   - Sortând evenimentele

4. Faceți clic pe butonul **Salvează raport** în partea din dreapta sus a ferestrei.

5. În fereastra care se deschide, specificați folderul de destinație pentru fișierul de raport.

6. Introduceți numele fișierului raport.

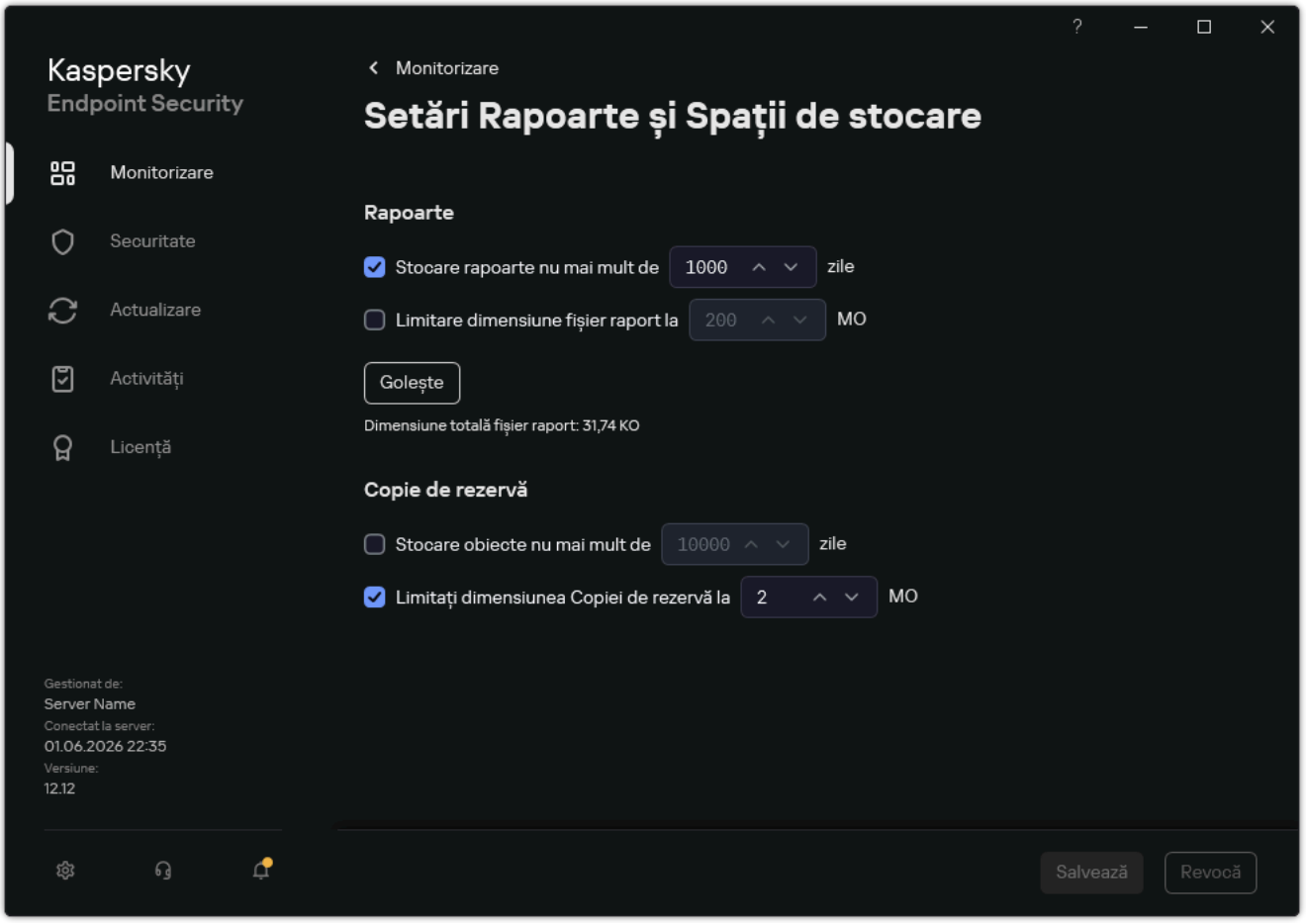
7. Selectați formatul necesar al fișierului raport: TXT sau CSV.

8. Salvați-vă modificările.

Golire rapoarte

Pentru a elimina informații din rapoarte:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra de setări a aplicației, în **Setări generale** fă clic pe opțiunea **Rapoarte și Spații de stocare**.



Setări rapoarte

3. În blocul **Rapoarte**, fă clic pe butonul **Golește**.
4. Dacă protecția prin parolă este activată, Kaspersky Endpoint Security vă poate solicita acreditările contului de utilizator. Aplicația solicită acreditările contului dacă utilizatorul nu are permisiunea necesară.

Kaspersky Endpoint Security va șterge toate rapoartele pentru toate componentele și activitățile aplicației.

Autoprotecția aplicației Kaspersky Endpoint Security

Autoprotecția împiedică alte aplicații să efectueze acțiuni care pot interfera cu funcționarea Kaspersky Endpoint Security și, de exemplu, să elimine Kaspersky Endpoint Security de pe computer. Setul de tehnologii de autoprotecție disponibile pentru Kaspersky Endpoint Security depinde de sistemul de operare, dacă este pe 32-biți sau pe 64-biți (consultați tabelul de mai jos). Autoprotecție include și Protecție prin parolă și Protecție conexiune Server de administrare.

Protecția prin parolă vă permite să restricționați accesul utilizatorilor la Kaspersky Endpoint Security în conformitate cu permisiunile acordate acestora (de exemplu, permisiunea de a părăsi aplicația).

Protecție conexiune Server de administrare previne reconectarea neautorizată a computerului la un server care nu este de încredere.

Tehnologii de autoprotecție Kaspersky Endpoint Security

Tehnologie	Descriere	Computer x86	Computer x64
Mecanism de autoprotecție	Tehnologia blochează accesul la următoarele componente ale aplicației: • fișierele din directorul de instalare Kaspersky Endpoint Security și alte fișiere ale aplicației; • cheile de regiștri cu înregistrări ce aparțin aplicației; • procesele pe care le execută aplicația.	✓	✓
AM-PPL (Antimalware Protected Process Light)	Tehnologia protejează procesele Kaspersky Endpoint Security împotriva acțiunilor rău intenționate. Pentru mai multe detalii despre tehnologia AM-PPL, vizitați site-ul web Microsoft. Tehnologia AM-PPL este disponibilă pentru Windows 10 versiunea 1703 (RS2) sau ulterioară și pentru sistemele de operare Windows Server 2019.	✓	✓
Mecanism de apărare împotriva gestionării externe	Această tehnologie împiedică alte aplicații (de exemplu, TeamViewer sau RemotelyAnywhere) să obțină acces la Kaspersky Endpoint Security.	✓	– (cu excepția Windows 7)

Activarea și dezactivarea Autoprotecției

Kaspersky Endpoint Security previne alterarea sau ștergerea fișierelor aplicației de pe unitatea de hard disk, a proceselor de memorie și a înregistrărilor din registry-ul sistemului.

Tehnologia blochează accesul la următoarele componente ale aplicației:

- fișierele din directorul de instalare Kaspersky Endpoint Security și alte fișiere ale aplicației;
- cheile de regiștri cu înregistrări ce aparțin aplicației;
- procesele pe care le execută aplicația.

Mecanismul de autoprotecție a aplicației Kaspersky Endpoint Security este activat în mod implicit.

Cum se activează sau dezactivează componenta Autoprotecție în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Setări generale** → **Setări aplicație**.
4. Utilizați caseta de selectare **Activează Autoprotecție** pentru a activa sau dezactiva mecanismul de Autoprotecție.
5. Salvați-vă modificările.

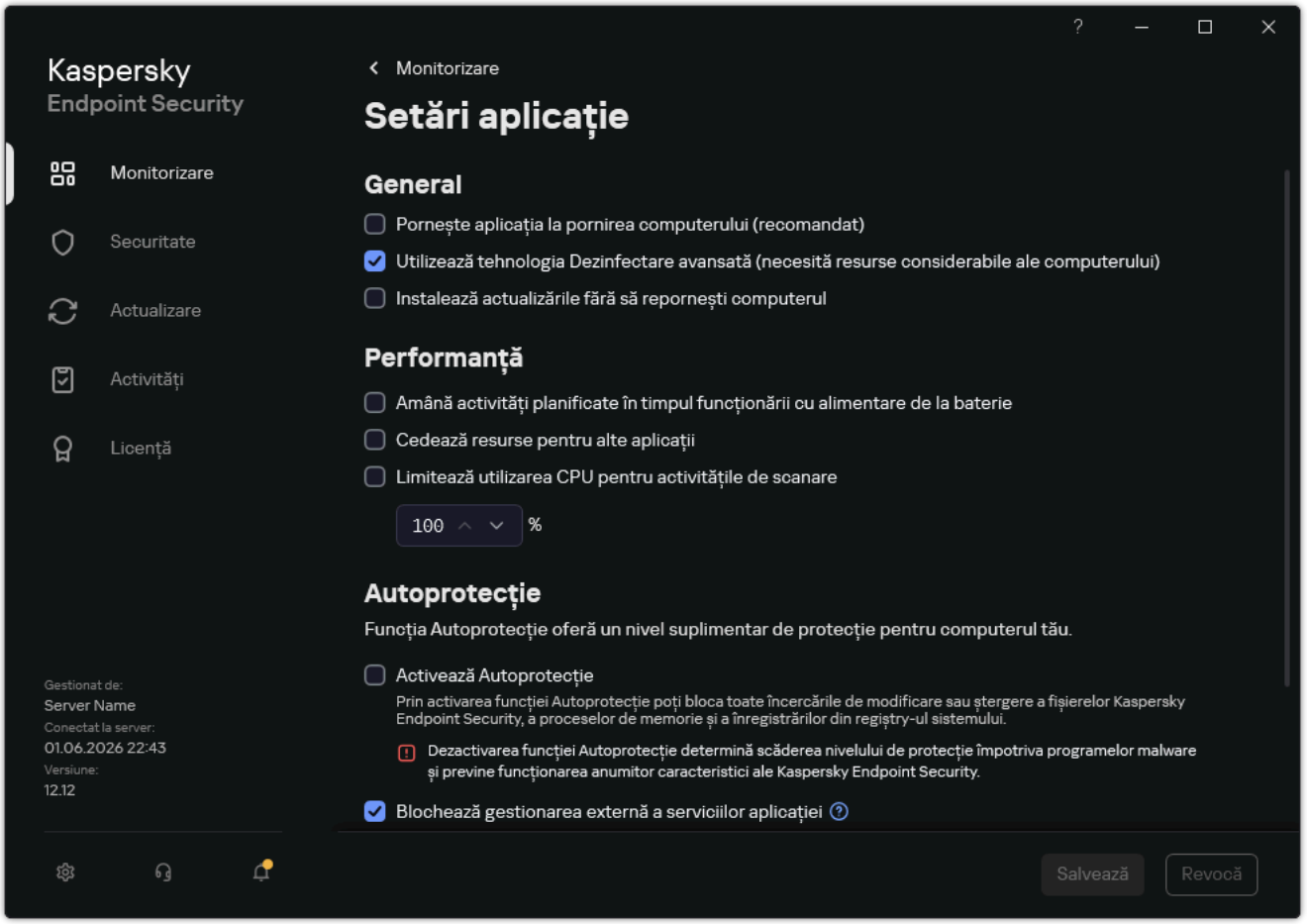
Cum se activează sau dezactivează componenta Autoprotecție în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **General Settings** → **Self-Defense**.
5. Utilizează comutatorul **Self-Defense ENABLED** pentru a activa sau dezactiva mecanismul de Autoprotecție.
6. Salvați-vă modificările.

Cum se activează sau dezactivează componenta Autoprotecție în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul .
2. În fereastra cu setările aplicației, selectați **Setări generale** → **Setări aplicație**.



Setări Kaspersky Endpoint Security for Windows

3. Utilizați caseta de selectare **Activează Autoprotecție** pentru a activa sau dezactiva mecanismul de Autoprotecție.
4. Salvați-vă modificările.

Activarea și dezactivarea suportului pentru AM-PPL

Kaspersky Endpoint Security acceptă tehnologia Antimalware Protected Process Light (denumită în continuare „AM-PPL") de la Microsoft. AM-PPL protejează procesele Kaspersky Endpoint Security împotriva acțiunilor dăunătoare (de exemplu, închiderea aplicației). AM-PPL permite executarea numai a proceselor de încredere. Procesele Kaspersky Endpoint Security sunt semnate în conformitate cu cerințele de securitate Windows și, prin urmare, sunt de încredere. Pentru mai multe detalii despre tehnologia AM-PPL, vizitați site-ul web Microsoft. Tehnologia AM-PPL este activată implicit.

Kaspersky Endpoint Security are, de asemenea, mecanisme integrate pentru protejarea proceselor aplicației. Suportul pentru AM-PPL vă permite să delegați funcțiile de securitate ale proceselor în sistemul de operare. Puteți crește astfel viteza aplicației și puteți reduce consumul de resurse ale computerului.

Utilizează continuu tehnologia AM-PPL. AM-PPL este o componentă importantă a protecției sistemului de operare. Dezactivarea suportului AM-PPL poate cauza funcționarea defectuoasă a unor caracteristici Kaspersky Endpoint Security (de exemplu, integrarea aplicației cu Windows Security Center). Dezactivarea suportului AM-PPL este permisă numai într-un mediu de testare separat, în scopul depanării.

Tehnologia AM-PPL este disponibilă pentru Windows 10 versiunea 1703 (RS2) sau ulterioară și pentru sistemele de operare Windows Server 2019.

Pentru a activa sau dezactiva tehnologia AM-PPL:

1. Opriți mecanismul de autoprotecție al aplicației.

   Mecanismul de autoprotecție previne modificarea și ștergerea proceselor aplicației din memoria computerului, inclusiv schimbarea stării AM-PPL.

2. Executați interpretorul de linii de comandă (cmd.exe) ca administrator.

3. Deschideți directorul în care se află fișierul executabil Kaspersky Endpoint Security.

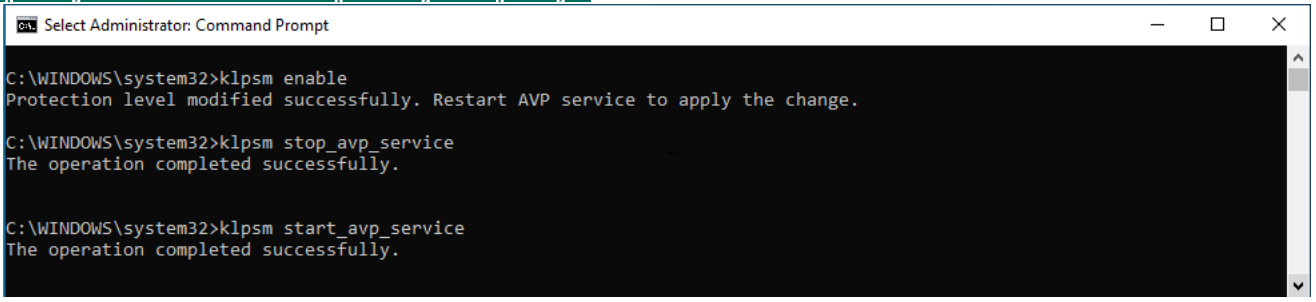
   Puteți adăuga calea către fișierul executabil la variabila de sistem %PATH% în timpul instalării aplicației.

4. Tastați următoarele în linia de comandă:

   - `klpsm.exe enable` - activați suportul pentru tehnologia AM-PPL (consultați figura de mai jos).
   - `klpsm.exe disable` - dezactivați suportul pentru tehnologia AM-PPL.

5. Repornește Kaspersky Endpoint Security.

6. Reporniți mecanismul de autoprotecție al aplicației.



Activarea suportului pentru tehnologia AM-PPL

Protejarea serviciilor aplicației împotriva gestionării externe

Protejarea serviciilor aplicației împotriva gestionării externe blochează încercările utilizatorilor și ale altor aplicații să oprească serviciile Kaspersky Endpoint Security. Protecția asigură funcționarea următoarelor servicii:

- Serviciul Kaspersky Endpoint Security (AVP.KES.14.1)
- Serviciul Kaspersky Seamless Update Service (AVPSUS.KES.14.1)

Pentru a părăsi aplicația din linia de comandă, dezactivați protecția serviciilor Kaspersky Endpoint Security împotriva gestionării externe.

Poți permite gestionarea externă a serviciilor aplicației numai pe computere care nu acceptă tehnologia AM-PPL sau pe computere care au tehnologia dezactivată.

Cum se activează sau dezactivează Protejarea serviciilor aplicației împotriva gestionării externe în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Setări generale** → **Setări aplicație**.
4. Utilizați caseta de selectare **Blochează gestionarea externă a serviciilor aplicației** pentru a activa sau dezactiva protecția serviciilor Kaspersky Endpoint Security împotriva gestionării externe.
5. Salvați-vă modificările.

Cum se activează sau dezactivează Protejarea serviciilor aplicației împotriva gestionării externe în Web Console și Cloud Console

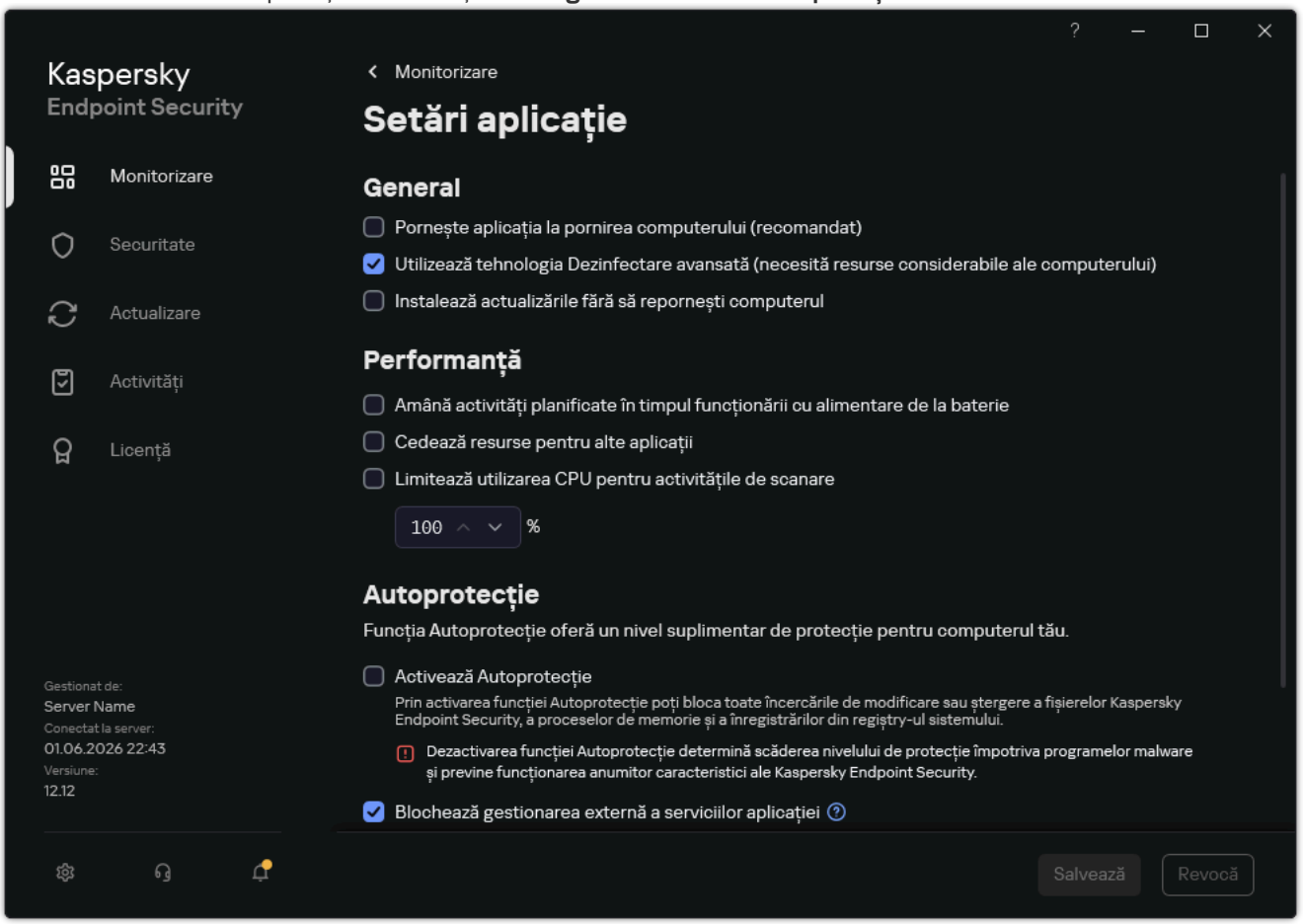
1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **General Settings** → **Self-Defense**.
5. Utilizați caseta de selectare **Block external management of application services** pentru a activa sau dezactiva protecția serviciilor Kaspersky Endpoint Security împotriva gestionării externe.
6. Salvați-vă modificările.

Cum se activează sau dezactivează Protejarea serviciilor aplicației împotriva gestionării externe în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Setări generale** → **Setări aplicație**.

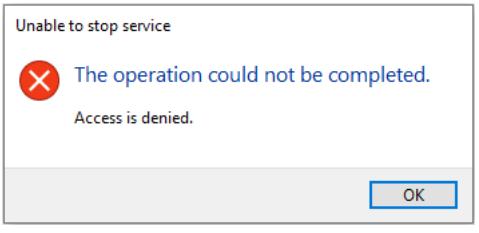


Setări Kaspersky Endpoint Security for Windows

3. Utilizați caseta de selectare **Blochează gestionarea externă a serviciilor aplicației** pentru a activa sau dezactiva protecția serviciilor Kaspersky Endpoint Security împotriva gestionării externe.

4. Salvați-vă modificările.

Drept urmare, atunci când un utilizator încearcă să oprească serviciile aplicației, apare o fereastră de sistem care conține un mesaj de eroare. Utilizatorul poate gestiona serviciile aplicației doar din interfața Kaspersky Endpoint Security.



Eroare privind accesul la serviciile aplicației

Acceptarea aplicațiilor de administrare la distanță

Ocazional, este posibil să aveți nevoie să folosiți o aplicație de administrare la distanță, în timp ce este activată protecția împotriva gestionării externe.

Pentru a activa funcționarea aplicațiilor de administrare la distanță:

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Setări generale → Excluderi și tipuri de obiecte detectate**.
3. În blocul **Excluderi**, faceți clic pe linkul **Specifică aplicațiile de încredere**.
4. În fereastra care se deschide, faceți clic pe butonul **Adaugă**.
5. Selectați fișierul executabil al aplicației de administrare la distanță.

   De asemenea, puteți introduce calea manual. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști.
6. Bifați caseta de selectare **Permite interacțiunea cu interfața Kaspersky Endpoint Security**.
7. Salvați-vă modificările.

Protecția prin parolă

Pe un computer pot avea acces mai mulți utilizatori, cu niveluri diferite de cunoștințe privind computerele. Dacă utilizatorii ar avea acces nelimitat la Kaspersky Endpoint Security și la setările sale, nivelul general de protecție a computerului s-ar putea reduce. Protecția prin parolă vă permite să restricționați accesul utilizatorilor la Kaspersky Endpoint Security în conformitate cu permisiunile acordate acestora (de exemplu, permisiunea de a părăsi aplicația).

Dacă utilizatorul care a pornit sesiunea Windows (*utilizatorul sesiunii*) are permisiunea de a efectua acțiunea, Kaspersky Endpoint Security nu solicită numele de utilizator și parola sau o parolă temporară. Utilizatorul primește acces la Kaspersky Endpoint Security în conformitate cu permisiunile acordate.

Dacă un utilizator de sesiune nu are permisiunea de a efectua o acțiune, utilizatorul poate obține acces la aplicație în următoarele moduri:

- Introdu un nume de utilizator și parola.

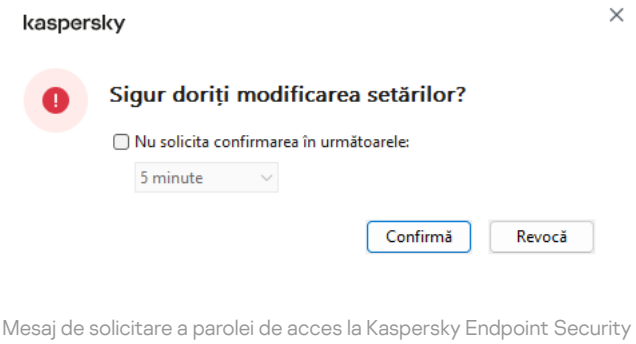
  Această metodă este adecvată pentru operațiile de zi cu zi. Pentru a efectua o acțiune protejată prin parolă, trebuie să introduceți acreditările contului de domeniu ale utilizatorului cu permisiunea necesară. În acest caz, computerul trebuie să fie în acel domeniu. Dacă computerul nu face parte din domeniu, poți utiliza contul KLAdmin sau un cont adăugat manual.

- Introdu o parolă temporară.

  Această metodă este adecvată pentru acordarea permisiunilor temporare de efectuare a acțiunilor blocate (de exemplu, ieșirea din aplicație) utilizatorilor din afara rețelei corporației. Când o parolă temporară expiră sau când o sesiune se încheie, Kaspersky Endpoint Security readuce setările la starea inițială.

Când un utilizator încearcă să efectueze o acțiune protejată prin parolă, Kaspersky Endpoint Security solicită utilizatorului numele de utilizator și parola sau o parolă temporară (vezi figura de mai jos).

În fereastra de introducere a parolei, puteți schimba limba doar apăsând **ALT+SHIFT**. Utilizarea altor comenzi rapide, chiar dacă sunt configurate în sistemul de operare, nu funcționează pentru comutarea limbilor.



Mesaj de solicitare a parolei de acces la Kaspersky Endpoint Security

Nume de utilizator și parolă

Pentru a accesa Kaspersky Endpoint Security, trebuie să introduci acreditările contului. Protecția prin parolă este compatibilă cu următoarele conturi:

- **KLAdmin**. Un cont de administrator cu acces nerestricționat la Kaspersky Endpoint Security. Contul KLAdmin are dreptul de a efectua orice acțiune care este protejată prin parolă. Permisiunile pentru contul KLAdmin nu pot fi revocate. Când activezi protecția prin parolă, Kaspersky Endpoint Security îți solicită să setezi o parolă pentru contul KLAdmin.

- **Cont adăugat manual**. Un cont din afara domeniului Active Directory. Poți utiliza acest cont de serviciu în loc de KLAdmin dacă nu dorești să partajezi parola de administrator. Poți seta orice nume de utilizator și orice parolă și poți configura permisiuni individuale.

- **Grupul Toți**. Un grup încorporat în Windows care include toți utilizatorii din rețeaua corporației. Utilizatorii din grupul Toți pot să acceseze aplicația în conformitate cu permisiunile care le sunt acordate.

- **Utilizatori individuali sau grupuri**. Conturi de utilizatori pentru care poți să configurezi permisiuni individuale. De exemplu, dacă o acțiune este blocată pentru grupul Toți, poți să permiți această acțiune pentru un utilizator individual sau pentru un grup.

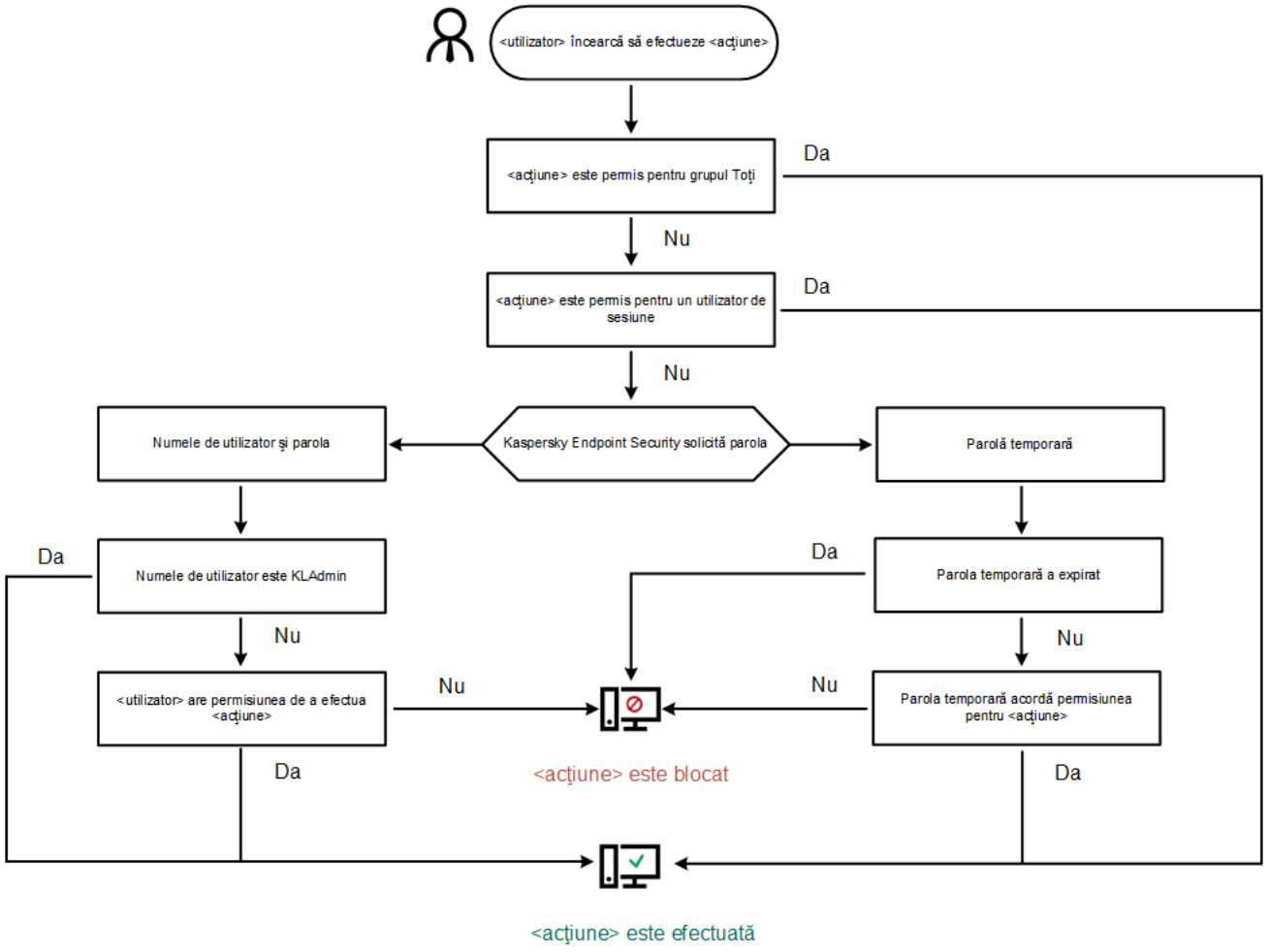
- **Utilizator de sesiune**. Contul utilizatorului care a inițiat sesiunea Windows. Poți să comuți la un alt utilizator de sesiune când ți se solicită o parolă (caseta de selectare **Salvează parolă pentru sesiunea curentă**). În acest caz, Kaspersky Endpoint Security tratează ca utilizator de sesiune utilizatorul ale căror acreditări de cont au fost introduse și nu utilizatorul care a inițiat sesiunea Windows.

Parolă temporară

Se poate utiliza o parolă temporară pentru a acorda acces temporar la Kaspersky Endpoint Security pentru un computer individual din afara rețelei companiei. Administratorul generează o parolă temporară pentru un computer individual în proprietățile computerului din Kaspersky Security Center. Administratorul selectați acțiunile care vor fi protejate cu parola temporară și specifică perioada de valabilitate a parolei temporare.

Algoritmul de funcționare a protecției prin parolă

Kaspersky Endpoint Security decide dacă va permite sau va bloca o acțiune protejată prin parolă pe baza următorului algoritm (vezi figura de mai jos).



Algoritmul de funcționare a protecției prin parolă

Activarea protecției prin parolă

Protecția prin parolă vă permite să restricționați accesul utilizatorilor la Kaspersky Endpoint Security în conformitate cu permisiunile acordate acestora (de exemplu, permisiunea de a părăsi aplicația).

Cum se activează Protecția prin parolă în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Setări generale** → **Interfață**.
4. În blocul **Protecție prin parolă**, fă clic pe butonul **Setări**.

   Aceasta deschide o fereastră cu setările Protecției prin parolă.
5. Utilizează caseta de selectare **Activează protecția prin parolă** pentru a activa sau a dezactiva componenta.

6. În **Permisiuni**, selectați contul KLAdmin.
7. Aceasta deschide o fereastră; în acea fereastră, faceți clic pe **Parolă** și setați o parolă pentru contul KLAdmin.

   Contul KLAdmin are dreptul de a efectua orice acțiune care este protejată prin parolă.

   > Dacă ai uitat parola contului KLAdmin, poți reseta parola în proprietățile politicii.

8. Reveniți la lista de conturi.
9. Setați permisiuni pentru toți utilizatorii din rețeaua corporației:

   a. În **Permisiuni**, selectați grupul „Oricine”.

      Grupul Toți este un grup încorporat în Windows care include toți utilizatorii din rețeaua corporației.

   b. În fereastra care se deschide, bifați casetele de selectare de lângă acțiunile pe care utilizatorii vor avea permisiunea de a le efectua fără a introduce parola.

      În cazul în care o casetă de selectare este debifată, utilizatorii sunt blocați pentru efectuarea acțiunii. De exemplu, în cazul în care caseta de selectare de lângă permisiunea **Părăsește aplicația** este debifată, puteți părăsi aplicația numai dacă sunteți conectat ca KLAdmin sau ca utilizator individual care are permisiunea necesară ori dacă introduceți o parolă temporară.

      > Permisiunile Protecție prin parolă au câteva aspecte importante care trebuie luate în considerare. Asigurați-vă că toate condițiile pentru accesarea aplicației Kaspersky Endpoint Security sunt îndeplinite.

10. Salvați-vă modificările.

Cum se activează Protecția prin parolă în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.
4. Accesați **General Settings** → **Self-Defense**.
5. În **Password Protection**, utilizați comutatorul **Password Protection ENABLED** pentru a activa sau dezactiva componenta.
6. Specificați parola pentru contul KLAdmin și confirmați-o.

   Contul KLAdmin are dreptul de a efectua orice acțiune care este protejată prin parolă.

   > Dacă ai uitat parola contului KLAdmin, poți reseta parola în proprietățile politicii.

7. Reveniți la lista de conturi.

8. Setați permisiuni pentru toți utilizatorii din rețeaua corporației:

   a. În tabelul de conturi, selectați grupul „Oricine”.

      Grupul Toți este un grup încorporat în Windows care include toți utilizatorii din rețeaua corporației.

   b. În fereastra care se deschide, bifați casetele de selectare de lângă acțiunile pe care utilizatorii vor avea permisiunea de a le efectua fără a introduce parola.

      În cazul în care o casetă de selectare este debifată, utilizatorii sunt blocați pentru efectuarea acțiunii. De exemplu, în cazul în care caseta de selectare de lângă permisiunea **Exit the application** este debifată, puteți părăsi aplicația numai dacă sunteți conectat ca KLAdmin sau ca utilizator individual care are permisiunea necesară ori dacă introduceți o parolă temporară.

      Permisiunile Protecție prin parolă au câteva aspecte importante care trebuie luate în considerare. Asigurați-vă că toate condițiile pentru accesarea aplicației Kaspersky Endpoint Security sunt îndeplinite.

9. Salvați-vă modificările.

Cum se activează Protecția prin parolă în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Setări generale** → **Interfață**.

3. Utilizați comutatorul **Protecție prin parolă** pentru a activa sau a dezactiva componenta.

4. Specificați parola pentru contul KLAdmin și confirmați-o.

   Contul KLAdmin are dreptul de a efectua orice acțiune care este protejată prin parolă.

   Dacă un computer funcționează în baza unei politici, administratorul poate să reseteze parola pentru contul KLAdmin în proprietățile politicii. În cazul în care computerul nu este conectat la Kaspersky Security Center și ați uitat parola pentru contul KLAdmin, nu este posibilă recuperarea parolei.

5. Setați permisiuni pentru toți utilizatorii din rețeaua corporației:

   a. În tabelul contului, faceți clic pe butonul **Editează** pentru a deschide lista de permisiuni pentru grupul Oricine.

      Grupul Toți este un grup încorporat în Windows care include toți utilizatorii din rețeaua corporației.

   b. Bifați casetele de selectare de lângă acțiunile pe care utilizatorii vor avea permisiunea de a le efectua fără a introduce parola.

      În cazul în care o casetă de selectare este debifată, utilizatorii sunt blocați pentru efectuarea acțiunii. De exemplu, în cazul în care caseta de selectare de lângă permisiunea **Părăsește aplicația** este debifată, puteți părăsi aplicația numai dacă sunteți conectat ca KLAdmin sau ca utilizator individual care are permisiunea necesară ori dacă introduceți o parolă temporară.

      Permisiunile Protecție prin parolă au câteva aspecte importante care trebuie luate în considerare. Asigurați-vă că toate condițiile pentru accesarea aplicației Kaspersky Endpoint Security sunt îndeplinite.

6. Salvați-vă modificările.

Când protecția prin parolă este activată, aplicația va restricționa accesul utilizatorilor la Kaspersky Endpoint Security în conformitate cu permisiunile acordate grupului Toți. Puteți efectua acțiunile care sunt blocate pentru grupul Toți numai dacă folosiți contul KLAdmin, un alt cont căruia i s-au acordat permisiunile necesare sau dacă introduceți o parolă temporară.

Puteți dezactiva protecția prin parolă numai dacă sunteți autentificat ca KLAdmin. Nu este posibil să dezactivați protecția prin parolă dacă utilizați un alt cont de utilizator sau o parolă temporară.

Cu ocazia verificării parolei, puteți să bifați caseta de selectare **Salvează parolă pentru sesiunea curentă**. În acest caz, Kaspersky Endpoint Security nu va solicita nicio parolă atunci când un utilizator va încerca să efectueze o altă acțiune protejată prin parolă pe durata sesiunii.

Acordarea de permisiuni utilizatorilor individuali sau grupurilor

Protecția prin parolă permite acordarea accesului componentei Kaspersky Endpoint Security la conturile de utilizator Active Directory individuale și la conturile de utilizator adăugate manual.

Conturile de utilizator Active Directory

Poți acorda acces la Kaspersky Endpoint Security unor utilizatori individuali sau grupuri din cadrul domeniului Active Directory. De exemplu, dacă părăsirea aplicației este blocată pentru grupul Toți, poți acorda permisiunea **Părăsește aplicația** unui utilizator individual. Prin urmare, poți părăsi aplicația numai dacă ești conectat ca acel utilizator sau ca KLAdmin.

Puteți utiliza acreditările contului pentru a accesa aplicația numai dacă computerul este în domeniu. Dacă computerul nu este în domeniu, puteți utiliza contul KLAdmin sau o parolă temporară.

Conturile de utilizator adăugate manual

Poți să creezi un cont de utilizator care nu este prezent în Active Directory și să atribui permisiuni individuale acestui cont de utilizator. Adică, poți crea un *cont de utilizator de serviciu* și îl poți utiliza în locul lui KLAdmin. Astfel, nu trebuie să partajezi parola KLAdmin cu alți utilizatori sau să creezi noi conturi de utilizator Active Directory. Poți specifica orice nume de utilizator și orice parolă. De exemplu, poți să acorzi permisiunea **Vizualizează rapoarte** pentru contul de utilizator al serviciului. Drept rezultat, dacă vizualizarea rapoartelor este interzisă pentru grupul „Toți”, poți deschide rapoartele utilizând contul de utilizator al serviciului sau contul de utilizator KLAdmin.

Acordarea de permisiuni utilizatorilor individuali sau grupurilor

Cum se acordă permisiuni utilizatorilor individuali sau grupurilor în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

3. În fereastra politicii, selectați **Setări generale** → **Interfață**.

4. În blocul **Protecție prin parolă**, fă clic pe butonul **Setări**.

   Aceasta deschide o fereastră cu setările Protecției prin parolă.

5. În tabelul contului, faceți clic **Adaugă**.

6. Selectează tipul resursei pe care dorești să o adaugi:

   - **Selectează un utilizator/grup din Active Directory** – conturile de utilizator Active Directory

     Pentru a selecta un cont de utilizator, fă clic pe **Selectează**. Selectați un utilizator sau un grup în Active Directory și confirmă selecția.

   - **Adaugă manual un utilizator / grup de utilizatori** pentru un cont de utilizator al serviciului adăugat manual.

     Pentru a adăuga un cont de utilizator al serviciului, introdu un nume de utilizator și o parolă (de exemplu, SecureAdmin).

     > Puteți reseta parola unui cont de utilizator de servicii în setările politicii. Parola contului de utilizator al serviciului trebuie resetată în același mod ca și parola KLAdmin. Dacă este permisă editarea setărilor componentei Protecție prin parolă („lacătul" este deschis) sau dacă nu este aplicată nicio politică pe computer, poți reseta parola contului de utilizator de serviciu în interfața aplicației. Pentru a face acest lucru, confirmă modificarea informațiilor contului de utilizator de servicii utilizând parola KLAdmin.

7. În lista **Permisiuni**, bifați casetele de selectare de lângă acțiunile pe care utilizatorul sau grupul selectat va avea permisiunea să le efectueze fără a li se solicita o parolă.

   În cazul în care o casetă de selectare este debifată, utilizatorii sunt blocați pentru efectuarea acțiunii. De exemplu, în cazul în care caseta de selectare de lângă permisiunea **Părăsește aplicația** este debifată, puteți părăsi aplicația numai dacă sunteți conectat ca KLAdmin sau ca utilizator individual care are permisiunea necesară ori dacă introduceți o parolă temporară.

   > Permisiunile Protecție prin parolă au câteva aspecte importante care trebuie luate în considerare. Asigurați-vă că toate condițiile pentru accesarea aplicației Kaspersky Endpoint Security sunt îndeplinite.

8. Salvați-vă modificările.

Cum se acordă permisiuni utilizatorilor individuali sau grupurilor în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **General Settings** → **Self-Defense**.

5. În blocul **Password Protection**, faceți clic pe linkul **User permissions**.

   Această acțiune deschide formularul pentru acordarea permisiunilor de activare a parolei.

6. Fă clic pe **Add**.

7. Selectează tipul resursei pe care dorești să o adaugi:

   - **Select from Active Directory** – conturile de utilizator Active Directory

     Pentru a selecta un cont de utilizator, fă clic pe **Edit**. Selectați un utilizator sau un grup în Active Directory și confirmă selecția.

   - **Add manually** pentru un cont de utilizator al serviciului adăugat manual.

     Pentru a adăuga un cont de utilizator al serviciului, introdu un nume de utilizator și o parolă (de exemplu, SecureAdmin).

     > Puteți reseta parola unui cont de utilizator de servicii în setările politicii. Parola contului de utilizator al serviciului trebuie resetată în același mod ca și parola KLAdmin. Dacă este permisă editarea setărilor componentei Protecție prin parolă („lacătul" este deschis) sau dacă nu este aplicată nicio politică pe computer, poți reseta parola contului de utilizator de serviciu în interfața aplicației. Pentru a face acest lucru, confirmă modificarea informațiilor contului de utilizator de servicii utilizând parola KLAdmin.

8. În lista **Permissions**, bifați casetele de selectare de lângă acțiunile pe care utilizatorul sau grupul selectat va avea permisiunea să le efectueze fără a li se solicita o parolă.

   În cazul în care o casetă de selectare este debifată, utilizatorii sunt blocați pentru efectuarea acțiunii. De exemplu, în cazul în care caseta de selectare de lângă permisiunea **Exit the application** este debifată, puteți părăsi aplicația numai dacă sunteți conectat ca KLAdmin sau ca utilizator individual care are permisiunea necesară ori dacă introduceți o parolă temporară.

   > Permisiunile Protecție prin parolă au câteva aspecte importante care trebuie luate în considerare. Asigurați-vă că toate condițiile pentru accesarea aplicației Kaspersky Endpoint Security sunt îndeplinite.

9. Fă clic pe **Add**.

10. Salvați-vă modificările.

Cum se acordă permisiuni utilizatorilor individuali sau grupurilor în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Setări generale** → **Interfață**.

3. În tabelul contului, faceți clic **Adaugă**.

4. Selectează tipul resursei pe care dorești să o adaugi:

   - **Selectează un utilizator/grup din Active Directory** – conturile de utilizator Active Directory

     Pentru a selecta un cont de utilizator, fă clic pe **Selectează utilizatorul sau grupul**. Selectați un utilizator sau un grup în Active Directory și confirmă selecția.

   - **Adaugă manual un utilizator** pentru un cont de utilizator al serviciului adăugat manual.

     Pentru a adăuga un cont de utilizator al serviciului, introdu un nume de utilizator și o parolă (de exemplu, SecureAdmin).

Puteți reseta parola unui cont de utilizator de servicii în setările politicii. Parola contului de utilizator al serviciului trebuie resetată în același mod ca și parola KLAdmin. Dacă este permisă editarea setărilor componentei Protecție prin parolă („lacătul" este deschis) sau dacă nu este aplicată nicio politică pe computer, poți reseta parola contului de utilizator de serviciu în interfața aplicației. Pentru a face acest lucru, confirmă modificarea informațiilor contului de utilizator de servicii utilizând parola KLAdmin.

5. În lista **Permisiuni**, bifați casetele de selectare de lângă acțiunile pe care utilizatorul sau grupul selectat va avea permisiunea să le efectueze fără a li se solicita o parolă.

   În cazul în care o casetă de selectare este debifată, utilizatorii sunt blocați pentru efectuarea acțiunii. De exemplu, în cazul în care caseta de selectare de lângă permisiunea **Părăsește aplicația** este debifată, puteți părăsi aplicația numai dacă sunteți conectat ca KLAdmin sau ca utilizator individual care are permisiunea necesară ori dacă introduceți o parolă temporară.

   Permisiunile Protecție prin parolă au câteva aspecte importante care trebuie luate în considerare. Asigurați-vă că toate condițiile pentru accesarea aplicației Kaspersky Endpoint Security sunt îndeplinite.

6. Salvați-vă modificările.

Ca urmare, dacă accesul la aplicație este restricționat pentru grupul Toți, utilizatorii vor primi permisiuni de accesare a aplicației Kaspersky Endpoint Security în conformitate cu permisiunile individuale ale utilizatorilor.

Utilizarea unei parole temporare pentru acordarea de permisiuni

Se poate utiliza o parolă temporară pentru a acorda acces temporar la Kaspersky Endpoint Security pentru un computer individual din afara rețelei companiei. Acest lucru este necesar pentru a permite utilizatorului să efectueze o acțiune blocată fără a obține acreditările contului KLAdmin. Pentru a utiliza o parolă temporară, computerul trebuie să adăugat la Kaspersky Security Center.

Cum permiți unui utilizator să efectueze o acțiune blocată utilizând o parolă temporară prin Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Managed devices** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectează fila **Devices**.
4. Fă dublu clic pentru a deschide fereastra cu proprietățile computerului.
5. În fereastra cu proprietățile computerului, selectează secțiunea **Applications**.
6. În lista de aplicații Kaspersky instalate pe computer, selectează **Kaspersky Endpoint Security for Windows (14.1)** și fă dublu clic pentru a deschide proprietățile aplicației.
7. În fereastra cu setările aplicației, selectați **Setări generale** → **Interfață**.
8. În blocul **Protecție prin parolă**, fă clic pe butonul **Setări**.
9. În fereastra care se deschide, în blocull **Parolă temporară**, fă clic pe butonul **Lista parolelor temporare**.

   Se deschide fereastra de gestionare a parolelor temporare.

10. Fă clic pe **Adaugă**.

11. În câmpul **Data expirării**, specifică data când va expira parola temporară.

12. În tabelul **Domeniu parolă temporară**, bifează casetele de selectare de lângă acțiunile care vor fi disponibile pentru utilizator după introducerea parolei temporare.

13. Fă clic pe **Generează**.

    Se va deschide o fereastră conținând parola temporară (vezi figura de mai jos).

14. Copiază parola și furnizeaz-o utilizatorului.

Cum permiți unui utilizator să efectueze o acțiune blocată utilizând o parolă temporară prin Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Assets (Devices)**.

2. Fă clic pe numele computerului pe care dorești să permiți unui utilizator să efectueze o acțiune blocată.

3. Selectați fila **Applications**.

4. Fă clic pe **Kaspersky Endpoint Security for Windows**.

   Se vor deschide setările locale pentru aplicație.

5. Selectați fila **Application settings**.

6. În fereastra cu setările aplicației, selectați **General settings** → **Interface**.

7. În blocul **Temporary passwords**, fă clic pe butonul **Add**.

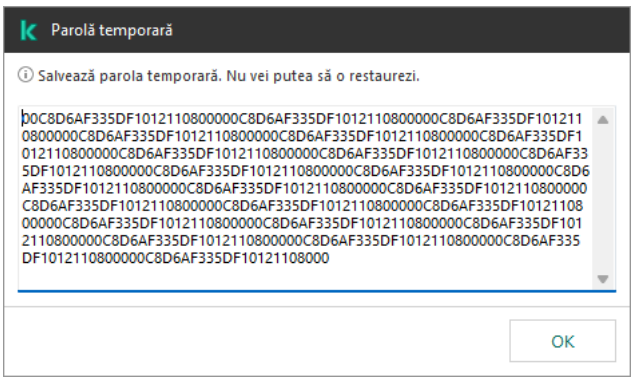
8. În câmpul **Data expirării**, specifică data când va expira parola temporară.

9. În tabelul **Domeniu parolă temporară**, bifează casetele de selectare de lângă acțiunile care vor fi disponibile pentru utilizator după introducerea parolei temporare.

10. Fă clic pe **Generează**.

    Se deschide o fereastră care conține parola temporară.

11. Copiază parola și furnizeaz-o utilizatorului.

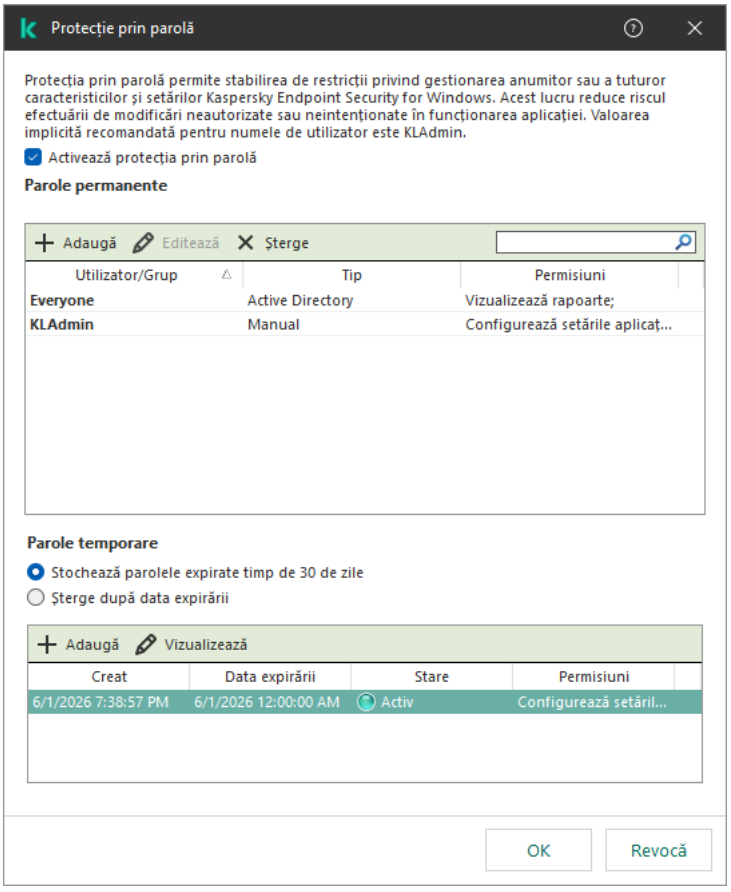


Parolă temporară

Revocarea parolei temporare

Începând cu versiunea 12.9, Kaspersky Endpoint Security for Windows include funcționalitatea *Gestionarea parolelor temporare*. Gestionarea parolelor temporare îți permite să efectuezi următoarele acțiuni:

- Să salvezi istoricul parolelor (până la 30 de zile).
- Să monitorizezi starea parolelor temporare: *Activ*, *Expirat*, *Anulează*.
- Să revoci parolele temporare.



Gestionarea parolelor temporare

Gestionarea parolelor temporare actualizează starea parolei și revocă parola numai după sincronizarea computerului cu Kaspersky Security Center.

Cum se revocă parola temporară utilizând Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Managed devices** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectează fila **Devices**.
4. Fă dublu clic pentru a deschide fereastra cu proprietățile computerului.
5. În fereastra cu proprietățile computerului, selectează secțiunea **Applications**.

6. În lista de aplicații Kaspersky instalate pe computer, selectează **Kaspersky Endpoint Security for Windows (14.1)** și fă dublu clic pentru a deschide proprietățile aplicației.

7. În fereastra cu setările aplicației, selectați **Setări generale** → **Interfață**.

8. În blocul **Protecție prin parolă**, fă clic pe butonul **Setări**.

9. Această acțiune deschide o fereastră; în această fereastră, sub **Parolă temporară**, configurează setările de stocare pentru parolele expirate.

10. Fă clic pe **Lista parolelor temporare**.

    Se deschide fereastra de gestionare a parolelor temporare. Gestionarea parolelor temporare afișează data de expirare a parolei, starea parolei și lista de permisiuni.

11. Selectează parola temporară activă pe care dorești să o revoci și fă dublu clic pe parolă pentru a deschide proprietățile acesteia.

12. În fereastra care se deschide, faceți clic pe butonul **Anulează**.

13. Salvați-vă modificările. Pentru a aplica politica pe computere, închide lacătele .

Cum se revocă parolele temporare în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Assets (Devices)**.

2. Fă clic pe numele computerului pe care dorești să permiți unui utilizator să efectueze o acțiune blocată.

3. Selectați fila **Applications**.

4. Fă clic pe **Kaspersky Endpoint Security for Windows**.

   Se vor deschide setările locale pentru aplicație.

5. Selectați fila **Application settings**.

6. În fereastra cu setările aplicației, selectați **General settings** → **Interface**.

7. În **Temporary passwords**, configurează spațiul de stocare a parolelor expirate.

8. Faceți clic pe linkul **Temporary password**.

   Se deschide fereastra de gestionare a parolelor temporare. Gestionarea parolelor temporare afișează data de expirare a parolei, starea parolei și lista de permisiuni.

9. Selectează parola temporară activă pe care dorești să o revoci.

10. În fereastra care se deschide, faceți clic pe butonul **Revoke password**.

11. Salvați-vă modificările. Pentru a aplica politica pe computere, închide lacătele .

Ca rezultat, Gestionarea parolelor temporare setează starea parolei la *Se revocă (se sincronizează cu o gazdă)*. După sincronizarea computerului cu Kaspersky Security Center, aplicația revocă parola temporară și blochează imediat permisiunile acordate.

Aspecte speciale ale permisiunilor Protecție prin parolă

Permisiunile Protecție prin parolă au câteva aspecte importante și limitări care trebuie luate în considerare.

Configurează setările aplicației

În cazul în care computerul unui utilizator funcționează în baza unei politici, asigură-te că toate setările necesare din cadrul politicii pot fi editate (atributele trebuie să fie deschise).

Părăsește aplicația

Nu există considerații sau limitări speciale.

Dezactivează componentele de protecție

- Nu este posibil să acordați permisiunea de a dezactiva componentele de protecție pentru grupul Toți. Pentru a permite altor utilizatori decât KLAdmin să dezactiveze componentele de control, adăugați un utilizator sau un grup care are permisiunea **Dezactivează componentele de protecție** în setările opțiunii Protecție prin parolă.
- În cazul în care computerul unui utilizator funcționează în baza unei politici, asigură-te că toate setările necesare din cadrul politicii pot fi editate (atributele trebuie să fie deschise).
- Pentru a dezactiva componentele de protecție în setările aplicației, un utilizator trebuie să aibă permisiunea **Configurează setările aplicației**.
- Pentru a dezactiva componentele de protecție din meniul contextual (utilizând elementul de meniu **Pauză protecție**), un utilizator trebuie să aibă și permisiunea **Dezactivează componentele de protecție** pe lângă cea de **Dezactivează componentele de control**.

Dezactivează componentele de control

- Nu este posibil să acordați permisiunea de a dezactiva componentele de control pentru grupul Toți. Pentru a permite altor utilizatori decât KLAdmin să dezactiveze componentele de control, adăugați un utilizator sau un grup care are permisiunea **Dezactivează componentele de control** în setările opțiunii Protecție prin parolă.
- În cazul în care computerul unui utilizator funcționează în baza unei politici, asigură-te că toate setările necesare din cadrul politicii pot fi editate (atributele trebuie să fie deschise).

- Pentru a dezactiva componentele de control în setările aplicației, un utilizator trebuie să aibă permisiunea **Configurează setările aplicației**.

- Pentru a dezactiva componentele de control din meniul contextual (utilizând elementul de meniu **Pauză protecție**), un utilizator trebuie să aibă și permisiunea **Dezactivează componentele de control** pe lângă cea de **Dezactivează componentele de protecție**.

Dezactivează politica Kaspersky Security Center

Nu puteți acorda grupului „Toți" permisiunea de a dezactiva politica Kaspersky Security Center. Pentru a permite altor utilizatori decât KLAdmin să dezactiveze politica, adăugați un utilizator sau un grup care are permisiunea de **Dezactivează politica Kaspersky Security Center** în setările opțiunii Protecție prin parolă.

Elimină cheia

Nu există considerații sau limitări speciale.

Elimină/modifică/restaurează aplicația

Dacă ați permis grupului „Toți" să șteargă, să modifice și să restabilească aplicația, Kaspersky Endpoint Security nu va solicita o parolă, atunci când utilizatorul va încerca să efectueze aceste acțiuni. Așadar, orice utilizator, inclusiv din afara domeniului, poate instala, modifica sau restabili aplicația.

Restaurează accesul la datele de pe unitățile criptate

Poți să restaurezi accesul la datele de pe unitățile criptate doar dacă ești conectat în calitate de KLAdmin. Permisiunea de a efectua această acțiune nu poate fi acordată niciunui alt utilizator.

Vizualizează rapoarte

Nu există considerații sau limitări speciale.

Restaurează din Copii de rezervă

Nu există considerații sau limitări speciale.

Exportă setările

În mod implicit, exportul setărilor aplicației este refuzat grupului „Toate”. Poți exporta setările aplicației utilizând contul de utilizator KLAdmin. Exportul setărilor aplicației include doar crearea unui fișier de configurare cu setările Kaspersky Endpoint Security în interfața aplicației. Permisiunea nu restricționează exportul listelor cu excluderi de la scanare, adrese web de încredere, dispozitive de încredere sau al altor liste gestionate de componentele aplicației.

Resetarea parolei KLAdmin

Dacă ai uitat parola contului KLAdmin, poți reseta parola în proprietățile politicii. Nu poți reseta parola în interfața aplicației.

Poți efectua acțiuni protejate prin parolă folosind a parolă temporară. În acest caz, nu este necesar să introduceți acreditările KLAdmin.

În cazul în care computerul nu este conectat la Kaspersky Security Center și ați uitat parola pentru contul KLAdmin, nu este posibilă recuperarea parolei.

Cum se resetează parola contului KLAdmin utilizând Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Setări generale** → **Interfață**.
4. În blocul **Protecție prin parolă**, fă clic pe butonul **Setări**.
5. În fereastra care se deschide, debifați caseta de selectare **Activează protecția prin parolă**.
6. Salvați-vă modificările.
7. Bifează din nou caseta de selectare **Activează protecția prin parolă**.
8. Fă clic pe **OK**.
   Aceasta deschide fereastra pentru parola administratorului.
9. Specifică noua parolă pentru contul KLAdmin și confirm-o.
10. Salvați-vă modificările.

Cum se resetează parola contului KLAdmin în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Assets (Devices)**.
2. Selectează computerul pentru care dorești să configurezi setări locale pentru aplicație.
   Se vor deschide proprietățile computerului.
3. Selectați fila **Applications**.

4. Fă clic pe **Kaspersky Endpoint Security for Windows**.

   Se vor deschide setările locale pentru aplicație.

5. Selectați fila **Application settings**.

6. Accesați **General Settings** → **Self-Defense**.

7. În **Protecție prin parolă**, dezactivează comutatorul **Protecție prin parolă**.

8. Salvați-vă modificările.

9. Reactivează comutatorul **Protecție prin parolă**.

10. Specifică noua parolă pentru contul KLAdmin și confirm-o.

11. Salvați-vă modificările.

Ca rezultat, parola contului tău KLAdmin este actualizată după aplicarea politicii.

Protecție conexiune la Serverul de administrare

Conectarea computerului la Serverul de administrare se realizează cu ajutorul componentei *Network Agent* a Kaspersky Security Center. În cazul în care un intrus are drepturi suficiente pentru a modifica setările de conectare la server, există riscul de a conecta calculatorul la un server care nu este de încredere. Acest lucru ar permite intrusului să își aplice propriile politici de grup și, de exemplu, să dezactiveze autoprotecția aplicației. Kaspersky Endpoint Security poate preveni reconectarea neautorizată a unui computer la un alt server. Pentru a proteja conexiunea la server, aplicația sugerează setarea unei parole și folosirea Password-Based key Derivation Function (PBKDF2). Prin urmare, accesul la aplicație fără o parolă este imposibil.

Pentru a asigura o protecție completă pentru Kaspersky Endpoint Security și Agentul de rețea împotriva accesului neautorizat, îți recomandăm să activezi o protecție suplimentară. Pentru Kaspersky Endpoint Security, îți recomandăm să activezi Protecție prin parolă. Pentru a proteja Agentul de rețea, îți recomandăm să setezi o parolă pentru dezinstalare. Pentru detalii despre protejarea Agentului de rețea împotriva eliminării, consultă pagina Ajutor pentru Kaspersky Security Center.

Gestionarea conectării computerului la Serverul de administrare se realizează cu ajutorul activității *Protecție conexiune Server de administrare*. Aplicația îți permite să efectuezi următoarele acțiuni:

- setarea unei parole pentru protejarea conexiunii la server;
- modificarea parolei;
- reconectarea computerului la un alt server;
- dezactivarea protecției conexiunii la server.

Autentificarea computerului la conectarea la Serverul de administrare

După setarea unei parole, aplicația creează o matrice de date utilizând transformarea PBKDF2 a parolei. Aplicația criptează apoi această matrice de date cu ajutorul cheii Agent de rețea. Aplicația utilizează matricea de date criptate pentru a verifica drepturile și privilegiile Serverului de administrare pentru conexiunile ulterioare.

Ulterior, de fiecare dată când se încearcă reconectarea computerului la Serverul de administrare, aplicația decriptează matricea de date cu cheia Agent de rețea și o compară cu copia locală. În cazul în care nu se potrivesc, accesul la aplicație este restricționat.

Protecție conexiune la Serverul de administrare

Cum se setează o parolă pentru protecția conexiunii la server în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **New task**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Selectarea tipului activității

Selectați **Kaspersky Endpoint Security for Windows (14.1)** → **Protecție conexiune Server de administrare**.

Pasul 2. Protejarea conexiunii la Serverul de administrare

Setarea unei parole pentru protejarea conexiunii la Serverul de administrare:

1. În **Protecție conexiune Server de administrare**, selectează **Protejează cu o parolă**.
2. În lista verticală **Serverul de administrare**, selectează **Server nou**.
3. În câmpul **Parola pentru conectarea la Serverul de administrare**, setează o parolă pentru conectarea la Serverul de administrare și confirm-o.

   Dacă uiți parola, o poți schimba cu ajutorul unei activități.

4. Dacă ai instalat Kaspersky Endpoint Security 12.7 sau o versiune anterioară a aplicației, bifează caseta de selectare **Activează compatibilitatea cu criptarea parolei pentru versiunile anterioare ale aplicației (12.7 și versiunile anterioare)**.

   Începând cu Kaspersky Endpoint Security 12.8 for Windows, aplicația folosește o criptare mai puternică a parolelor. Dacă ai instalat Kaspersky Endpoint Security 12.8 sau o versiune ulterioară, îți recomandăm să debifezi această casetă de selectare și să utilizați criptarea mai puternică a parolei. Versiunile anterioare ale aplicației nu acceptă criptarea puternică a parolei. Pentru a executa activitatea, trebuie să bifezi caseta de selectare.

Pasul 3. Selectarea contului pentru executarea activității

Selectați **Default account**. În mod implicit, Kaspersky Endpoint Security pornește activitatea drept cont de utilizator de sistem (SYSTEM).

Pasul 4. Configurarea unei planificări de pornire a activității

În **Scheduled start**, selectează **Manually**.

Pasul 5. Definirea numelui activității

Introdu un nume pentru activitate, de exemplu, *Parola de conectare la serverul principal*.

Pasul 6. Finalizarea creării activității

Ieșiți din Expert. Bifează caseta de selectare **Run the task after the wizard finishes** sau execută activitatea manual. Puteți monitoriza progresul activității în proprietățile activității.

Cum se setează o parolă pentru protecția conexiunii la server în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **Add**.

   Expertul de activitate pornește.

3. Configurați setările pentru activitate:

   a. În lista verticală **Application**, selectează **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. În lista verticală **Task type**, selectează **Administration Server connection protection**.

   c. În câmpul **Task name**, introdu o descriere succintă, de exemplu *Parola pentru conectarea la serverul principal*.

   d. În blocul **Devices to which the task will be assigned**, selectați domeniul activității.

4. Selectați dispozitive în funcție de opțiunea selectată pentru domeniul activității. Mergeți la pasul următor.

5. Selectează un cont de utilizator implicit. În mod implicit, Kaspersky Endpoint Security pornește activitatea drept cont de utilizator de sistem (SYSTEM).

6. Ieșiți din Expert.

   Se va afișa o activitate nouă în lista de activități.

7. Faceți clic pe activitatea **Administration Server connection protection** a Kaspersky Endpoint Security.

   Se va deschide fereastra de proprietăți a activității.

8. Selectați fila **Application settings**.

9. În **Administration Server connection protection**, selectează **Protect with a password**.

10. În lista verticală **Connection to the Administration Server**, selectează **New password**.

11. În câmpul **Password**, setează o parolă pentru conectarea la Serverul de administrare și confirm-o.

    Dacă uiți parola, o poți schimba cu ajutorul unei activități.

12. Dacă ai instalat Kaspersky Endpoint Security 12.7 sau o versiune anterioară a aplicației, bifează caseta de selectare **Enable password encryption compatibility for previous application versions (12.7 and lower)**.

    Începând cu Kaspersky Endpoint Security 12.8 for Windows, aplicația folosește o criptare mai puternică a parolelor. Dacă ai instalat Kaspersky Endpoint Security 12.8 sau o versiune ulterioară, îți recomandăm să debifezi această casetă de selectare și să utilizați criptarea mai puternică a parolei. Versiunile anterioare ale aplicației nu acceptă criptarea puternică a parolei. Pentru a executa activitatea, trebuie să bifezi caseta de selectare.

13. Salvați-vă modificările.

14. Bifați caseta de selectare de lângă activitate.

15. Fă clic pe **Start**.

Poți monitoriza starea activității și numărul de dispozitive pe care activitatea a fost finalizată cu succes sau finalizată cu o eroare.

Reconectarea computerului la un alt Server de administrare

Reconectarea computerului la un alt Server de administrare implică următorii pași:

1. În consola serverului curent `[KSC1]`, execută activitatea *Change Administration Server* pentru Agentul de rețea.

   După executarea activității, computerul este reconectat la noul server `[KSC2]`.

   Computerul va fi afișat în consola serverului `[KSC1]` cu starea *Critical*. Configurarea aplicației cu ajutorul politicilor sau executarea de la distanță a activităților pe computer este imposibilă.

2. În consola noului server `[KSC2]`, creează o nouă activitate *Protecție conexiune Server de administrare* pentru Kaspersky Endpoint Security. În proprietățile activității, introdu parola serverului anterior și setează o parolă pentru noul server.

   Cum se setează o nouă parolă pentru reconectarea la un nou server în Consola de administrare (MMC)

   1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Tasks**.

      Lista activităților se deschide.

   2. Fă clic pe **New task**.

   Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Selectarea tipului activității

Selectați **Kaspersky Endpoint Security for Windows (14.1)** → **Protecție conexiune Server de administrare**.

Pasul 2. Protejarea conexiunii la Serverul de administrare

Setează o parolă pentru a proteja conexiunea la noul Server de administrare:

1. În **Protecție conexiune Server de administrare**, selectează **Protejează cu o parolă**.
2. În lista verticală **Serverul de administrare**, selectează **Reconectează de la un alt server**.
3. În câmpul **Parolă actuală**, introdu parola setată pentru conectarea la serverul de încredere utilizat anterior.
4. În câmpul **Parola nouă**, setează o parolă pentru conectarea la Serverul de administrare și confirmă parola.

   Dacă uiți parola, o poți schimba cu ajutorul unei activități.
5. Dacă ai instalat Kaspersky Endpoint Security 12.7 sau o versiune anterioară a aplicației, bifează caseta de selectare **Activează compatibilitatea cu criptarea parolei pentru versiunile anterioare ale aplicației (12.7 și versiunile anterioare)**.

   Începând cu Kaspersky Endpoint Security 12.8 for Windows, aplicația folosește o criptare mai puternică a parolelor. Dacă ai instalat Kaspersky Endpoint Security 12.8 sau o versiune ulterioară, îți recomandăm să debifezi această casetă de selectare și să utilizați criptarea mai puternică a parolei. Versiunile anterioare ale aplicației nu acceptă criptarea puternică a parolei. Pentru a executa activitatea, trebuie să bifezi caseta de selectare.

Pasul 3. Selectarea contului pentru executarea activității

Selectați **Default account**. În mod implicit, Kaspersky Endpoint Security pornește activitatea drept cont de utilizator de sistem (SYSTEM).

Pasul 4. Configurarea unei planificări de pornire a activității

În **Scheduled start**, selectează **Manually**.

Pasul 5. Definirea numelui activității

Introdu un nume pentru activitate, de exemplu, *Parola de conectare la serverul principal*.

Pasul 6. Finalizarea creării activității

Ieșiți din Expert. Bifează caseta de selectare **Run the task after the wizard finishes** sau execută activitatea manual. Puteți monitoriza progresul activității în proprietățile activității.

Cum se setează o nouă parolă pentru reconectarea la un nou server în Web Console și Cloud Console.

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **Add**.

   Expertul de activitate pornește.

3. Configurați setările pentru activitate:

   a. În lista verticală **Application**, selectează **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. În lista verticală **Task type**, selectează **Administration Server connection protection**.

   c. În câmpul **Task name**, introdu o descriere succintă, de exemplu *Parola pentru conectarea la serverul principal*.

   d. În blocul **Devices to which the task will be assigned**, selectați domeniul activității.

4. Selectați dispozitive în funcție de opțiunea selectată pentru domeniul activității. Mergeți la pasul următor.

5. Selectează un cont de utilizator implicit. În mod implicit, Kaspersky Endpoint Security pornește activitatea drept cont de utilizator de sistem (SYSTEM).

6. Ieșiți din Expert.

   Se va afișa o activitate nouă în lista de activități.

7. Faceți clic pe activitatea **Administration Server connection protection** a Kaspersky Endpoint Security.

   Se va deschide fereastra de proprietăți a activității.

8. Selectați fila **Application settings**.

9. În **Administration Server connection protection**, selectează **Protect with a password**.

10. În lista verticală **Connection to the Administration Server**, selectează **Reconnect from another server**.

11. În câmpul **Current password**, introdu parola setată pentru conectarea la serverul de încredere utilizat anterior.

12. În câmpul **New password**, setează o parolă pentru conectarea la Serverul de administrare și confirmă parola.

    Dacă uiți parola, o poți schimba cu ajutorul unei activități.

13. Dacă ai instalat Kaspersky Endpoint Security 12.7 sau o versiune anterioară a aplicației, bifează caseta de selectare **Activează compatibilitatea cu criptarea parolei pentru versiunile anterioare ale aplicației (12.7 și versiunile anterioare)**.

    Începând cu Kaspersky Endpoint Security 12.8 for Windows, aplicația folosește o criptare mai puternică a parolelor. Dacă ai instalat Kaspersky Endpoint Security 12.8 sau o versiune ulterioară, îți recomandăm să debifezi această casetă de selectare și să utilizați criptarea mai puternică a parolei. Versiunile anterioare ale aplicației nu acceptă criptarea puternică a parolei. Pentru a executa activitatea, trebuie să bifezi caseta de selectare.

14. Salvați-vă modificările.

15. Bifați caseta de selectare de lângă activitate.

16. Fă clic pe **Start**.

    Poți monitoriza starea activității și numărul de dispozitive pe care activitatea a fost finalizată cu succes sau finalizată cu o eroare.

După ce ai finalizat activitatea, asigură-te că în consola noului server `[KSC2]`, computerul are starea *OK*. Testează dacă poți executa activități de la distanță și configura aplicația cu ajutorul politicilor.

Resetarea parolei de conectare la Serverul de administrare

Dacă ai uitat parola de conectare la Serverul de administrare sau dacă parola este compromisă, poți reseta parola în proprietățile activității. De asemenea, poți reseta parola și seta o nouă parolă pentru un grup de calculatoare cu diferite stări de protecție a conexiunii la Serverul de administrare. Adică, dacă unele computere au protecția activată, iar altele o au dezactivată, activitatea setează o parolă pentru toate computerele.

Poți reseta parola de conectare la Serverul de administrare numai în consola serverului de încredere la care este conectat computerul.

Cum se resetează parola de conectare la Serverul de administrare cu ajutorul Consolei de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.

2. În arborele consolei, selectați **Tasks**.

3. Selectează activitatea **Protecție conexiune Server de administrare** și fă dublu clic pentru a deschide proprietățile activității.

4. În fereastra cu proprietățile activității, selectați secțiunea **Setări**.

5. În **Protecție conexiune Server de administrare**, selectează **Protejează și schimbă parola**.

6. În câmpul **Parola pentru conectarea la Serverul de administrare**, setează o parolă pentru conectarea la serverul de încredere curent și confirmă parola.

7. Salvați-vă modificările.

8. Execută activitatea.

Cum se resetează parola de conectare la Serverul de administrare în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe activitatea **Administration Server connection protection** a Kaspersky Endpoint Security.

   Se va deschide fereastra de proprietăți a activității.

3. Selectați fila **Application settings**.

4. În **Administration Server connection protection**, selectează **Protect and change password**.

5. În câmpul **Password**, setează o parolă pentru conectarea la serverul de încredere curent și confirmă parola.

6. Salvați-vă modificările.

7. Bifați caseta de selectare de lângă activitate.

8. Fă clic pe **Start**.

Ca urmare, parola de conectare la Serverul de administrare este resetată după finalizarea activității.

Dezactivarea protecției conexiunii la Serverul de administrare

Poți dezactiva de la distanță protecția conexiunii la Serverul de administrare numai în consola serverului de încredere la care este conectat computerul. De asemenea, poți dezactiva protecția local, în linia de comandă.

Cum se dezactivează protecția conexiunii la server în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.

2. În arborele consolei, selectați **Tasks**.

3. Selectează activitatea **Protecție conexiune Server de administrare** și fă dublu clic pentru a deschide proprietățile activității.

4. În fereastra cu proprietățile activității, selectați secțiunea **Setări**.

5. În **Protecție conexiune Server de administrare**, selectează **Nu proteja**.

6. Salvați-vă modificările.

7. Execută activitatea.

   Poți monitoriza starea activității și numărul de dispozitive pe care activitatea a fost finalizată cu succes sau finalizată cu o eroare.

Cum se dezactivează protecția conexiunii la server în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe activitatea **Administration Server connection protection** a Kaspersky Endpoint Security.

   Se va deschide fereastra de proprietăți a activității.

3. Selectați fila **Application settings**.

4. În **Administration Server connection protection**, selectează **Do not protect**.

5. Salvați-vă modificările.

6. Bifați caseta de selectare de lângă activitate.

7. Fă clic pe **Start**.

   Poți monitoriza starea activității și numărul de dispozitive pe care activitatea a fost finalizată cu succes sau finalizată cu o eroare.

Cum se dezactivează protecția conexiunii la server în linia de comandă

1. Executați interpretorul de linii de comandă (cmd.exe) ca administrator.

2. Deschideți directorul în care se află fișierul executabil Kaspersky Endpoint Security.

3. Execută următoare comandă:

   ```
   avp.com SERVERBINDINGDISABLE [/password=<password>]
   ```

   unde `<password>` este parola contului de utilizator KL Admin sau parola din activitatea *Protecție conexiune Server de administrare*. Dacă parametrul nu este specificat, Kaspersky Endpoint Security îți solicită să introduci o parolă pe linia următoare.

   > Pentru a executa această comandă, funcția Protecție prin parolă trebuie activată.

Exemplu

```
avp.com SERVERBINDINGDISABLE /password=samplePassword
```

Data Encryption

Kaspersky Endpoint Security îți permite să criptezi fișiere și directoare stocate pe unitățile locale și amovibile sau să criptezi întregi unități amovibile și unități de hard disk. Criptarea datelor reduce riscul pierderilor de informații atunci când un computer portabil, o unitate portabilă sau o unitate de hard disk este pierdută sau furată sau atunci când datele sunt accesate de către utilizatori sau aplicații neautorizate. Kaspersky Endpoint Security utilizează algoritmul de criptare Advanced Encryption Standard (AES).

Dacă licența a expirat, aplicația nu criptează date noi, iar datele vechi criptate rămân criptate și sunt disponibile pentru utilizare. În acest caz, criptarea datelor noi necesită activarea aplicației cu o licență nouă care permite utilizarea criptării.

Dacă Kaspersky Endpoint Security este instalat pe un computer bazat pe arhitectura Arm, este disponibil doar BitLocker Drive Encryption. Aplicația nu acceptă alte componente de criptare a datelor.

Dacă licența a expirat sau Acordul de licență pentru utilizatorul final a fost încălcat, cheia de licență, Kaspersky Endpoint Security sau componentele de criptare au fost eliminate, starea de criptare a fișierelor criptate anterior nu este garantată. Acest lucru se datorează faptului că unele aplicații, cum ar fi Microsoft Office Word, creează o copie temporară a fișierelor în cursul editării. Atunci când fișierul original este salvat, copia temporară înlocuiește fișierul original. Prin urmare, pe un computer care nu are funcționalitate de criptare sau aceasta este inaccesibilă, fișierul rămâne necriptat.

Kaspersky Endpoint Security oferă următoarele aspecte pentru protecția datelor:

- **File Level Encryption pe unitățile locale ale computerului**. Poți compila liste de fișiere după extensie sau după grupuri de extensii și liste de directoare stocate pe unitățile locale ale computerului și poți crea reguli pentru criptarea fișierelor care sunt create de aplicații specifice. După aplicarea unei politici, Kaspersky Endpoint Security criptează și decriptează următoarele fișiere:
  - fișiere adăugate separat la liste pentru criptare și decriptare;
  - fișiere stocate în directoare adăugate la liste pentru criptare și decriptare;
  - Fișiere create de aplicații separate.
- **Encryption of removable drives**. Poți specifica o regulă de criptare implicită, conform căreia aplicația execută aceeași acțiune asupra tuturor unităților amovibile sau poți specifica reguli de criptare pentru unități amovibile individuale.

  Regula de criptare implicită are o prioritate mai mică decât regulile de criptare create pentru unități amovibile individuale. Regulile de criptare create pentru unități amovibile cu modelul de dispozitiv specificat au o prioritate mai mică decât regulile de criptare create pentru unități amovibile cu ID-ul de dispozitiv specificat.

  Pentru a selecta o regulă de criptare pentru fișiere de pe o unitate amovibilă, Kaspersky Endpoint Security verifică dacă modelul și ID-ul dispozitivului sunt cunoscute sau nu. Aplicația efectuează apoi una dintre următoarele operațiuni:
  - Dacă modelul de dispozitiv este cunoscut, aplicația folosește regula de criptare (dacă există) creată pentru unități amovibile cu modelul de dispozitiv specific.
  - Dacă ID-ul de dispozitiv este cunoscut, aplicația folosește regula de criptare (dacă există) creată pentru unități amovibile cu ID-ul de dispozitiv specific.

- Dacă modelul și ID-ul de dispozitiv sunt cunoscute, aplicația folosește regula de criptare (dacă există) creată pentru unități amovibile cu ID-ul de dispozitiv specific. Dacă nu există o astfel de regulă, dar există o regulă de criptare pentru unități amovibile cu modelul de dispozitiv specific, aplicația folosește această regulă. Dacă nu este specificată nicio regulă de criptare pentru ID-ul de dispozitiv specific și nici pentru modelul de dispozitiv specific, aplicația folosește recula de criptare implicită.

- Dacă nici modelul, nici ID-ul de dispozitiv nu sunt cunoscute, aplicația folosește regula de criptare implicită.

Aplicația îți permite să pregătești o unitate amovibilă pentru a folosi date criptate stocate pe ea în modul portabil. După activarea modului portabil, poți accesa fișiere criptate de pe unități amovibile conectate la un computer fără funcționalitate de criptare.

- **Administrarea regulilor de acces al aplicațiilor la fișiere criptate**. Pentru orice aplicație poți crea o regulă de acces la fișiere criptate care blochează accesul la fișierele criptate sau care permite accesul la fișierele criptate doar ca text cifrat, o secvență de caractere obținute la aplicarea criptării.

- **Crearea pachetelor criptate**. Poți crea arhive cifrate și poți proteja accesul la aceste arhive prin parolă. Conținutul arhivelor criptate poate fi accesat doar dacă sunt introduse parolele prin care protejezi accesul la arhivele respective. Aceste arhive pot fi transmise în mod sigur prin rețele sau pe unități amovibile.

- **Full Disk Encryption**. Puteți selecta o tehnologie de criptare: Kaspersky Disk Encryption sau BitLocker Drive Encryption (denumită în continuare pur și simplu „BitLocker”).

  BitLocker este o tehnologie care face parte din sistemul de operare Windows. Dacă un computer este echipat cu un Trusted Platform Module (TPM), BitLocker îl folosește pentru a stoca cheile de recuperare care asigură accesul la o unitate de hard disk criptată. Atunci când computerul pornește, BitLocker solicită cheile de recuperare pentru unitatea de hard disk de la Trusted Platform Module și deblochează unitatea. Poți configura utilizarea unei parole și/sau a unui cod PIN pentru accesarea cheilor de recuperare.

  Poți specifica regula de criptare implicită pentru întreaga unitate de hard disk și poți crea o listă de unități de hard disk care să fie excluse de la criptare. Kaspersky Endpoint Security efectuează criptarea Full Disk Encryption sector cu sector după ce este aplicată politica aplicației Kaspersky Security Center. Aplicația criptează toate partițiile logice ale unităților de hard disk simultan.

  După ce unitățile de hard disk de sistem au fost criptate, la următoarea pornire a computerului utilizatorul trebuie să finalizeze autentificarea folosind Agentul de Autentificare pentru ca unitățile de hard disk să poată fi accesate și sistemul de operare să fie încărcat. Acest lucru necesită introducerea parolei pentru simbolul sau cardul inteligent conectat la computer sau a numelui de utilizator și a parolei pentru contul de Agent de Autentificare creat de administratorul rețelei locale folosind activitatea *Gestionare conturi Agent de Autentificare*. Aceste conturi se bazează pe conturile Microsoft Windows sub care utilizatorii se conectează la sistemul de operare. Poți utiliza, de asemenea, tehnologia Single Sign-On (SSO), care îți permite să te conectezi automat la sistemul de operare folosind numele de utilizator și parola contului Agent de Autentificare.

  > Dacă faci o copie de rezervă unui computer și apoi criptezi datele computerului, după care restaurezi copia de rezervă a computerului și criptezi datele computerului din nou, Kaspersky Endpoint Security creează dubluri ale conturilor Agent de Autentificare. Pentru a elimina conturile dublate, trebuie să folosești utilitarul klmover cu cheia `dupfix`. Utilitarul klmover este inclus în pachetul Kaspersky Security Center. Poți citi mai multe despre funcționarea sa în secțiunea de ajutor din Kaspersky Security Center.

  Accesul la unitățile de hard disk criptate va fi posibil numai de pe computerele pe care este instalat Kaspersky Endpoint Security cu funcționalitate full disk encryption. Această precauție reduce riscul pierderilor de date de pe o unitate de hard disk criptată atunci când se încearcă accesarea acesteia în afara rețelei locale a companiei.

Pentru a cripta unitățile de hard disk și unitățile amovibile, poți folosi funcția Criptează doar spațiul de disc utilizat. Se recomandă folosirea acestei funcții numai pentru dispozitive noi care nu au fost utilizate anterior. Dacă aplici criptarea unui dispozitiv aflat deja în uz, este recomandat să criptezi întregul dispozitiv. Astfel se asigură protecția tuturor datelor – chiar și a datelor șterse care pot conține informații ce pot fi recuperate.

Înainte de a începe criptarea, Kaspersky Endpoint Security obține o hartă cu sectoarele sistemului de fișiere. Primul val de criptare include sectoare care sunt ocupate de fișiere în momentul în care începe criptarea. Al doilea val de criptare include sectoare care au fost scrise după ce a început criptarea. După finalizarea criptării, toate sectoarele care conțin date sunt criptate.

După finalizarea criptării, dacă un utilizator șterge un fișier, sectoarele care au stocat fișierul devin disponibile pentru stocarea unor informații noi, la nivelul sistemului de fișiere, dar ele rămân în continuare criptate. Astfel, atunci când fișierele se scriu pe un dispozitiv nou și dispozitivul este criptat periodic cu funcția **Criptează doar spațiul de disc utilizat** activată, toate sectoarele vor fi criptate după un timp.

Datele necesare pentru decriptarea fișierelor The data sunt furnizate de serverul de administrare Kaspersky Security Center care controla computerul la momentul criptării. În cazul în care computerul cu obiecte criptate a fost gestionat de un alt server de administrare din anumite motive, puteți obține acces la datele criptate într-unul din următoarele moduri:

- Servere de administrare în aceeași ierarhie:
    - Nu trebuie să întreprindeți nicio acțiune suplimentară. Utilizatorul va păstra accesul la obiectele criptate. Cheile de criptare sunt distribuite tuturor serverelor de administrare.
- Servere de administrare separate:
    - solicitați acces la obiectele criptate de la administratorul rețelei LAN.
    - Restaurează date pe dispozitivele criptate folosind Utilitarul de restaurare.
    - Restaurează configurația serverului de administrare a Kaspersky Security Center care a controlat computerul la momentul criptării dintr-o copie de rezervă și utilizează această configurație pe serverul de administrare care controlează acum computerul cu obiectele criptate.

Dacă nu există acces la datele criptate, urmați instrucțiunile speciale pentru lucrul cu datele criptate (Restaurarea accesului la fișierele criptate, Lucrul cu dispozitive criptate atunci când nu există acces la ele).

Limitările funcționalității de criptare

Funcționalitatea Data Encryption are următoarele limitări:

- Aplicația creează fișiere de depanare în cursul criptării. Aproximativ 0.5% din spațiul liber nefragmentat de pe unitatea de hard disk este necesar pentru stocarea acestora. Dacă nu există suficient spațiu liber nefragmentat pe unitatea de hard disk, criptarea nu va începe până când nu eliberezi suficient spațiu.
- Puteți gestiona toate componentele de criptare a datelor în Kaspersky Security Center Administration Console și în Kaspersky Security Center Web Console. În Kaspersky Security Center Cloud Console puteți gestiona doar Bitlocker.
- Componenta Data Encryption este disponibilă numai atunci când se utilizează Kaspersky Endpoint Security cu sistemul de administrare Kaspersky Security Center sau Kaspersky Security Center Cloud Console (doar BitLocker). Utilizarea funcționalității Data Encryption când se utilizează Kaspersky Endpoint Security în modul offline nu este posibilă, deoarece Kaspersky Endpoint Security stochează cheile de criptare în Kaspersky Security Center.

- În cazul în care Kaspersky Endpoint Security este instalat pe un computer pe care se execută Microsoft Windows pentru servere, este disponibilă numai criptarea completă a unității de hard disk utilizându-se tehnologia BitLocker Drive Encryption. În cazul în care Kaspersky Endpoint Security este instalat pe un computer pe care se execută Windows pentru stații de lucru, criptarea completă a datelor este disponibilă integral.

- Dacă Kaspersky Endpoint Security este instalat pe un computer bazat pe arhitectura ARM, este disponibilă doar componenta Full Disk Encryption folosind tehnologia BitLocker Drive Encryption; celelalte componente de criptare nu sunt acceptate.

Criptarea completă a unității de hard disk folosind tehnologia Kaspersky Disk Encryption nu este disponibilă pentru unitățile de hard disk care nu îndeplinesc cerințele hardware și software.

Compatibilitatea dintre funcționalitatea de criptare a întregului disc din Kaspersky Endpoint Security și Kaspersky Anti-Virus for UEFI nu beneficiază de suport. Kaspersky Anti-Virus for UEFI pornește înainte de încărcarea sistemului de operare. Atunci când se utilizează criptarea întregului disc, aplicația va detecta absența unui sistem de operare instalat pe computer. În consecință, funcționarea Kaspersky Anti-Virus for UEFI se va termina cu o eroare. File Level Encryption (FLE) nu afectează funcționarea Kaspersky Anti-Virus pentru UEFI.

Kaspersky Endpoint Security acceptă următoarele configurări:

- unități HDD, SSD și USB.

  Tehnologia Kaspersky Disk Encryption (FDE) acceptă lucrul cu SSD, păstrând în același timp performanța și durata de viață a unităților SSD.

- Unități conectate prin magistrală: SCSI, ATA, IEEE1934, USB, RAID, SAS, SATA, NVME.

- Unități fixe conectate prin magistrala SD sau MMC.

- Unități cu sectoare de 512 octeți.

- Unități cu sectoare de 4096 octeți care emulează 512 octeți.

- Unități cu următorul tip de partiții: GPT, MBR și VBR (unități amovibile).

- Software încorporat al standardului UEFI 64 și Legacy BIOS.

- Software încorporat al standardului UEFI cu compatibilitate Secure Boot.

  Secure Boot este o tehnologie concepută pentru a verifica semnăturile digitale pentru aplicațiile de încărcare și driverele UEFI. Secure Boot blochează pornirea aplicațiilor și a driverelor UEFI care nu sunt semnate sau sunt semnate de editori necunoscuți. Kaspersky Disk Encryption (FDE) este complet compatibil cu Secure Boot. Agentul de autentificare este semnat de un certificat Microsoft Windows UEFI Driver Publisher.

  Pe unele dispozitive (de exemplu, Microsoft Surface Pro și Microsoft Surface Pro 2), o listă învechită a certificatelor de verificare a semnăturii digitale poate fi instalată în mod implicit. Înainte de a cripta unitatea, trebuie să actualizați lista certificatelor.

- Software încorporat al standardului UEFI cu compatibilitate Fast Boot.

  Fast Boot este o tehnologie care ajută computerul să pornească mai repede. Când tehnologia Fast Boot este activată, în mod normal computerul încarcă doar setul minim de drivere UEFI necesare pentru pornirea sistemului de operare. Când tehnologia Fast Boot este activată, tastaturile USB, mouse-urile, tokenurile USB, touchpadurile și ecranele tactile pot să nu funcționeze în timp ce se execută Agentul de Autentificare.

Pentru a utiliza Kaspersky Disk Encryption (FDE), se recomandă dezactivarea tehnologiei Fast Boot. Puteți utiliza utilitarul de testare FDE pentru a testa funcționarea Kaspersky Disk Encryption (FDE).

Kaspersky Endpoint Security nu acceptă următoarele configurații:

- Programul de încărcare pentru boot este amplasat pe o unitate, iar sistemul de operare pe o altă unitate.
- Sistemul conține software încorporat cu standardul UEFI 32.
- Sistemul are Intel® Rapid Start Technology și unități care au o partiție dedicată pentru hibernare, chiar dacă tehnologia Intel® Rapid Start Technology este dezactivată.
- Unități în format MBR cu mai mult de 10 partiții extinse.
- Sistemul are un fișier swap localizat pe o unitate non-sistem.
- Sistem multiboot cu mai multe sisteme de operare instalate simultan.
- Partiții dinamice (sunt acceptat doar partiții primare).
- Unități cu mai puțin de 0.5% spațiu liber nefragmentat pe unitatea de disc.
- Unități cu o dimensiune a sectorului alta decât 512 octeți sau 4096 de octeți care emulează 512 octeți.
- Unități hibride.
- Sistemul are încărcătoare terțe.
- Unități cu directoare NTFS comprimate.
- Tehnologia Kaspersky Disk Encryption (FDE) este incompatibilă cu alte tehnologii complete de criptare a discului (cum ar fi BitLocker, McAfee Drive Encryption și WinMagic SecureDoc).
- Tehnologia Kaspersky Disk Encryption (FDE) este incompatibilă cu tehnologia ExpressCache.
- Crearea, ștergerea și modificarea partițiilor pe o unitate criptată nu este acceptată. Ați putea pierde date.
- Formatarea sistemului de fișiere nu este acceptată. Ați putea pierde date.

  Dacă trebuie să formatați o unitate care a fost criptată cu tehnologia Kaspersky Disk Encryption (FDE), formatați unitatea pe un computer care nu are Kaspersky Endpoint Security for Windows și utilizați doar criptarea completă a discului.

  O unitate criptată formatată cu opțiunea de formatare rapidă poate fi identificată greșit ca fiind criptată data viitoare când este conectată la un computer care are instalat Kaspersky Endpoint Security for Windows. Datele utilizatorului nu vor fi disponibile.
- Agentul de Autentificare nu acceptă mai mult de 100 de conturi.
- Tehnologia Single Sign-On este incompatibilă cu alte tehnologii ale dezvoltatorilor terți.

- Tehnologia Kaspersky Disk Encryption (FDE) nu este acceptată pe următoarele modele de dispozitive:
  - Dell Latitude E6410 (modul UEFI)
  - HP Compaq nc8430 (modul Legacy BIOS)
  - Lenovo ThinkCentre 8811 (modul Legacy BIOS)
- Agentul de Autentificare nu acceptă lucrul cu tokenuri USB atunci când Legacy USB Support este activat. Pe computer va fi posibilă doar autentificarea bazată pe parolă.
- Când criptați o unitate în modul Legacy BIOS, vi se recomandă să activați Legacy USB Support pe următoarele modele de dispozitive:
  - 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 (placă de bază)

Modificarea lungimii cheii de criptare (AES56/AES256)

Kaspersky Endpoint Security utilizează algoritmul de criptare Advanced Encryption Standard (AES). Kaspersky Endpoint Security acceptă algoritmul de criptare AES cu o lungime efectivă a cheii de 256 sau 56 de biți. Algoritmul de criptare a datelor depinde de biblioteca de criptare AES care este inclusă în pachetul de distribuție: *Strong encryption (AES256)* sau *Lite encryption (AES56)*. Biblioteca de criptare AES este instalată împreună cu aplicația.

Modificarea lungimii cheii de criptare este disponibilă numai pentru Kaspersky Endpoint Security 11.2.0 sau o versiune ulterioară.

Modificarea lungimii cheii de criptare constă în următorii pași:

1. Decriptați obiectele pe care Kaspersky Endpoint Security le-a criptat înainte de a începe schimbarea algoritmului de criptare.
   a. Decriptează unitățile de hard disk.
   b. Decriptați fișierele de pe unitățile locale.
   c. Decriptați unitățile amovibile.

   După modificarea lungimii cheii de criptare, obiectele criptate anterior devin indisponibile.
2. Eliminați aplicația Kaspersky Endpoint Security.
3. Instalați Kaspersky Endpoint Security din pachetul de distribuție Kaspersky Endpoint Security care conține o bibliotecă de criptare diferită.

De asemenea, puteți modifica lungimea cheii de criptare făcând upgrade aplicației. Lungimea cheii poate fi modificată printr-un upgrade al aplicației numai dacă sunt îndeplinite următoarele condiții:

- Kaspersky Endpoint Security versiunea 10 Service Pack 2 sau o versiune ulterioară este instalat pe computer.
- Componentele de criptare a datelor (File Level Encryption, Full Disk Encryption) nu sunt instalate pe computer.

  În mod implicit, componentele de criptare a datelor nu sunt incluse în Kaspersky Endpoint Security. Componenta Gestionare BitLocker nu afectează modificarea lungimii cheii de criptare.

Pentru a modifica lungimea cheii de criptare, executați fișierul kes_win.msi sau setup_kes.exe din pachetul de distribuție care conține biblioteca de criptare necesară. De asemenea, puteți face upgrade de la distanță a aplicației, utilizând pachetul de instalare.

Este imposibil să schimbați lungimea cheii de criptare utilizând pachetul de distribuție al aceleiași versiuni a aplicației instalate pe computer, fără să dezinstalați mai întâi aplicația.

Kaspersky Disk Encryption

Kaspersky Disk Encryption nu este acceptat pe computerele bazate pe arhitectura ARM.

Kaspersky Disk Encryption este disponibil numai pentru computerele pe care rulează un sistem de operare Windows pentru stații de lucru. Pentru computerele pe care rulează un sistem de operare Windows pentru servere, utilizați tehnologia BitLocker Drive Encryption.

Kaspersky Endpoint Security acceptă criptarea integrală a discurilor în sistemele de fișiere FAT32, NTFS și exFat.

Înainte de a începe criptarea Full Disk Encryption, aplicația rulează o serie de verificări pentru a determina dacă dispozitivul poate fi criptat, ceea ce include verificarea unității de hard disk de sistem pentru a vedea dacă este compatibilă cu Agentul de Autentificare sau cu componentele de criptare BitLocker. Pentru a verifica această compatibilitate, computerul trebuie repornit. După repornirea computerului, aplicația efectuează automat toate verificările necesare. Dacă verificarea compatibilității se încheie cu succes, criptarea Full Disk Encryption începe după încărcarea sistemului de operare și pornirea aplicației. Dacă se descoperă că unitatea de hard disk de sistem este incompatibilă cu Agentul de Autentificare sau componentele de criptare BitLocker, computerul trebuie pornit apăsând pe butonul hardware de resetare. Kaspersky Endpoint Security înregistrează în jurnal informațiile despre incompatibilitate. Pe baza acestor informații, aplicația nu începe criptarea Full Disk Encryption la pornirea sistemului de operare. Informații despre acest eveniment sunt înregistrare în rapoartele Kaspersky Security Center.

Dacă s-a schimbat configurația hardware a computerului, informațiile despre incompatibilitate înregistrate în jurnal de către aplicație la precedenta verificare trebuie șterse pentru a verifica din nou compatibilitatea unității de hard disk de sistem cu Agentul de Autentificare și componentele de criptare BitLocker. Pentru aceasta, înainte de criptarea Full Disk Encryption, tastează `avp pbatestreset` în linia de comandă. Dacă încărcarea sistemului de operare nu reușește după verificarea compatibilității unității de hard disk de sistem cu Agentul de Autentificare, trebuie să ștergi obiectele și datele rămase după operațiunea de testare pentru Agentul de Autentificare folosind Utilitarul de restaurare și apoi trebuie să pornești Kaspersky Endpoint Security și să execuți din nou comanda `avp pbatestreset`.

După începerea criptării Full Disk Encryption, Kaspersky Endpoint Security criptează toate datele scrise pe unitățile de hard disk.

Dacă utilizatorul oprește sau repornește computerul în cursul criptării Full Disk Encryption, Agentul de Autentificare se încarcă înainte de următoarea pornire a sistemului de operare. Kaspersky Endpoint Security reia criptarea Full Disk Encryption după autentificarea cu succes în Agentul de Autentificare și pornirea cu succes a sistemului de operare.

Dacă sistemul de operare trece în modul Hibernare în timpul criptării Full Disk Encryption, Agentul de Autentificare este încărcat atunci când sistemul de operare revine din modul Hibernare. Kaspersky Endpoint Security reia criptarea Full Disk Encryption după autentificarea cu succes în Agentul de Autentificare și pornirea cu succes a sistemului de operare.

Dacă sistemul de operare trece în modul Repaus în timpul criptării Full Disk Encryption, Kaspersky Endpoint Security reia criptarea Full Disk Encryption atunci când sistemul de operare revine din modul Hibernare, fără a încărca Agentul de Autentificare.

Autentificarea utilizatorului în Agentul de Autentificare poate fi efectuată în două moduri:

- Introdu numele de utilizator și parola pentru contul de Agent de Autentificare creat de administratorul rețelei LAN folosind instrumentele Kaspersky Security Center.
- Introdu parola pentru un simbol sau un simbol sau un card inteligent conectat la computer.

  Folosirea unui simbol sau card inteligent este disponibilă dacă unitățile de hard disk ale computerului au fost criptate utilizându-se algoritmul de criptare AES256. În cazul în care unitățile de hard disk ale computerului a fost criptate utilizându-se algoritmul de criptare AES56, adăugarea fișierului de certificat electronic la comandă va fi refuzată.

Agentul de Autentificare acceptă structuri de tastaturi pentru următoarele limbi:

- Engleză (Marea Britanie)
- Engleză (USA)
- Arabă (Algeria, Maroc, Tunisia; structură AZERTY)
- Spaniolă (America Latină)
- Italiană
- Germană (Germania și Austria)
- Germană (Elveția)
- Portugheză (Brazilia, structură ABNT2)
- Rusă (pentru tastaturi IBM/Windows cu 105 taste și structură QWERTY)
- Turcă (structură QWERTY)
- Franceză (Franța)
- Franceză (Elveția)

- Franceză (Belgia, structură AZERTY)
- Japoneză (pentru tastaturi cu 106 taste și structură QWERTY)

O structură de tastatură devine disponibilă în Agentul de Autentificare dacă acea structură a fost adăugată în setările de limbă și cele pentru standarde regionale din sistemul de operare și a devenit disponibilă în ecranul de bun venit din Microsoft Windows.

Dacă numele de cont din Agentul de Autentificare conține simboluri care nu pot fi introduse folosind structurile de tastatură disponibile în Agentul de Autentificare, unitățile de hard disk criptate pot fi accesate numai după ce sunt restaurate folosind Unitarul de restaurare sau după ce numele de cont și parola pentru Agentul de Autentificare sunt restaurate.

Caracteristici speciale ale criptării unității SSD

Aplicația acceptă criptarea unităților SSD, a unităților SSHD hibride și a unităților cu caracteristica Intel Smart Response. Aplicația nu acceptă criptarea unităților cu caracteristica Intel Rapid Start. Dezactivați caracteristica Intel Rapid Start înainte de a cripta o astfel de unitate.

Criptarea unităților SSD are următoarele caracteristici speciale:

- Dacă o unitate SSD este nouă și nu conține date confidențiale, activați criptarea numai a spațiului ocupat. Acest lucru vă permite să suprascrieți sectoarele de unitate relevante.
- Dacă o unitate SSD este utilizată și are date confidențiale, selectați una dintre următoarele opțiuni:
  - Ștergeți complet unitatea SSD (Secure Erase), instalați sistemul de operare și rulați criptarea unității SSD cu opțiunea de a cripta numai spațiul ocupat activată.
  - Rulați criptarea unității SSD cu opțiunea de a cripta numai spațiul ocupat dezactivată.

Criptarea unei unități SSD necesită 5-10 GO de spațiu liber. Cerințele de spațiu liber pentru stocarea datelor de administrare a criptării sunt furnizate în tabelul de mai jos.

Cerințe de spațiu liber pentru stocarea datelor de administrare a criptării

Dimensiunea unității SSD (GB)	Spațiu liber pe partiția principală a unității SSD (MB)	Spațiu liber pe partiția secundară a unității SSD (MB)
128	250	64
256	250	640
512	300	128

Pornirea Kaspersky Disk Encryption

Înainte de a începe criptarea Full Disk Encryption, vă recomandăm să vă asigurați că respectivul computer nu este infectat. Pentru aceasta, începe o activitate Scanare completă sau Scanare zone critice. Executarea unei criptări Full Disk Encryption pe un computer infectat de un rootkit poate face computer inutilizabil.

Înainte de a începe criptarea discului, trebuie să verifici setările conturilor Agent de Autentificare. Componenta Agent de autentificare este necesară pentru a lucra cu unități protejate folosind tehnologia Kaspersky Disk Encryption (FDE). Înainte de a încărcarea sistemul de operare, utilizatorul trebuie să completeze autentificarea cu Agentul. Kaspersky Endpoint Security vă permite să creați automat conturi Agent de Autentificare înainte de a cripta o unitate. Poți activa crearea automată a conturilor Agent de Autentificare în setările politicii Full Disk Encryption (consultă instrucțiunile de mai jos). Puteți utiliza, de asemenea, tehnologia Single Sign-On (SSO).

Kaspersky Endpoint Security îți permite să creezi automat Agentul de Autentificare pentru următoarele grupuri de utilizatori:

- **Toate conturile de pe computer**. Toate conturile de pe computer care au fost active în orice moment.
- **Toate conturile de domeniu de pe computer**. Toate conturile de pe computer care aparțin unui domeniu și care au fost active în orice moment.
- **Toate conturile locale de pe computer**. Toate conturile locale de pe computer care au fost active în orice moment.
- **Cont serviciu cu parolă de unică folosință**. Contul serviciului este necesar pentru a obține acces la computer, de exemplu, atunci când utilizatorul uită parola. De asemenea, poți utiliza contul serviciului drept cont de rezervă. Trebuie să introduci numele contului (în mod implicit, `ServiceAccount`). Kaspersky Endpoint Security creează automat o parolă. Poți găsi parola în consola Kaspersky Security Center.
- **Administrator local**. Kaspersky Endpoint Security creează un cont de utilizator pentru Agentul de Autentificare pentru administratorul local al computerului.
- **Manager computer**. Kaspersky Endpoint Security creează un cont de utilizator pentru Agentul de Autentificare pentru contul managerului computerului. Puteți vedea ce cont are rolul de manager de computer în proprietățile computerului din Active Directory. În mod implicit, rolul de manager de computer nu este definit, adică nu corespunde niciunui cont.
- **Cont activ**. Kaspersky Endpoint Security creează automat un cont Agent de Autentificare pentru contul care este activ în momentul criptării discului.

Activitatea *Gestionare conturi Agent de Autentificare* este concepută pentru configurarea setărilor de autentificare a utilizatorului. Puteți utiliza această activitate pentru a adăuga conturi noi, pentru a modifica setările conturilor curente sau pentru a elimina conturi, dacă este necesar. Puteți utiliza activități locale pentru calculatoare individuale, precum și activități de grup pentru computere din grupuri de administrare separate sau o selecție de computere.

Cum se execută Kaspersky Disk Encryption prin Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Criptare date** → **Full Disk Encryption**.
4. În lista verticală **Tehnologia de criptare**, selectează **Kaspersky Disk Encryption**.

   Tehnologia Kaspersky Disk Encryption nu poate fi folosită dacă computerul are unități de hard disk criptate de BitLocker.

5. În lista verticală **Mod criptare**, selectează **Se criptează toate unitățile de hard disk**.

Dacă pe computer sunt instalate mai multe sisteme de operare, după criptarea tuturor unităților de hard disk vei putea încărca doar sistemul de operare pe care este instalată aplicația.

Dacă trebuie să excluzi unele unități de hard disk de la procesul de criptare, creează o listă cu aceste unități de hard disk.

6. Configurați opțiunile avansate pentru componenta Kaspersky Disk Encryption (consultați tabelul de mai jos).
7. Salvați-vă modificările.

Cum se execută componenta Kaspersky Disk Encryption din Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.
   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Data Encryption** → **Full Disk Encryption**.
5. Selectează tehnologia **Kaspersky Disk Encryption**.

Tehnologia Kaspersky Disk Encryption nu poate fi folosită dacă computerul are unități de hard disk criptate de BitLocker.

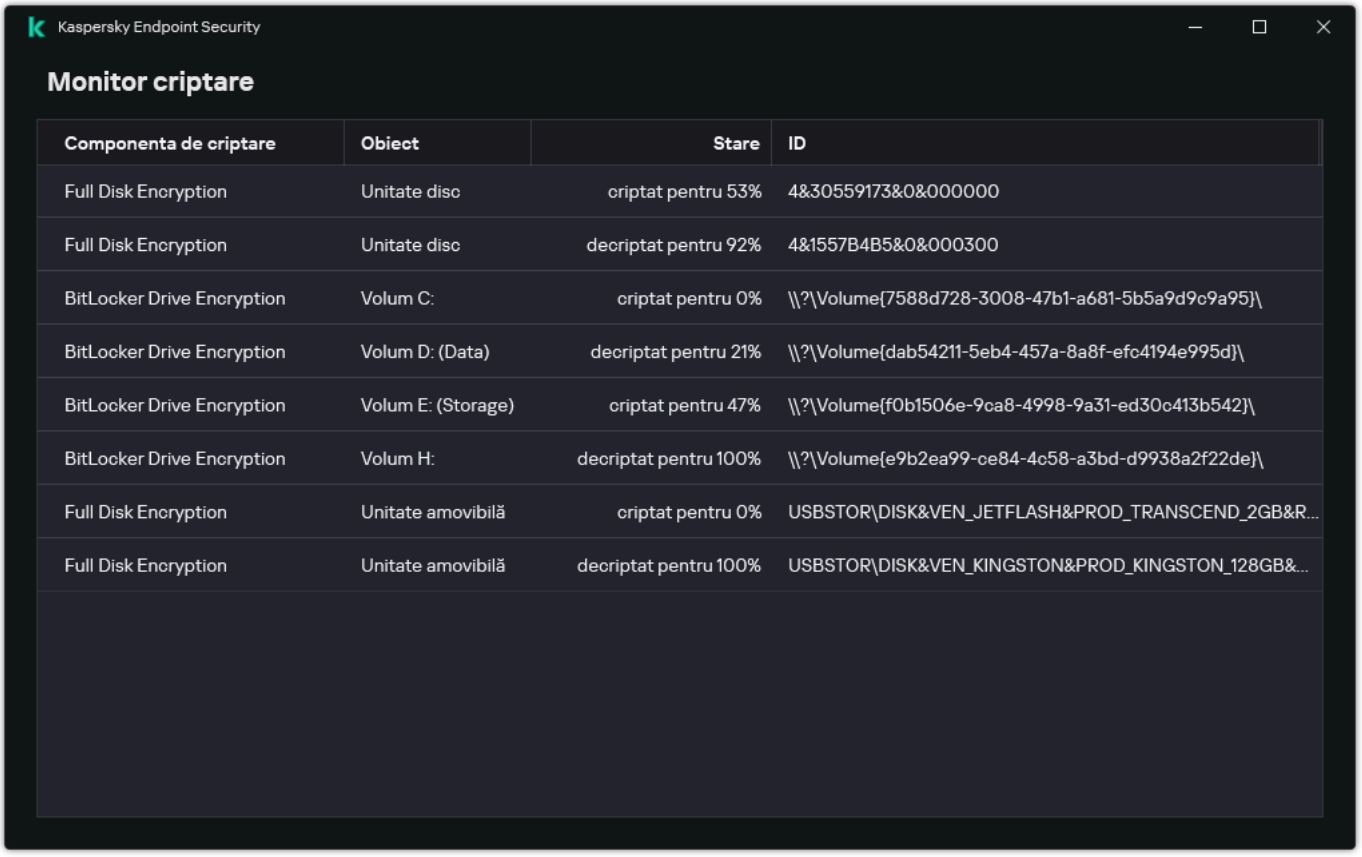
6. În secțiunea **Action on devices**, selectați **Encrypt all hard drives**.

Dacă pe computer sunt instalate mai multe sisteme de operare, după criptare vei putea încărca doar sistemul de operare cu care s-a efectuat criptarea.

Dacă trebuie să excluzi unele unități de hard disk de la procesul de criptare, creează o listă cu aceste unități de hard disk.

7. Configurați opțiunile avansate pentru componenta Kaspersky Disk Encryption (consultați tabelul de mai jos).
8. Salvați-vă modificările.

Puteți utiliza instrumentul Monitor criptare pentru controla procesul de criptare sau decriptare a discului de pe computerul unui utilizator. Puteți executa instrumentul Monitor criptare din fereastra principală a aplicației.



Monitor criptare

Dacă unitățile de hard disk de sistem sunt criptate, Agentul de Autentificare se încarcă înainte de pornirea sistemului de operare. Utilizează Agentul de Autentificare pentru a finaliza autentificarea și a obține accesul la unități de hard disk de sistem criptate și a încărca sistemul de operare. După finalizarea cu succes a procedurii de autentificare, se încarcă sistemul de operare. Procesul de autentificare se repetă de fiecare dată când sistemul de operare repornește.

Setările componentei Kaspersky Disk Encryption

Parametru	Descriere
Creați automat conturi Agent de autentificare pentru utilizatori în timpul criptării	Dacă această casetă de selectare este bifată, aplicația creează conturi Agent de autentificare pe baza listei conturilor de utilizatori Windows din computer. În mod implicit, Kaspersky Endpoint Security folosește toate conturile locale și de domenii cu care utilizatorul s-a conectat la sistemul de operare în ultimele 30 de zile.
Creați automat conturi Agent de autentificare pentru toți utilizatorii acestui computer după conectare	Dacă această casetă de selectare este bifată, aplicația verifică informații despre conturile utilizatorilor Windows de pe computer înainte de a porni Agentul de autentificare. Dacă Kaspersky Endpoint Security detectează un cont de utilizator Windows care nu are un cont Agent de autentificare, aplicația va crea un cont nou pentru accesarea unităților de disk criptate. Noul cont Agent de autentificare va avea următoarele setări implicite: numai conectare protejată prin parolă și modificarea parolei la prima autentificare. Prin urmare, nu trebuie să adăugați manual conturi Agent de autentificare utilizând activitatea *Gestionare conturi Agent de Autentificare* pentru computerele ale căror unități de hard disk sunt deja criptate.
Salvează nume de utilizator introdus în Agentul de Autentificare	Dacă această casetă de selectare este bifată, aplicația salvează numele contului Agent de Autentificare. Nu ți se va solicita să introduci numele contului la următoarea încercare de finalizare a autorizării în Agentul de Autentificare când folosești același cont.

Parametru	Descriere
Criptează doar spațiu de disc utilizat (reduce durata criptării)	Această casetă de selectare activează/dezactivează opțiunea care limitează zona de criptare la sectoarele ocupate de pe unitatea de hard disk. Această limită îți permite reducerea timpului necesar pentru criptare. Activarea sau dezactivarea caracteristicii **Criptează doar spațiu de disc utilizat (reduce durata criptării)** după pornirea criptării nu modifică această setare până când unitățile de hard disk nu sunt decriptate. Trebuie să bifezi sau să debifezi această casetă de selectare înainte de a începe criptarea. Dacă această casetă de selectare este bifată, sunt criptate numai poțiunile de pe unitatea de hard disk care sunt ocupate de fișiere. Kaspersky Endpoint Security criptează automat datele noi atunci când sunt adăugate. Dacă această casetă de selectare este debifată, va fi criptată întreaga unitate de hard disk, inclusiv fragmentele reziduale din fișiere șterse și modificate anterior. Această opțiune este recomandată pentru unități de hard disk noi, ale căror date nu au fost modificate sau șterse. Dacă aplici criptarea unei unități de hard disk aflate deja în uz, se recomandă să criptezi întreaga unitate de hard disk. Aceasta asigură protecția pentru toate datele, chiar și pentru datele șterse care pot fi eventual recuperate. În mod implicit, caseta de selectare este debifată.
Utilizează Legacy USB Support (nu se recomandă)	Această casetă de selectare activează sau dezactivează funcționalitatea Legacy USB Support. *Legacy USB Support* **este** o funcție BIOS/UEFI care vă permite să folosiți dispozitive USB (cum ar fi un token de securitate) în faza de pornire a computerului, înainte de a porni sistemul de operare (modul BIOS). Legacy USB Support nu afectează acceptarea dispozitivelor USB după pornirea sistemului de operare. Dacă această casetă de selectare este bifată, este activată acceptarea dispozitivelor USB la pornirea inițială a computerului. Când funcția Legacy USB Support este activată, Agentul de Autentificare în modul BIOS nu acceptă lucrul cu tokenuri prin USB. Se recomandă folosirea acestei opțiuni numai atunci când există o problemă de compatibilitate hardware și numai pentru acele computere pe care a apărut problema.

Crearea unei liste de unități de hard disk excluse de la criptare

Poți crea o listă de excluderi de la criptare numai pentru tehnologia Kaspersky Disk Encryption.

Pentru a crea o listă de unități de hard disk excluse de la criptare:

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Criptare date** → **Full Disk Encryption**.
4. În lista verticală **Tehnologia de criptare**, selectează **Kaspersky Disk Encryption**.

   Înregistrările care corespund unităților de hard disk excluse de la criptare apar în tabelul **Nu se criptează următoarele unități hard disk**. Acest tabel este gol dacă nu ai format anterior o listă de unități de hard disk care să fie excluse de la criptare.

5. Pentru a adăuga unități de hard disk noi la lista de unități de hard disk excluse de la criptare:

   a. Fă clic pe **Adaugă**.

   b. În fereastra care se deschide, specificați valorile pentru **Nume dispozitiv**, **Computer**, **Tip de disc**, **Kaspersky Disk Encryption**.

   c. Fă clic pe **Împrospătează**.

   d. În coloana **Nume**, bifează casetele de selectare din rândurile tabelului care corespund unităților de hard disk pe care dorești să le adaugi la lista de unități de hard disk excluse de la criptare.

   e. Fă clic pe **OK**.

   Unitățile de hard disk selectate apar în tabelul **Nu se criptează următoarele unități hard disk**.

6. Salvați-vă modificările.

Exportarea și importarea unei liste de unități de hard disk excluse de la criptare

Puteți exporta lista excluderilor de criptare a hard diskului într-un fișier XML. Apoi puteți modifica fișierul pentru a adăuga, de exemplu, un număr mare de excluderi de același tip. De asemenea, puteți utiliza funcția de export/import pentru a face o copie de rezervă a listei de excluderi sau pentru a migra excluderile pe un alt server.

Cum se exportă și se importă o listă de excluderi de criptare a hard diskului în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.

2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

3. În fereastra politicii, selectați **Criptare date** → **Full Disk Encryption**.

4. În lista verticală **Tehnologia de criptare**, selectează **Kaspersky Disk Encryption**.

   Înregistrările care corespund unităților de hard disk excluse de la criptare apar în tabelul **Nu se criptează următoarele unități hard disk**.

5. Pentru a exporta lista de excluderi:

   a. Selectați excluderile pe care doriți să le exportați. Pentru a selecta mai multe porturi, utilizați tastele **CTRL** sau **SHIFT**.

   Dacă nu ați selectat nicio excludere, Kaspersky Endpoint Security va exporta toate excluderile.

   b. Fă clic pe butonul → **Exportă**.

   c. În fereastra care se deschide, specificați numele fișierului XML în care doriți să exporți lista de excluderi și selectați directorul în care doriți să salvați acest fișier.

   d. Salvați fișierul.

   Kaspersky Endpoint Security exportă întreaga listă de excluderi în fișierul XML.

6. Pentru a importa lista de reguli:

   a. Fă clic pe butonul → **Importă**.

   b. În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de excluderi.

   c. Deschideți fișierul.

      În cazul în care computerul are deja o listă de excluderi, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul XML.

7. Salvați-vă modificările.

Cum se exportă și se importă o listă de excluderi de criptare a hard diskului în Consola Web

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **Data Encryption** → **Full Disk Encryption**.

   Selectează tehnologia **Kaspersky Disk Encryption**.

5. Faceți clic pe linkul **Exclusions**.

   Se deschide lista cu excluderi.

6. Pentru a exporta lista de reguli:

   a. Selectați excluderile pe care doriți să le exportați.

   b. Fă clic pe butonul → **Export**.

      Kaspersky Endpoint Security exportă lista de excluderi într-un fișier JSON în directorul pentru descărcări implicit.

7. Pentru a importa lista de excluderi:

   a. Fă clic pe butonul → **Import**.

      În fereastra care se deschide, selectați fișierul JSON din care doriți să importați lista de excluderi.

   b. Deschideți fișierul.

      În cazul în care computerul are deja o listă de excluderi, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul JSON.

8. Salvați-vă modificările.

Activarea tehnologiei Single Sign-On (SSO)

Tehnologia Single Sign-On (SSO) îți permite să te conectezi automat la sistemul de operare folosind acreditările Agentului de Autentificare. Aceasta înseamnă că un utilizator trebuie să introducă o parolă o singură dată când se conectează la Windows (parola contului Agent de Autentificare). Tehnologia Single Sign-On vă permite, de asemenea, să actualizați automat parola contului Agent de Autentificare atunci când parola contului Windows este schimbată.

Când utilizați tehnologia Single Sign-on, Agentul de Autentificare ignoră cerințele privind complexitatea parolei specificate în Kaspersky Security Center. Puteți seta cerințele privind complexitatea parolei în setările sistemului de operare.

Activarea tehnologiei Single Sign-On

Cum se activează tehnologia Single Sign-On în Consola de administrare. (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Criptare date** → **Setări de criptare comune**.
4. În blocul **Setări parolă**, fă clic pe butonul **Setări**.
5. În fereastra care se deschide, în fila **Agent de Autentificare**, bifează caseta de selectare **Utilizare tehnologia Single Sign-On (SSO)**.
6. Dacă utilizezi un furnizor de acreditări terț, bifează caseta de selectare **Încadrare furnizori acreditări terți**.
7. Salvați-vă modificările.

Drept urmare, utilizatorul trebuie să finalizeze procedura de autentificare doar o singură dată cu Agentul. Procedura de autentificare nu este necesară pentru încărcarea sistemului de operare. Sistemul de operare se încarcă automat.

Cum se activează utilizarea tehnologiei Single Sign-On în Web Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Data Encryption** → **Full Disk Encryption**.
5. Selectează tehnologia **Kaspersky Disk Encryption**.
6. În blocul **Password settings**, bifați caseta de selectare **Use Single Sign-On (SSO) technology**.

7. Dacă utilizezi un furnizor de acreditări terț, bifează caseta de selectare **Wrap third-party credential providers**.

8. Salvați-vă modificările.

Drept urmare, utilizatorul trebuie să finalizeze procedura de autentificare doar o singură dată cu Agentul. Procedura de autentificare nu este necesară pentru încărcarea sistemului de operare. Sistemul de operare se încarcă automat.

Pentru ca funcția Single Sign-On să funcționeze, parola contului Windows și parola pentru contul de Agent de Autentificare trebuie să se potrivească. Dacă parolele nu se potrivesc, utilizatorul trebuie să efectueze procedura de autentificare de două ori: în interfața Agentului de Autentificare și înainte de a încărca sistemul de operare. Aceste acțiuni trebuie efectuate o singură dată pentru a sincroniza parolele. După aceea, Kaspersky Endpoint Security înlocuiește parola contului Agentului de autentificare cu parola contului de Windows. Când parola contului Windows este schimbată, aplicația va actualiza automat parola pentru contul Agent de Autentificare.

Furnizori de acreditări terți

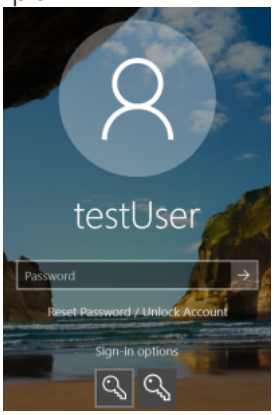
Kaspersky Endpoint Security acceptă furnizorul de acreditări terț ADSelfService Plus.

Când lucrați cu furnizori de acreditări terți, Agentul de Autentificare interceptează parola înainte ca sistemul de operare să fie încărcat. Aceasta înseamnă că un utilizator trebuie să introducă o parolă o singură dată când se conectează la Windows. După ce se conectează la Windows, utilizatorul poate utiliza capacitățile unui furnizor de acreditări terț pentru autentificare în serviciile corporative, de exemplu. Furnizorii de acreditări terți permit utilizatorilor să-și reseteze în mod independent propria parolă. În acest caz, Kaspersky Endpoint Security va actualiza automat parola pentru Agentul de Autentificare.

Dacă utilizați un furnizor de acreditări terț care nu este acceptat de aplicație, este posibil să întâmpinați anumite limitări în funcționarea tehnologiei Single Sign-On. Când vă conectați la Windows, vor fi disponibile două profiluri pentru utilizator: furnizorul de acreditări din sistem și furnizorul de acreditări terț. Pictogramele acestor profiluri vor fi identice (vezi figura de mai jos). Utilizatorul va avea următoarele opțiuni pentru a continua:

- Dacă utilizatorul selectează *furnizorul de acreditări terț*, Agentul de Autentificare nu va putea sincroniza parola cu contul Windows. Prin urmare, dacă utilizatorul a schimbat parola contului Windows, Kaspersky Endpoint Security nu poate actualiza parola pentru contul Agent de Autentificare. Ca rezultat, dacă parolele nu se potrivesc, utilizatorul trebuie să efectueze procedura de autentificare de două ori: în interfața Agentului de Autentificare și înainte de a încărca sistemul de operare. În acest caz, utilizatorul poate utiliza capacitățile unui furnizor de acreditări terț pentru autentificare în serviciile corporative, de exemplu.

- Dacă utilizatorul selectează *furnizorul de acreditări din sistem*, Agentul de Autentificare va sincroniza parolele cu contul Windows. În acest caz, utilizatorul nu poate utiliza capacitățile unui furnizor de acreditări terț pentru autentificare în serviciile corporative, de exemplu.



Profilul de autentificare în sistem și profilul de autentificare terț pentru conectarea la Windows

Gestionarea conturilor Agentului de Autentificare

Componenta Agent de autentificare este necesară pentru a lucra cu unități protejate folosind tehnologia Kaspersky Disk Encryption (FDE). Înainte de a încărcarea sistemul de operare, utilizatorul trebuie să completeze autentificarea cu Agentul. Activitatea *Gestionare conturi Agent de Autentificare* este concepută pentru configurarea setărilor de autentificare a utilizatorului. Puteți utiliza activități locale pentru calculatoare individuale, precum și activități de grup pentru computere din grupuri de administrare separate sau o selecție de computere.

Nu puteți configura o programare pentru pornirea activității *Gestionare conturi Agent de Autentificare*. De asemenea, este imposibil să opriți forțat o activitate.

Cum se creează activitatea Gestionare conturi Agent de Autentificare în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **New task**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Selectarea tipului activității

Selectați **Kaspersky Endpoint Security for Windows (14.1)** → **Gestionare conturi Agent de Autentificare**.

Pasul 2. Selectarea unei comenzi de gestionare a contului Agent de Autentificare

Generați o listă de comenzi de administrare a contului Agent de Autentificare. Comenzile de gestionare vă permit să adăugați, să modificați și să ștergeți conturile Agent de Autentificare (consultați instrucțiunile de mai jos). Doar utilizatorii care au un cont Agent de Autentificare pot finaliza procedura de autentificare, încărca sistemul de operare și obține acces la unitatea criptată.

Pasul 3. Selectarea dispozitivelor cărora le va fi atribuită activitatea

Selectați computerele pe care se va efectua activitatea. Sunt disponibile următoarele opțiuni:

- Atribuirea activității unui grup de administrare. În acest caz, activitatea este atribuită computerelor incluse într-un grup de administrare creat anterior.
- Selectare computere detectate în rețea de Serverul de administrare: *dispozitive neatribuite*. Dispozitivele specifice pot include dispozitive din grupuri de administrare, precum și dispozitive neatribuite.
- Specificarea manuală a adreselor computerelor sau importarea adreselor dintr-o listă. Poți specifica nume NetBIOS, adrese IP și subrețele IP ale dispozitivelor cărora dorești să le atribui activitatea.

Pasul 4. Definirea numelui activității

Introduceți un nume pentru activitate, de exemplu, *Conturi de administrator*.

Pasul 5. Finalizarea creării activității

Ieșiți din Expert. Dacă este necesar, bifați caseta de selectare **Run the task after the wizard finishes**. Puteți monitoriza progresul activității în proprietățile activității.

Drept urmare, după ce activitatea este finalizată la următoarea pornire a computerului, noul utilizator poate finaliza procedura de autentificare, încărca sistemul de operare și obține acces la unitatea criptată.

Cum se creează activitatea Gestionare conturi Agent de Autentificare în Web Console

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **Add**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Configurarea setările generale ale activității

Configurați setările generale pentru activitate:

1. În lista verticală **Application**, selectează **Kaspersky Endpoint Security for Windows (14.1)**.
2. În lista verticală **Task type**, selectează **Manage Authentication Agent accounts**.
3. În câmpul **Task name**, introduceți o descriere succintă, cum ar fi *Conturi de administrator*.
4. În blocul **Devices to which the task will be assigned**, selectați domeniul activității.

Pasul 2. Gestionarea conturilor Agentului de Autentificare

Generați o listă de comenzi de administrare a contului Agent de Autentificare. Comenzile de gestionare vă permit să adăugați, să modificați și să ștergeți conturile Agent de Autentificare (consultați instrucțiunile de mai jos). Doar utilizatorii care au un cont Agent de Autentificare pot finaliza procedura de autentificare, încărca sistemul de operare și obține acces la unitatea criptată.

Pasul 3. Finalizarea creării activității

Ieșiți din Expert. Se va afișa o activitate nouă în lista de activități.

Pentru a executa o activitate, bifează caseta de selectare de lângă activitate și fă clic pe butonul **Start**.

Drept urmare, după ce activitatea este finalizată la următoarea pornire a computerului, noul utilizator poate finaliza procedura de autentificare, încărca sistemul de operare și obține acces la unitatea criptată.

Pentru a adăuga un cont de Agent de Autentificare, trebuie să adăugați o comandă specială la activitatea *Gestionare conturi Agent de Autentificare*. Este convenabil să folosiți o activitate de grup, de exemplu, pentru a adăuga un cont de administrator la toate computerele.

Kaspersky Endpoint Security vă permite să creați automat conturi Agent de Autentificare înainte de a cripta o unitate. Puteți activa crearea automată a conturilor Agentului de Autentificare în Full Disk Encryption policy settings. Puteți utiliza, de asemenea, tehnologia Single Sign-On (SSO).

Cum se adaugă un cont Agent de Autentificare prin Consola de administrare (MMC)

1. Deschideți proprietățile activității *Gestionare conturi Agent de Autentificare*.
2. În proprietățile activității, selectați secțiunea **Setări**.
3. Faceți clic pe **Adaugă** → **Comandă de adăugare cont**.
4. În fereastra care se deschide, în câmpul **Cont Windows**, specificați numele contului Microsoft Windows care va fi utilizat pentru a crea contul Agent de Autentificare.
5. Dacă ați introdus manual numele contului Windows, faceți clic pe butonul **Permite** pentru a defini identificatorul de securitate al contului (SID).

   Dacă ai ales să nu determini identificatorul de securitate (SID) făcând clic pe butonul **Permite**, SID-ul va fi determinat atunci când este executată activitatea pe computer.

   > Definirea unui identificator de securitate a contului Windows este necesară pentru a verifica dacă numele contului Windows a fost introdus corect. În cazul în care contul Windows nu există pe computer sau în domeniul de încredere, activitatea *Gestionare conturi Agent de Autentificare* se va încheia cu o eroare.

6. Bifați caseta de selectare **Înlocuire cont existent** dacă vrei să înlocuiești un cont existent creat anterior pentru Agentul de Autentificare cu contul creat acum.

   Acest pas este disponibil atunci când adaugi o comandă de creare pentru contul de Agent de Autentificare în proprietățile unei activități de grup pentru administrarea conturilor de Agent de Autentificare. Acest pas este disponibil atunci când adăgați o comandă de creare pentru contul de Agent de Autentificare în proprietățile unei activități locale pentru *Gestionare conturi Agent de Autentificare*.

7. În câmpul **Nume utilizator**, tastează numele contului de Agent de Autentificare care trebuie introdus în cursul autentificării pentru a accesa unitățile de hard disk criptate.

8. Bifați caseta de selectare **Permitere autentificare pe bază de parolă** dacă dorești ca aplicația să solicite utilizatorului introducerea parolei de cont de Agent de Autentificare în cursul autentificării pentru a accesa unitățile de hard disk criptate. Setați o parolă pentru contul Agent de Autentificare. Dacă este necesar, puteți solicita o nouă parolă de la utilizator după prima autentificare.

9. Bifați caseta de selectare **Permitere autentificare pe bază de certificat** dacă dorești ca aplicația să solicite utilizatorului să conecteze un simbol sau un card inteligent la computer în cursul procesului de autentificare, pentru a accesa unitățile de hard disk criptate. Selectați un fișier certificat pentru autentificare cu un card inteligent sau un simbol.

10. Dacă este nevoie, în câmpul **Descriere comandă**, introdu detaliile pentru contul de Agent de Autentificare de care ai nevoie pentru administrarea comenzii.

11. În blocul **Acces la autentificare în Agentul de Autentificare**, configurați accesul la autentificare în Agentul de Autentificare pentru utilizatorul care folosește contul specificat în comandă.

12. Salvați-vă modificările.

Cum se adaugă un cont Agent de Autentificare prin Web Console

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe activitatea **Manage Authentication Agent accounts** a Kaspersky Endpoint Security.

   Se va deschide fereastra de proprietăți a activității.

3. Selectați fila **Application settings**.

4. În lista de conturi Agent de Autentificare, faceți clic pe butonul **Add**.

   Aceasta pornește Expertul de gestionare a contului Agent de Autentificare.

5. Selectați tipul de comandă **Add**.

6. Selectați un cont de utilizator. Puteți selecta un cont din lista conturilor de domeniu sau puteți introduce manual numele contului. Mergeți la pasul următor.

   Kaspersky Endpoint Security determină identificatorul de securitate al contului (SID). Acest lucru este necesar pentru verificarea contului. Dacă ați introdus greșit numele de utilizator, Kaspersky Endpoint Security va încheia sarcina cu o eroare.

7. Configurați setările contului Agent de Autentificare.

   - **Create a new Authentication Agent account to replace the existing account**. Kaspersky Endpoint Security scanează conturile existente pe computer. Dacă ID-ul de securitate al utilizatorului pe computer și în potrivirea activităților, Kaspersky Endpoint Security va modifica setările contului utilizatorului în conformitate cu activitatea.

   - **User name**. Numele de utilizator implicit al contului Agent de autentificare corespunde numelui de domeniu al utilizatorului.

   - **Allow password-based authentication**. Setați o parolă pentru contul Agent de Autentificare. Dacă este necesar, puteți solicita o nouă parolă de la utilizator după prima autentificare. În acest fel, fiecare utilizator va avea propria parolă unică. Puteți seta, de asemenea, cerințele privind complexitatea parolei pentru contul Agent de Autentificare în politică.

   - **Allow certificate-based authentication**. Selectați un fișier certificat pentru autentificare cu un card inteligent sau un simbol. În acest fel, utilizatorul va trebui să introducă parola pentru cardul inteligent sau simbol.

   - **Account access to encrypted data**. Configurați accesul utilizatorului la unitatea criptată. Puteți, de exemplu, dezactiva temporar autentificarea utilizatorului în loc să ștergeți contul Agent de Autentificare.

   - **Comment**. Introduceți o descriere a contului, dacă este necesar.

8. Salvați-vă modificările.

9. Bifați caseta de selectare de lângă activitate și faceți clic pe butonul **Start**.

   Drept urmare, după ce activitatea este finalizată la următoarea pornire a computerului, noul utilizator poate finaliza procedura de autentificare, încărca sistemul de operare și obține acces la unitatea criptată.

Pentru a schimba parola și alte setări ale contului Agent de Autentificare, trebuie să adăugați o comandă specială la activitatea *Gestionare conturi Agent de Autentificare*. Este convenabil să folosiți o activitate de grup, de exemplu, pentru a înlocui certificatul simbolului administratorului pe toate computerele.

Cum se modifică un cont Agent de Autentificare prin Consola de administrare (MMC)

1. Deschideți proprietățile activității *Gestionare conturi Agent de Autentificare*.

2. În proprietățile activității, selectați secțiunea **Setări**.

3. Faceți clic pe **Adaugă** → **Comandă de editare cont**.

4. În fereastra care se deschide, în câmpul **Cont Windows**, specificați numele contului de utilizator Microsoft Windows pe care doriți să îl schimbați.

5. Dacă ați introdus manual numele contului Windows, faceți clic pe butonul **Permite** pentru a defini identificatorul de securitate al contului (SID).

   Dacă ai ales să nu determini identificatorul de securitate (SID) făcând clic pe butonul **Permite**, SID-ul va fi determinat atunci când este executată activitatea pe computer.

   Definirea unui identificator de securitate a contului Windows este necesară pentru a verifica dacă numele contului Windows a fost introdus corect. În cazul în care contul Windows nu există pe computer sau în domeniul de încredere, activitatea *Gestionare conturi Agent de Autentificare* se va încheia cu o eroare.

6. Bifați caseta de selectare **Modificare nume utilizator** și introdu un nume nou pentru contul de Agent de autentificare dacă dorești ca aplicația Kaspersky Endpoint Security să modifice numele de utilizator pentru toate conturile de Agent de autentificare create folosind contul Microsoft Windows cu numele indicat în câmpul **Cont Windows** cu numele introdus în câmpul de mai jos.

7. Bifați caseta de selectare **Modificare setări de autentificare bazată pe parolă** pentru ca setările de autentificare bazate pe parolă să poată fi editate.

8. Bifați caseta de selectare **Permitere autentificare pe bază de parolă** dacă dorești ca aplicația să solicite utilizatorului introducerea parolei de cont de Agent de Autentificare în cursul autentificării pentru a accesa unitățile de hard disk criptate. Setați o parolă pentru contul Agent de Autentificare.

9. Bifați caseta de selectare **Editează regula de modificarea a parolei la autentificarea în Agentul de Autentificare** dacă dorești ca aplicația Kaspersky Endpoint Security să modifice valoare setării pentru modificarea parolei pentru toate conturile de Agent de autentificare create folosind contul Microsoft Windows cu numele indicat în câmpul **Cont Windows** cu valoarea pentru setare specificată mai jos.

10. Specifică valoarea pentru setarea de modificare a parolei la autentificarea în Agentul de Autentificare.

11. Bifați caseta de selectare **Modificare setări de autentificare bazată pe certificat** pentru a putea edita setările de autentificare bazate pe un certificat electronic al unui simbol sau card inteligent.

12. Bifați caseta de selectare **Permitere autentificare pe bază de certificat** dacă dorești ca aplicația să solicite utilizatorului să introducă parola pentru simbolul sau cardul inteligent conectat la computer în cursul procesului de autentificare, pentru a accesa unitățile de hard disk criptate. Selectați un fișier certificat pentru autentificare cu un card inteligent sau un simbol.

13. Bifați caseta de selectare **Editare descriere comandă** și editează descrierea comenzii dacă dorești ca aplicația Kaspersky Endpoint Security să modifice descrierea comenzii pentru toate conturile de Agent de autentificare create pe baza contului Microsoft Windows cu numele indicat în câmpul **Cont Windows**.

14. Bifați caseta de selectare **Editează regula de acces la autentificare în Agentul de Autentificare** dacă dorești ca aplicația Kaspersky Endpoint Security să modifice regula pentru accesul utilizatorului la dialogul de autentificare în Agentul de Autentificare cu valoarea specificată mai jos pentru toate conturile de Agent de Autentificare create utilizând contul Microsoft Windows cu numele indicat în câmpul **Cont Windows**.

15. Specifică regula pentru accesul la dialogul de autentificare în Agentul de Autentificare.

16. Salvați-vă modificările.

Cum se modifică un cont Agent de Autentificare prin Web Console

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe activitatea **Manage Authentication Agent accounts** a Kaspersky Endpoint Security.

   Se va deschide fereastra de proprietăți a activității.

3. Selectați fila **Application settings**.

4. În lista de conturi Agent de Autentificare, faceți clic pe butonul **Add**.

   Aceasta pornește Expertul de gestionare a contului Agent de Autentificare.

5. Selectați tipul de comandă **Change**.

6. Selectați un cont de utilizator. Puteți selecta un cont din lista conturilor de domeniu sau puteți introduce manual numele contului. Mergeți la pasul următor.

   Kaspersky Endpoint Security determină identificatorul de securitate al contului (SID). Acest lucru este necesar pentru verificarea contului. Dacă ați introdus greșit numele de utilizator, Kaspersky Endpoint Security va încheia sarcina cu o eroare.

7. Bifați casetele de selectare de lângă setările pe care doriți să le editați.

8. Configurați setările contului Agent de Autentificare.

   - **Create a new Authentication Agent account to replace the existing account**. Kaspersky Endpoint Security scanează conturile existente pe computer. Dacă ID-ul de securitate al utilizatorului pe computer și în potrivirea activităților, Kaspersky Endpoint Security va modifica setările contului utilizatorului în conformitate cu activitatea.

   - **User name**. Numele de utilizator implicit al contului Agent de autentificare corespunde numelui de domeniu al utilizatorului.

   - **Allow password-based authentication**. Setați o parolă pentru contul Agent de Autentificare. Dacă este necesar, puteți solicita o nouă parolă de la utilizator după prima autentificare. În acest fel, fiecare utilizator va avea propria parolă unică. Puteți seta, de asemenea, cerințele privind complexitatea parolei pentru contul Agent de Autentificare în politică.

   - **Allow certificate-based authentication**. Selectați un fișier certificat pentru autentificare cu un card inteligent sau un simbol. În acest fel, utilizatorul va trebui să introducă parola pentru cardul inteligent sau simbol.

   - **Account access to encrypted data**. Configurați accesul utilizatorului la unitatea criptată. Puteți, de exemplu, dezactiva temporar autentificarea utilizatorului în loc să ștergeți contul Agent de Autentificare.

   - **Comment**. Introduceți o descriere a contului, dacă este necesar.

9. Salvați-vă modificările.

10. Bifați caseta de selectare de lângă activitate și faceți clic pe butonul **Start**.

Pentru a șterge un cont Agent de Autentificare, trebuie să adăugați o comandă specială la activitatea *Gestionare conturi Agent de Autentificare*. Este convenabil să folosiți o activitate de grup, de exemplu, pentru a șterge contul unui angajat concediat.

Cum se șterge un cont Agent de Autentificare prin Consola de administrare (MMC)

1. Deschideți proprietățile activității *Gestionare conturi Agent de Autentificare*.

2. În proprietățile activității, selectați secțiunea **Setări**.

3. Faceți clic pe **Adaugă** → **Comandă de ștergere cont**.

4. În fereastra care se deschide, în câmpul **Cont Windows**, specificați numele contului de utilizator Windows care a fost folosit pentru a crea contul Agent de Autentificare pe care doriți să-l ștergeți.

5. Dacă ați introdus manual numele contului Windows, faceți clic pe butonul **Permite** pentru a defini identificatorul de securitate al contului (SID).

   Dacă ai ales să nu determini identificatorul de securitate (SID) făcând clic pe butonul **Permite**, SID-ul va fi determinat atunci când este executată activitatea pe computer.

Definirea unui identificator de securitate a contului Windows este necesară pentru a verifica dacă numele contului Windows a fost introdus corect. În cazul în care contul Windows nu există pe computer sau în domeniul de încredere, activitatea *Gestionare conturi Agent de Autentificare* se va încheia cu o eroare.

6. Salvați-vă modificările.

Cum se șterge un cont Agent de Autentificare prin Web Console

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe activitatea **Manage Authentication Agent accounts** a Kaspersky Endpoint Security.

   Se va deschide fereastra de proprietăți a activității.

3. Selectați fila **Application settings**.

4. În lista de conturi Agent de Autentificare, faceți clic pe butonul **Add**.

   Aceasta pornește Expertul de gestionare a contului Agent de Autentificare.

5. Selectați tipul de comandă **Delete**.

6. Selectați un cont de utilizator. Puteți selecta un cont din lista conturilor de domeniu sau puteți introduce manual numele contului.

7. Salvați-vă modificările.

8. Bifați caseta de selectare de lângă activitate și faceți clic pe butonul **Start**.

   Drept urmare, după finalizarea activității la următoarea pornire a computerului, utilizatorul nu va putea finaliza procedura de autentificare și încărca sistemul de operare. Kaspersky Endpoint Security va refuza accesul la datele criptate.

Pentru a vizualiza lista utilizatorilor care pot finaliza autentificarea cu Agentul și pot încărca sistemul de operare, trebuie să accesați proprietățile computerului gestionat.

Cum se vizualizează lista conturilor Agent de Autentificare prin Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.

2. În arborele consolei, selectați **Devices**.

3. Fă dublu clic pentru a deschide fereastra cu proprietățile computerului.

4. În fereastra cu proprietățile computerului, selectează secțiunea **Tasks**.

5. În lista de activități, selectează **Gestionare conturi Agent de Autentificare** și deschide proprietățile sarcinii făcând dublu clic.

6. În proprietățile activității, selectați secțiunea **Setări**.

   Drept urmare, veți putea accesa o listă de conturi Agent de Autentificare pe acest computer. Doar utilizatorii din listă pot finaliza autentificarea cu Agentul și pot încărca sistemul de operare.

Cum se vizualizează o listă a conturilor Agent de Autentificare prin Web Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Assets (Devices)**.
2. Faceți clic pe numele computerului pe care doriți să vizualizați lista conturilor Agent de Autentificare.
3. În proprietățile computerului, selectează fila **Tasks**.
4. În lista verticală, selectează **Manage Authentication Agent accounts**.
5. În proprietățile activității, selectați fila **Application settings**.

Drept urmare, veți putea accesa o listă de conturi Agent de Autentificare pe acest computer. Doar utilizatorii din listă pot finaliza autentificarea cu Agentul și pot încărca sistemul de operare.

Folosirea unui simbol/card inteligent cu Agentul de Autentificare

Un simbol sau un card inteligent poate fi folosit pentru autentificare atunci când se accesează unități de hard disk criptate. Pentru aceasta, trebuie să adăugați fișierul de certificat electronic a unui simbol sau card inteligent în activitatea *Gestionare conturi Agent de Autentificare*.

Folosirea unui simbol sau card inteligent este disponibilă dacă unitățile de hard disk ale computerului au fost criptate utilizându-se algoritmul de criptare AES256. În cazul în care unitățile de hard disk ale computerului a fost criptate utilizându-se algoritmul de criptare AES56, adăugarea fișierului de certificat electronic la comandă va fi refuzată.

Kaspersky Endpoint Security acceptă următoarele simboluri, cititoare de carduri inteligente și carduri inteligente:

- 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.

Pentru a adăuga fișierul certificatului electronic al unui simbol sau card inteligent la comanda de creare a unui cont de Agent de Autentificare, mai întâi trebuie să salvezi fișierul folosind software terț pentru administrarea certificatelor.

Certificatul simbolului sau al cardului inteligent trebuie să aibă următoarele proprietăți:

- Certificatul trebuie să fie conform cu standardul X.509 și fișierul certificatului trebuie să aibă codificarea DER.
- Certificatul conține o cheie RSA cu o lungime de cel puțin 1024 de biți.

Dacă certificatul electronic al simbolului sau cardului inteligent nu îndeplinește aceste cerințe, nu puteți încărca fișierul certificat în comandă pentru crearea unui cont Agent de Autentificare.

Parametrul `KeyUsage` al certificatului trebuie să aibă valoarea `keyEncipherment` sau `dataEncipherment`. Parametrul `KeyUsage` determină scopul certificatului. Dacă parametrul are o valoare diferită, Kaspersky Security Center va descărca fișierul certificat, dar va afișa un avertisment.

Dacă un utilizator a pierdut un token sau un card inteligent, administratorul trebuie să adauge fișierul unui certificat electronic pentru token sau cardul inteligent la comanda pentru crearea unui cont de Agent de Autentificare. Apoi utilizatorul trebuie să finalizeze procedura pentru acordarea accesului la dispozitivele criptate sau pentru restaurarea datelor pe dispozitive criptate.

Decriptarea unităților de hard disk

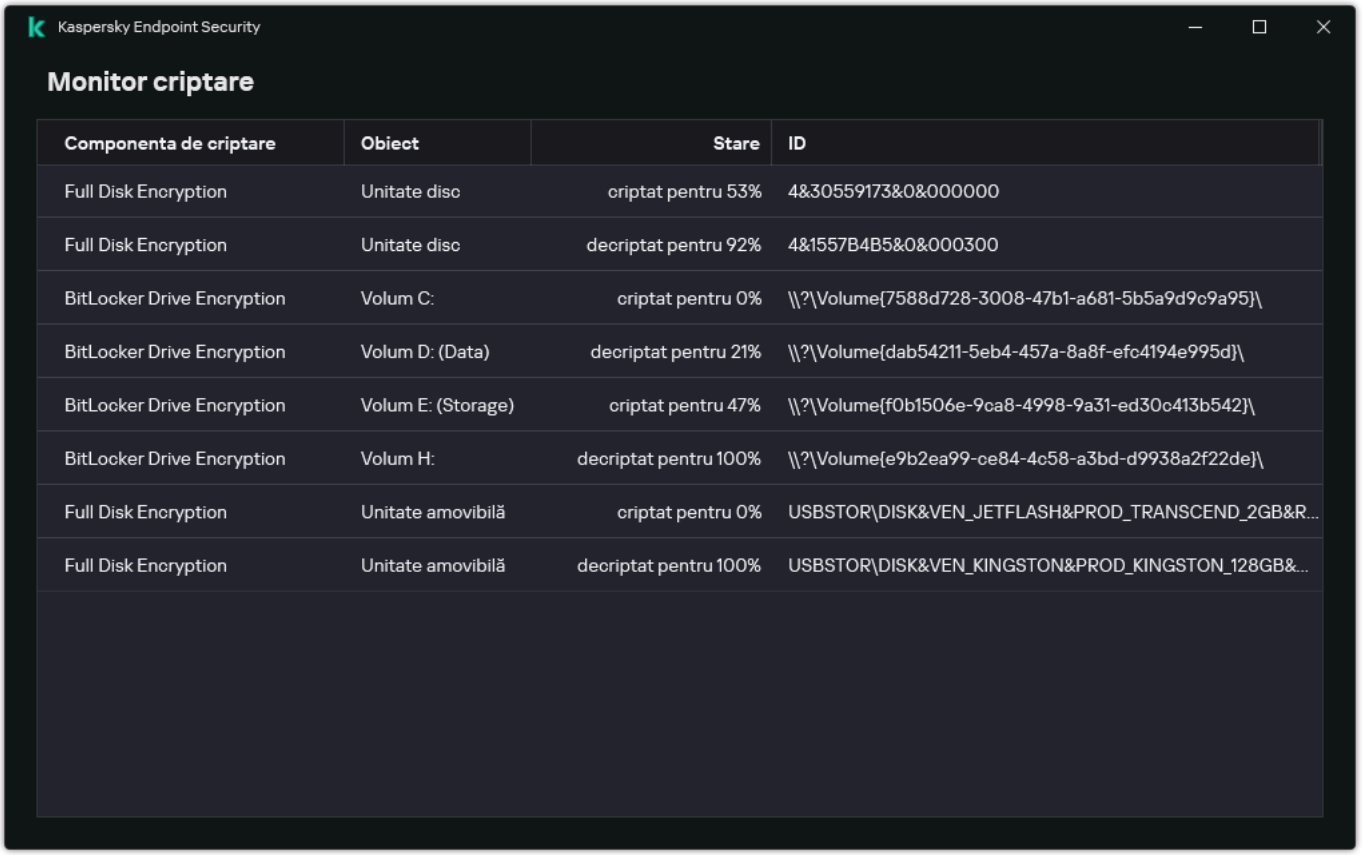
Poți decripta unități de hard disk chiar dacă nu există nicio licență curentă care permite criptarea datelor.

Pentru a decripta unități de hard disk:

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Criptare date** → **Full Disk Encryption**.
4. În lista verticală **Tehnologia de criptare**, selectați tehnologia cu care vor fi criptate unitățile de hard disk.
5. Efectuează una dintre următoarele acțiuni:
   - În lista verticală **Mod criptare**, selectați opțiunea **Se decriptează toate unitățile de hard disk** dacă dorești să decriptezi toate unitățile de hard disk criptate.
   - Adăugați unitățile de hard disk criptate pe care doriți să le decriptați în tabelul **Nu se criptează următoarele unități hard disk**.

     Această opțiune este disponibilă numai pentru tehnologia Kaspersky Disk Encryption.
6. Salvați-vă modificările.

Puteți utiliza instrumentul Monitor criptare pentru controla procesul de criptare sau decriptare a discului de pe computerul unui utilizator. Puteți executa instrumentul Monitor criptare din fereastra principală a aplicației.



Monitor criptare

Dacă utilizatorul închide sau repornește computerul în timpul decriptării unităților de hard disk care au fost criptate utilizându-se tehnologia Kaspersky Disk Encryption, Agentul de Autentificare se încarcă înainte de următoarea pornire a sistemului de operare. Kaspersky Endpoint Security reia criptarea unității de hard disk după autentificarea cu succes în Agentul de Autentificare și pornirea cu succes a sistemului de operare.

Dacă sistemul de operare trece în modul Hibernare în timpul decriptării unităților de hard disk care au fost criptate utilizându-se tehnologia Kaspersky Disk Encryption, Agentul de Autentificare se încarcă atunci când sistemul de operare revine din modul Hibernare. Kaspersky Endpoint Security reia criptarea unității de hard disk după autentificarea cu succes în Agentul de Autentificare și pornirea cu succes a sistemului de operare. După decriptarea unității de hard disk, modul Hibernare nu mai este disponibil până la următoarea rebootare a sistemului de operare.

Dacă sistemul de operare trece în modul Repaus în timpul decriptării unității de hard disk, Kaspersky Endpoint Security reia decriptarea unităților de hard disk atunci când sistemul de operare revine din modul Hibernare, fără a încărca Agentul de Autentificare.

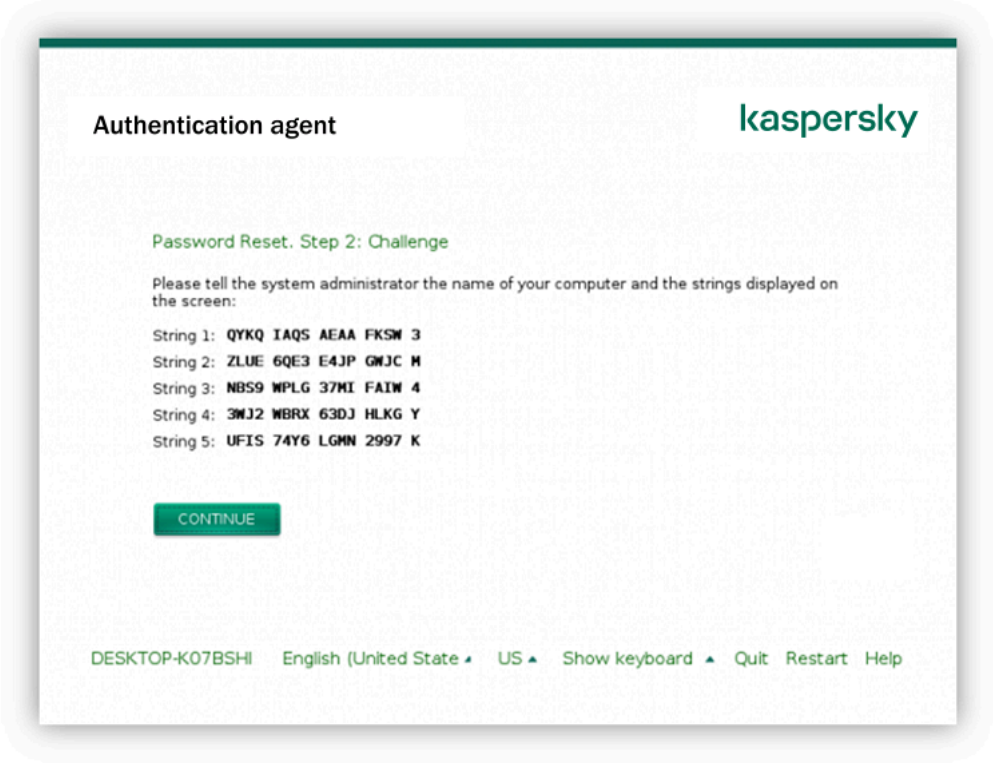
Restabilirea accesului la o unitate protejată de tehnologia Kaspersky Disk Encryption

Dacă un utilizator a uitat parola pentru accesarea unei unități de hard disk protejată de tehnologia Kaspersky Disk Encryption, trebuie să începeți procedura de recuperare (Solicitare-Răspuns). De asemenea, poți utiliza contul serviciului pentru a obține acces la unitatea de hard disk dacă această caracteristică este activată în setările de criptare a discului.

Restaurarea accesului la unitatea de hard disk a sistemului

Restaurarea accesului la o unitate de hard disk a sistemului protejată de tehnologia Kaspersky Disk Encryption constă în următorii pași:

1. Utilizatorul raportează administratorul blocurilor de solicitare (consultați figura de mai jos).
2. Administratorul introduce blocurile de solicitare în Kaspersky Security Center, primește blocurile de răspuns și raportează blocurile de răspuns utilizatorului.
3. Utilizatorul introduce blocurile de răspuns în interfața Agentului de Autentificare și obține acces la unitatea de hard disk.



Restaurarea accesului la o unitate de hard disk a sistemului protejată de tehnologia Kaspersky Disk Encryption

Pentru a începe procedura de recuperare, utilizatorul trebuie să facă clic pe butonul **Forgot your password** din interfața Agent de Autentificare.

Cum se obțin blocurile de răspuns pentru o unitate de hard disk a sistemului protejată de tehnologia Kaspersky Disk Encryption în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați **Devices**.
3. În fila **Devices**, selectați computerul utilizatorului care solicită accesul la datele criptate și faceți clic dreapta pe el pentru a deschide meniul contextual.
4. În meniul contextual, selectați **Acordare acces în modul offline**.
5. Se deschide o fereastră; în acea fereastră, selectați fila **Agent de Autentificare**.

6. În blocul **Algoritm de criptare aflat în uz**, selectați un algoritm de criptare: **AES56** sau **AES256**.

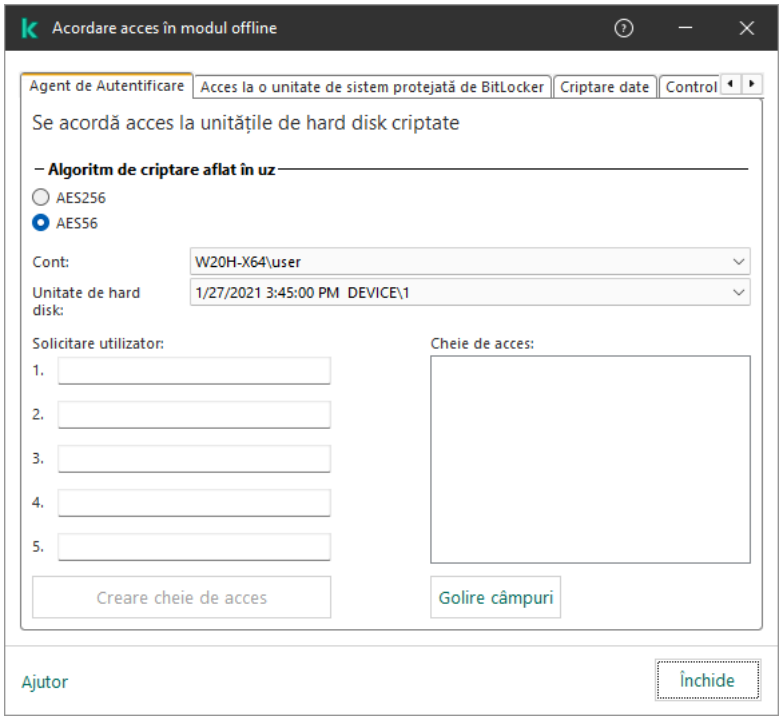
   Algoritmul de criptare a datelor depinde de biblioteca de criptare AES care este inclusă în pachetul de distribuție: *Strong encryption (AES256)* sau *Lite encryption (AES56)*. Biblioteca de criptare AES este instalată împreună cu aplicația.

7. În lista verticală **Cont**, selectați numele contului de Agent de Autentificare al utilizatorului care a solicitat recuperarea accesului la unitate.

8. În lista verticală **Unitate de hard disk**, selectați unitatea de hard disk criptată pentru care trebuie să recuperezi accesul.

9. În blocul **Solicitare utilizator**, introdu blocurile din solicitarea dictată de utilizator.

În consecință, conținutul blocurilor de răspunsul la solicitarea utilizatorului de recuperare a numelui de utilizator și a parolei unui cont de Agent de Autentificare va fi afișat în câmpul **Cheie de acces**. Transmite utilizatorului conținutul blocurilor de răspuns.



Acordarea accesului în modul offline

Cum se obțin blocurile de răspuns pentru o unitate de hard disk a sistemului protejată de tehnologia Kaspersky Disk Encryption în Web Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Assets (Devices)**.

2. Bifați caseta de selectare de lângă numele computerului la a cărui unitate doriți să restaurați accesul.

3. Fă clic pe **Grant access to the device in offline mode**.

4. În fereastra care se deschide, selectați secțiunea **Authentication Agent**.

5. În lista verticală **Account**, selectați numele contului de Agent de Autentificare creat pentru utilizatorul care solicită recuperarea numelui de utilizator și a parolei unui cont de Agent de Autentificare.

6. Introduceți blocurile de solicitare transmise de utilizator.

Conținutul blocurilor din răspunsul la solicitarea utilizatorului de recuperare a numelui de utilizator și a parolei contului de Agent de Autentificare este afișat în partea de jos a ferestrei. Transmite utilizatorului conținutul blocurilor de răspuns.

După finalizarea procedurii de recuperare, Agentul de autentificare va solicita utilizatorului să schimbe parola.

Restaurarea accesului la o unitate de hard disk care nu aparține sistemului

Restaurarea accesului la o unitate de hard disk care nu aparține sistemului dar este protejată de tehnologia Kaspersky Disk Encryption constă în următorii pași:

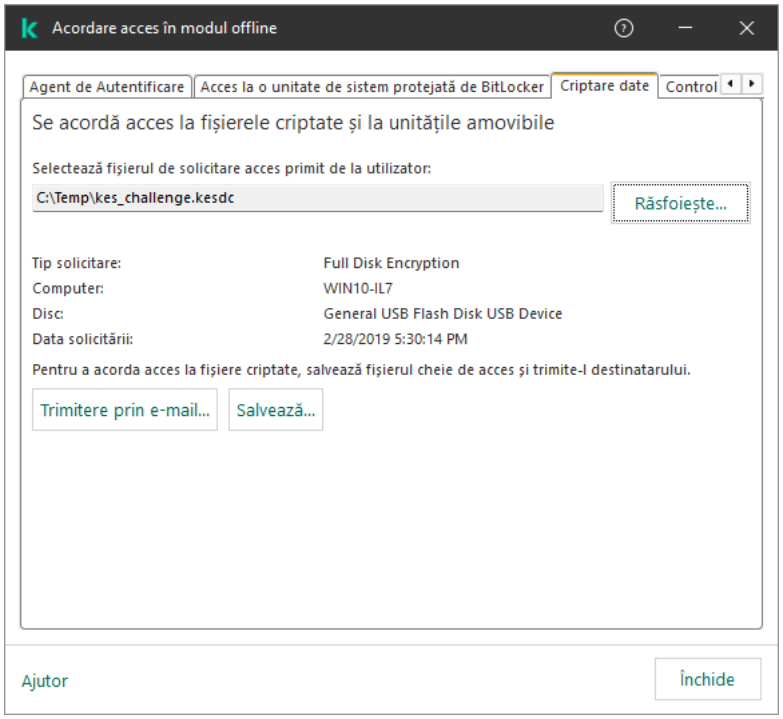
1. Utilizatorul trimite administratorului un fișier de solicitare a accesului.
2. Administratorul adaugă fișierul de solicitare a accesului în Kaspersky Security Center, creează un fișier cheie de acces și trimite fișierul către utilizator.
3. Utilizatorul adaugă fișierul cheie de acces în Kaspersky Endpoint Security și obține acces la unitatea de hard disk.

Pentru a începe procedura de recuperare, utilizatorul trebuie să încerce să acceseze o unitate de hard disk. Drept urmare, Kaspersky Endpoint Security va crea un fișier de solicitare a accesului (un fișier cu extensia KESDC), pe care utilizatorul trebuie să-l trimită administratorului, de exemplu, prin e-mail.

Cum se obține un fișier cheie de acces pentru o unitate de hard disk criptată care nu aparține sistemului în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați **Devices**.
3. În fila **Devices**, selectați computerul utilizatorului care solicită accesul la datele criptate și faceți clic dreapta pe el pentru a deschide meniul contextual.
4. În meniul contextual, selectați **Acordare acces în modul offline**.
5. Se deschide o fereastră; în acea fereastră, selectați fila **Criptare date**.
6. În fila **Criptare date**, faceți clic pe butonul **Răsfoiește**.
7. În fereastra pentru selectarea unui fișier de solicitare a accesului, specificați calea către fișierul primit de la utilizator.

Veți vedea informații despre solicitarea utilizatorului. Kaspersky Security Center generează un fișier cheie. Trimiteți utilizatorului prin e-mail fișierul cheie de acces la date criptate generat. Sau salvați fișierul de acces și utilizați orice metodă disponibilă pentru a transfera fișierul.



Acordarea accesului în modul offline

Cum se obține un fișier cheie de acces la unitatea de hard disk care nu aparține sistemului criptat în Web Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Assets (Devices)**.
2. Bifați caseta de selectare de lângă numele computerului la ale cărui date doriți să restaurați accesul.
3. Fă clic pe **Grant access to the device in offline mode**.
4. Selectați **Data Encryption**.
5. Faceți clic pe butonul **Select file** și selectați fișierul de solicitare a accesului pe care l-ați primit de la utilizator (un fișier cu extensia KESDC).

   Web Console va afișa informații despre solicitare. Acestea vor include numele computerului pe care utilizatorul solicită acces la fișier.
6. Faceți clic pe butonul **Save key** și selectați un director pentru a salva fișierul cheie de acces la datele criptate (un fișier cu extensia KESDR).

Drept urmare, veți putea obține cheia de acces la datele criptate, pe care va trebui să o transferați utilizatorului.

Conectarea cu ajutorul contul serviciului Agent de Autentificare

Kaspersky Endpoint Security vă permite să adăugați automat un cont serviciu Agent de Autentificare când se criptează o unitate. Contul serviciului este necesar pentru a obține acces la computer, de exemplu, atunci când utilizatorul uită parola. De asemenea, poți utiliza contul serviciului drept cont de rezervă. Pentru a adăuga un cont, selectează un cont de serviciu în setările de criptare a discului și introdu numele contului de utilizator (în mod implicit, `ServiceAccount`). Pentru a te autentifica folosind agentul, vei avea nevoie de o parolă de unică folosință.

Cum poți afla parola de unică folosință în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați **Devices**.
3. Fă dublu clic pentru a deschide fereastra cu proprietățile computerului.
4. În fereastra cu proprietățile computerului, selectează secțiunea **Tasks**.
5. În lista de activități, selectează **Gestionare conturi Agent de Autentificare** și deschide proprietățile sarcinii făcând dublu clic.
6. În fereastra cu proprietățile activității, selectați secțiunea **Setări**.
7. În lista de conturi, selectează contul serviciului Agent de Autentificare (de exemplu, `WIN10-USER\ServiceAccount`).
8. În lista verticală **Acțiune**, selectează **Vizualizează cont**.
9. În proprietățile contului, bifează caseta de selectare **Afișare parolă originală**.
10. Copie parola de unică folosință pentru conectarea cu ajutorul contului serviciului.

Cum poți afla parola de unică folosință în Web Console

1. În fereastra principală a Web Console, selectați **Asset management → Assets (Devices)**.
2. Faceți clic pe numele computerului pe care doriți să vizualizați lista conturilor Agent de Autentificare.

   Se vor deschide proprietățile computerului.
3. În proprietățile computerului, selectează fila **Tasks**.
4. În lista verticală, selectează **Manage Authentication Agent accounts**.
5. În proprietățile activității, selectați fila **Application settings**.
6. În lista de conturi, selectează contul serviciului Agent de Autentificare (de exemplu, `WIN10-USER\ServiceAccount`).
7. În proprietățile contului, bifează caseta de selectare **Show password**.
8. Copie parola de unică folosință pentru conectarea cu ajutorul contului serviciului.

Kaspersky Endpoint Security actualizează automat parola de fiecare dată când un utilizator se autentifică folosind contul serviciului. După autentificarea cu ajutorul agentului, trebuie să introduci parola contului Windows. Când te conectezi cu ajutorul contului serviciului, nu poți utiliza tehnologia SSO.

Actualizarea sistemului de operare

Există o serie de considerații speciale pentru actualizarea sistemului de operare al unui computer care este protejat de Full Disk Encryption (FDE). Actualizați sistemul de operare după cum urmează: mai întâi actualizați sistemul de operare pe un computer, apoi actualizați sistemul de operare pe câteva dintre computere, apoi actualizați sistemul de operare pe toate computerele rețelei.

Dacă utilizați tehnologia Kaspersky Disk Encryption, Agentul de autentificare este încărcat înainte de pornirea sistemului de operare. Utilizând aplicația Agent de autentificare, utilizatorul se poate conecta la sistem și poate primi acces la unitățile criptate. Apoi sistemul de operare începe să se încarce. Dacă porniți o actualizare a sistemului de operare pe un computer protejat folosind tehnologia Kaspersky Disk Encryption, expertul de actualizare a sistemului de operare va elimina aplicația Agent de autentificare. Drept urmare, computerul poate fi blocat deoarece încărcătorul sistemului de operare nu va putea accesa unitatea criptată.

Caracteristici ale actualizării sistemului de operare:

- **Actualizarea sistemului de operare prin WSUS**. Poți actualiza sistemul de operare în mod obișnuit.
- **Actualizarea sistemului de operare din ISO**. Pentru a actualiza sistemul de operare, trebuie să specifici directorul cu driverele Kaspersky de criptare a discului. Aplicația copiază automat driverele într-un director separat. Efectuează următoarele acțiuni:

  1. Montează imaginea ISO.
  2. Începe instalarea actualizării sistemului cu următoarea cheie:

     ```
     setup.exe /ReflectDrivers %ProgramFiles(x86)%\Kaspersky Lab\KES.14.1\reflect_drivers
     ```

Actualizarea automată a sistemului de operare este disponibilă numai dacă pe computer se execută Windows 10 1607 (RS1) sau o versiune ulterioară. Pentru a actualiza versiunile anterioare ale sistemului de operare, se recomandă să decriptezi mai întâi discul, să efectuezi o actualizare a sistemului de operare și apoi să criptezi discul.

Dacă utilizați tehnologia BitLocker Drive Encryption, nu este necesar să decriptați unitățile de hard disk pentru a actualiza Windows 10. Pentru mai multe detalii despre BitLocker, accesați site-ul web Microsoft.

Eliminarea erorilor de actualizare a funcționalității de criptare

Componenta Full Disk Encryption este actualizată atunci când se face upgrade pentru o versiune anterioară a aplicației la Kaspersky Endpoint Security for Windows 14.1.

La pornirea actualizării funcționalității Full Disk Encryption pot apărea următoarele erori:

- Imposibil de inițializat actualizarea.
- Dispozitivul este incompatibil cu Agentul de Autentificare.

Pentru a elimina erorile survenite la pornirea procesului de actualizare a funcționalității Full Disk Encryption în versiunea nouă a aplicației:

1. Decriptează unitățile de hard disk.
2. Criptează unitățile de hard disk din nou.

În timpul actualizării funcționalității Full Disk Encryption pot apărea următoarele erori:

- Imposibil de finalizat actualizarea.
- Derularea înapoi a upgrade-ului pentru Full Disk Encryption s-a finalizat cu o eroare.

Pentru a elimina erorile survenite în timpul procesului de actualizare a funcționalității Full Disk Encryption,

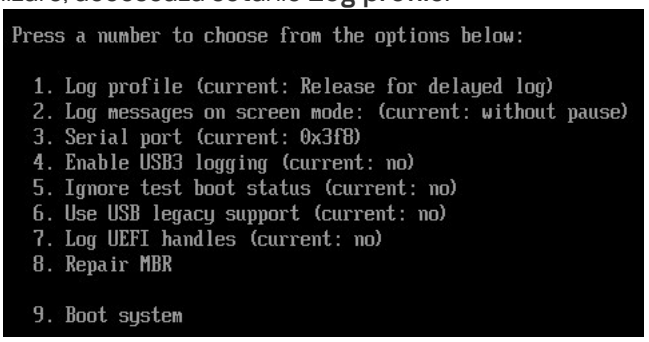
restaurează accesul la fișiere criptate folosind Utilitarul de restaurare.

Urmărirea Agentului de autentificare

Aplicația înregistrează în jurnal informațiile de serviciu despre funcționarea Agentului de Autentificare și informații despre operațiunile utilizatorului cu Agentul de Autentificare în fișierul de urmărire.

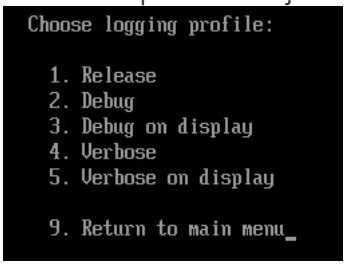
Pentru a activa urmărirea Agentului de autentificare:

1. Activează urmărirea Kaspersky Endpoint Security.
2. Repornește computerul.
3. Imediat ce computerul cu unitățile de hard disk criptate este pornit, apasă pe butonul **F3** pentru a apela o fereastră pentru configurarea setărilor Agentului de Autentificare.
4. După pornirea programului de inițializare a sistemului FDE, selectează managerul de inițializare **KES (FDE <version>)**.
5. În meniul managerului de inițializare, accesează setările **Log profile**.



Meniul managerului de inițializare

6. Selectează nivelul de urmărire în fereastra de setări a profilului de jurnal:



Niveluri de urmărire ale Agentului de autentificare

- **Release**. Dacă este selectată această opțiune, aplicația nu înregistrează în jurnal informațiile despre evenimentele Agentului de Autentificare în fișierul de urmărire.
- **Debug**. Dacă este selectată această opțiune, aplicația înregistrează în jurnal informațiile despre funcționarea Agentului de Autentificare și operațiunile utilizatorului cu Agentul de Autentificare în fișierul de urmărire.

- **Debug on display**. Dacă este selectată această opțiune, aplicația înregistrează în jurnal informațiile despre funcționarea Agentului de Autentificare și operațiunile utilizatorului cu Agentul de Autentificare în fișierul de urmărire și transmite aceste informații prin portul COM.

  Dacă un computer cu unități de hard disk criptate este conectat la un alt computer prin portul COM, evenimentele Agentului de Autentificare pot fi examinate de pe celălalt computer.

- **Verbose**. Dacă este selectată această opțiune, aplicația înregistrează în jurnal informațiile detaliate despre funcționarea Agentului de Autentificare și operațiunile utilizatorului cu Agentul de Autentificare în fișierul de urmărire.

  > Nivelul de detalii pentru înregistrările efectuate cu această opțiune este mai mare în comparație cu nivelul pentru opțiunea **Debug**. Un nivel mai mare de detalii pentru înregistrări poate încetini pornirea Agentului de Autentificare și a sistemului de operare.

- **Verbose on display**. Dacă este selectată această opțiune, aplicația înregistrează în jurnal informațiile detaliate despre funcționarea Agentului de Autentificare și operațiunile utilizatorului cu Agentul de Autentificare în fișierul de urmărire și transmite aceste informații prin portul COM.

  > Nivelul de detalii pentru înregistrările efectuate cu această opțiune este mai mare în comparație cu nivelul pentru opțiunea **Debug on display**. Un nivel mai mare de detalii pentru înregistrări poate încetini pornirea Agentului de Autentificare și a sistemului de operare.

După ce selectezi un nivel de urmărire, managerul de inițializare afișează din nou meniul.

7. În meniul managerului de inițializare, selectează **Boot system**.

   Programul de inițializare a sistemului FDE pornește Agentul de autentificare.

   Reprodu problema.

   Datele sunt înregistrate în fișierul de urmărire al Agentului de Autentificare dacă există unități de hard disk criptate pe computer sau în cursul criptării Full Disk Encryption.

8. Pentru a opri procesul de urmărire, revino la fereastra Instrumente de suport și dezactivează urmărirea.

Ca rezultat, fișierele de urmărire a funcționării KES.SRV a Agentului de autentificare sunt create în directorul `%ProgramData%\Kaspersky Lab\KES.14.1\Traces`. Fișierul de urmărire al Agentului de Autentificare nu este trimis către Kaspersky, spre deosebire de alte fișiere de urmărire ale aplicației. Dacă este necesar, poți trimite manual fișierul de urmărire al Agentului de Autentificare către Kaspersky pentru analiză.

Editarea textelor de ajutor ale Agentului de Autentificare

> Înainte de a edita mesajele de ajutor ale Agentului de Autentificare, recitiți lista caracterelor acceptare într-un mediu preîncărcare (vedeți mai jos).

Pentru a edita mesajele de ajutor ale Agentului de Autentificare:

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.

2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

3. În fereastra politicii, selectați **Criptare date** → **Setări de criptare comune**.

4. În blocul **Șabloane**, fă clic pe butonul **Ajutor**.

5. În fereastra care se deschide, procedează după cum urmează:

   - Selectați fila **Autentificare** pentru a edita textul de ajutor afișat în fereastra Agentului de Autentificare atunci când sunt introduse acreditările contului.

   - Selectați fila **Modifică parola** pentru a edita textul de ajutor afișat în fereastra Agentului de Autentificare atunci când parola pentru contul de Agent de Autentificare este modificată.

   - Selectați fila **Recuperare parolă** pentru a edita textul de ajutor afișat în fereastra Agentului de Autentificare atunci când parola pentru contul de Agent de Autentificare este recuperată.

6. Editează mesajele de ajutor.

   Dacă dorești să restaurezi textul original, faceți clic pe butonul **În mod implicit**.

   > Poți introduce text de ajutor care conține 16 rânduri sau mai puțin. Lungimea maximă este de 64 de caracter pe rând.

7. Salvați-vă modificările.

Suport limitat pentru caractere în mesajele de ajutor pentru Agentul de Autentificare

Într-un mediu preboot, sunt acceptate următoarele caractere Unicode:

- Alfabetul latin de bază (0000 - 007F)
- Caractere suplimentare Latin-1 (0080 - 00FF)
- Caractere extinse Latin-A (0100 - 017F)
- Caractere extinse Latin-B (0180 - 024F)
- Caractere ID extinse necombinate (02B0 - 02FF)
- Semne diacritice combinate (0300 - 036F)
- Alfabetele grecesc și cel copt (0370 - 03FF)
- Chirilic (0400 - 04FF)
- Ebraic (0590 - 05FF)
- Script arabic (0600 - 06FF)
- Caractere latine suplimentare extinse (1E00 - 1EFF)
- Semne de punctuație (2000 - 206F)
- Simboluri de monede (20A0 - 20CF)

- Simboluri de tip literă (2100 - 214F)
- Figuri geometrice (25A0 - 25FF)
- Forme de prezentare din setul arab script-B (FE70 - FEFF)

Caracterele care nu sunt specificate în această listă nu sunt acceptate într-un mediu preboot. Nu se recomandă utilizarea acestor caractere în mesajele de ajutor pentru Agentul de Autentificare.

Eliminarea obiectelor și datelor rămase după testarea funcționării Agentului de Autentificare

În cursul dezinstalării aplicației, dacă Kaspersky Endpoint Security detectează obiecte și date care au rămas pe unitatea de hard disk de sistem după operațiunea de testare pentru Agentul de Autentificare, dezinstalarea aplicației este întreruptă și devine imposibilă până când aceste obiecte și date nu sunt eliminate.

Obiectele și datele pot rămâne pe unitatea de hard disk de sistem după operațiunea de testare pentru Agentul de Autentificare numai în cazuri excepționale. De exemplu, acest lucru se poate întâmpla dacă computerul nu a fost repornit după aplicarea unei politici a Kaspersky Security Center cu setări de criptare sau dacă aplicația nu reușește să pornească după operațiunea de testare pentru Agentul de Autentificare.

Puteți elimina obiectele și datele rămase pe unitatea de hard disk a sistemului după operațiunea de testare pentru Agentul de Autentificare în următoarele moduri:

- Folosind politica aplicației Kaspersky Security Center.
- folosind Utilitarul de restaurare.

Pentru a folosi o politică a aplicației Kaspersky Security Center pentru a elimina obiectele și datele rămase după operațiunea de testare pentru Agentul de Autentificare:

1. Aplică pe computer o politică a aplicației Kaspersky Security Center cu setările configurate pentru decriptarea tuturor unităților de hard disk ale computerului.
2. Pornește Kaspersky Endpoint Security.

Pentru a folosi un Utilitar de restaurare pentru a elimina obiectele și datele rămase după operațiunea de testare pentru Agentul de Autentificare:

1. Executați fișierul numit fdert.exe, care este fișierul executabil al Utilitarului de restaurare. Acest fișier este creat de Kaspersky Endpoint Security.
2. În fereastra Utilitar de restaurare, selectați dispozitivul necesar.
3. Fă clic pe **Scanează**.
4. Dacă, după diagnosticarea hard disk-ului de sistem, primești un mesaj care indică faptul că obiecte și date au rămas din operațiunea de testare a Agentului de autentificare, fă clic pe **Șterge obiecte și date AA**.

Butonul **Șterge obiecte și date AA** este disponibil numai dacă sunt detectate obiecte și date rămase după operațiunea de testare a Agentului de autentificare.

Pentru a elimina informațiile despre incompatibilitatea aplicației cu Agentul de Autentificare,

tastează comanda `avp pbatestreset` în linia de comandă.

Gestionare Bitlocker

BitLocker este o tehnologie de criptare încorporată în sistemele de operare Windows. Kaspersky Endpoint Security îți permite să controlezi și să gestionezi Bitlocker folosind infrastructura Kaspersky Next. BitLocker criptează volumele logice. BitLocker nu poate fi utilizat pentru criptarea unităților amovibile. Pentru detalii suplimentare despre BitLocker, consultați documentația Microsoft.

La criptarea discului, BitLocker plasează programul de încărcare a comenzilor de inițiere și alte fișiere auxiliare în system partition. Această partiție nu este criptată. Sistemul de operare creează automat partiția de sistem în timpul instalării programului Windows. Dacă discul este partiționat complet înainte de instalarea programului Windows, sistemul de operare nu poate crea o partiție de sistem. În acest caz, când pornești criptarea discului cu BitLocker, sistemul de operare îți solicită să partiționeze din nou discul și să creezi o partiție de sistem. După crearea unei partiții de sistem, sistemul de operare pornește criptarea BitLocker.

Algoritmul de criptare BitLocker nu depinde de versiunea Bibliotecii AES inclusă în pachetul de distribuție (AES256 sau AES56). Criptarea utilizează biblioteca de criptare încorporată a sistemului de operare.

În mod implicit, aplicația utilizează algoritmul de criptare BitLocker cu o lungime efectivă a cheii de 256 de biți pentru a cripta dispozitivele care nu au fost niciodată criptate. Pentru un dispozitiv care a fost criptat înainte de instalarea aplicației, algoritmul de criptare poate fi diferit. Pentru informații detaliate despre selectarea algoritmului de criptare, consultați Site-ul web de asistență tehnică Microsoft. Începând cu versiunea 12.9, Kaspersky Endpoint Security trimite cheia de recuperare originală pentru dispozitivele criptate anterior de aplicații terțe către Kaspersky Security Center.

BitLocker asigură stocarea securizată a cheilor de acces folosind un modul de platformă de încredere. Un *Trusted Platform Module* (TPM) este un microcip dezvoltat pentru a furniza funcții de bază legate de securitate (de exemplu, pentru stocarea cheilor de criptare). Un Trusted Platform Module este de obicei instalat pe placa de bază a computerului și interacționează cu toate celelalte componente ale sistemului prin intermediul magistralei hardware. Utilizarea TPM este cea mai sigură modalitate de a stoca cheile de acces BitLocker, deoarece TPM oferă verificarea integrității sistemului înainte de pornire. Puteți cripta în continuare unitățile de pe computer fără un TPM. În acest caz, cheia de acces va fi criptată cu o parolă. BitLocker utilizează următoarele metode de autentificare:

- TPM.
- TPM și PIN.
- Parolă.

După criptarea hard disk-ului sistemului, utilizatorul trebuie să parcurgă procesul de autentificarea BitLocker pentru a porni sistemul de operare. După autentificare, BitLocker va permite utilizatorilor să se conecteze. BitLocker nu acceptă tehnologia de conectare unică (SSO).

După criptarea unei unități, BitLocker creează o cheie de recuperare. Kaspersky Endpoint Security trimite cheia de recuperare către Kaspersky Security Center astfel încât să poți restabili accesul la disc, de exemplu, dacă un utilizator și-a uitat parola.

Dacă un utilizator criptează un disc folosind BitLocker, Kaspersky Endpoint Security va trimite cheia de recuperare și informații despre criptarea discului către Kaspersky Security Center.

Dacă utilizați politicile de grup ale Windows, dezactivați gestionareaa BitLocker în setările politicii. Setările politicii Windows pot intra în conflict cu setările politicii Kaspersky Endpoint Security. Când criptați o unitate, pot apărea erori.

Pornirea BitLocker Drive Encryption

Înainte de a începe criptarea Full Disk Encryption, vă recomandăm să vă asigurați că respectivul computer nu este infectat. Pentru aceasta, începe o activitate Scanare completă sau Scanare zone critice. Executarea unei criptări Full Disk Encryption pe un computer infectat de un rootkit poate face computer inutilizabil.

Pentru a utiliza BitLocker Drive Encryption pe computerele pe care rulează sisteme de operare Windows pentru servere, poate fi necesară instalarea componentei BitLocker Drive Encryption. Instalați componenta folosind instrumentele sistemului de operare (Expert adăugare roluri și componente). Pentru mai multe informații despre instalarea BitLocker Drive Encryption, consultați documentația Microsoft.

Cum se rulează BitLocker Drive Encryption prin Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Criptare date** → **Full Disk Encryption**.
4. În lista verticală **Tehnologia de criptare**, selectează **BitLocker Drive Encryption**.
5. În lista verticală **Mod criptare**, selectează **Se criptează toate unitățile de hard disk**.

   Dacă pe computer sunt instalate mai multe sisteme de operare, după criptare vei putea încărca doar sistemul de operare cu care s-a efectuat criptarea.

6. Configurați opțiunile avansate pentru componenta BitLocker Drive Encryption (consultați tabelul de mai jos).
7. Salvați-vă modificările.

Cum se rulează componenta BitLocker Drive Encryption din Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.
   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Data Encryption** → **Full Disk Encryption**.

5. Selectează tehnologia **BitLocker Disk Encryption**.

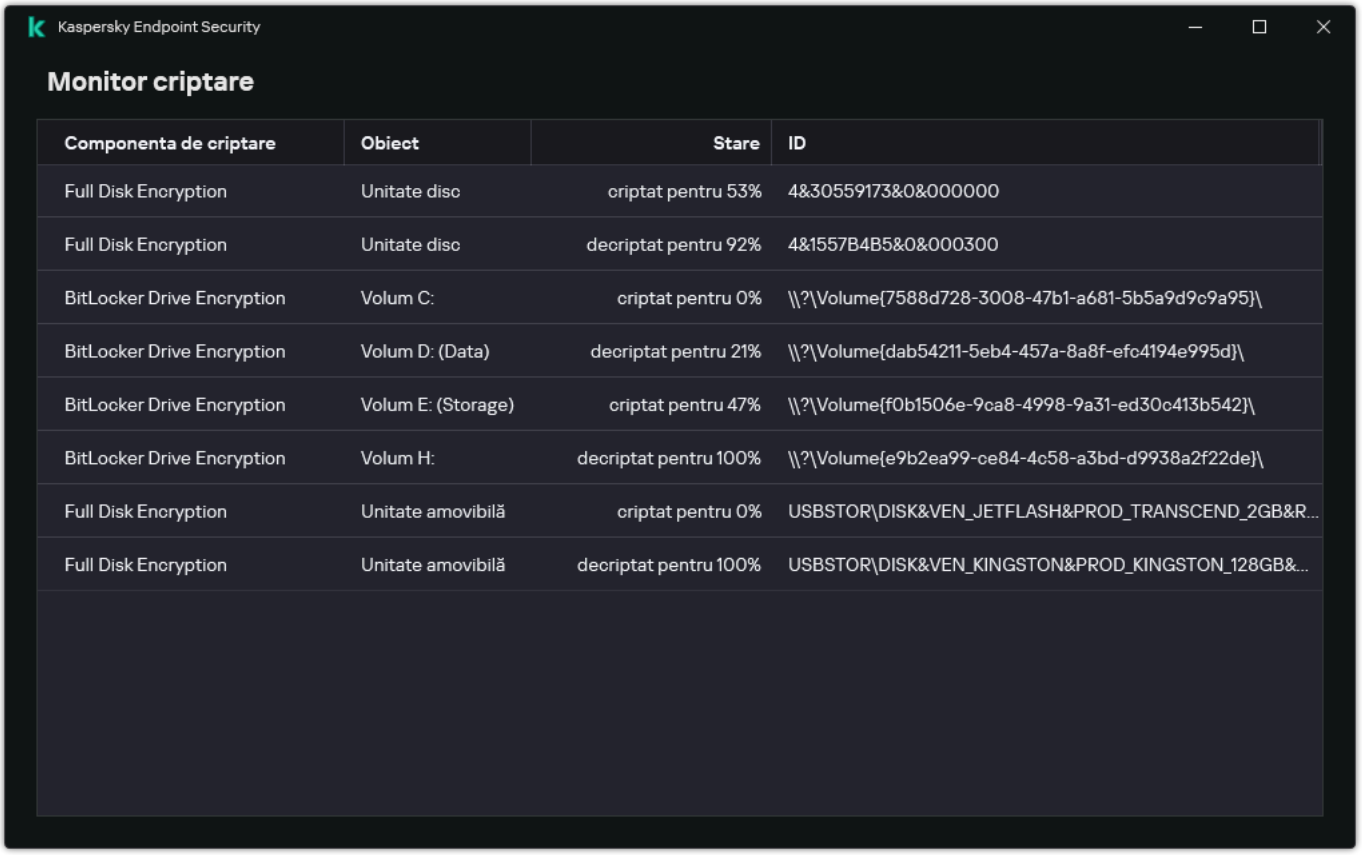
6. În secțiunea **Action on devices**, selectați **Encrypt all hard drives**.

Dacă pe computer sunt instalate mai multe sisteme de operare, după criptare vei putea încărca doar sistemul de operare cu care s-a efectuat criptarea.

7. Configurați opțiunile avansate pentru componenta BitLocker Drive Encryption (consultați tabelul de mai jos).

8. Salvați-vă modificările.

Puteți utiliza instrumentul Monitor criptare pentru controla procesul de criptare sau decriptare a discului de pe computerul unui utilizator. Puteți executa instrumentul Monitor criptare din fereastra principală a aplicației.



Monitor criptare

După ce politica este aplicată, aplicația va afișa următoarele interogări, în funcție de setările de autentificare:

- Numai TPM. Nu este necesară intervenția utilizatorului. Discul va fi criptat când repornește computerul.
- TPM + PIN / Parolă. Dacă este disponibil un modul TPM, va apărea o fereastră de solicitare a codului PIN. Dacă nu este disponibil un modul TPM, vei vedea o fereastră de solicitare a parolei pentru autentificarea preboot.
- Numai parolă. Vei vedea o fereastră de introducere a parolei pentru autentificarea preboot.

Dacă modul de compatibilitate standard Federal Information Processing este activat pentru sistemul de operare al computerului, atunci, în Windows 8 și versiuni anterioare ale sistemului de operare, se afișează o solicitare pentru conectarea unui dispozitiv de stocare pentru salvarea fișierului cheie de recuperare. Puteți salva mai multe fișiere cheie de recuperare pe un singur dispozitiv de stocare.

După setarea unei parole sau a unui cod PIN, BitLocker vă va solicita să reporniți computerul pentru a finaliza criptarea. În continuare, utilizatorul trebuie să parcurgă procedura de autentificare a componentei BitLocker. După procedura de autentificare, utilizatorul trebuie să se conecteze la sistem. După încărcarea sistemului de operare, BitLocker va finaliza criptarea.

Dacă nu există acces la cheile de criptare, utilizatorul îi poate solicita administratorului rețelei locale să îi furnizeze o cheie de recuperare (în cazul în care cheia de recuperare nu a fost salvată anterior pe dispozitivul de stocare sau a fost pierdută).

Setările componentei BitLocker Drive Encryption

Parametru	Descriere
Permite utilizare autentificare BitLocker, care solicită intrarea de la tastatură înaintea preîncărcării sistemului pe tablete	Utilizând o metodă de autentificare care necesită introducerea de date într-un mediu pre-bootare (înaintea încărcării sistemului), chiar dacă platforma nu acceptă introducerea înaintea încărcării sistemului (de exemplu, tastaturile de pe ecranul tactil al tabletelor). Ecranul tactil al computerelor tabletă nu este disponibil în mediul preboot. Pentru a finaliza autentificarea BitLocker pe computerele tabletă, utilizatorul trebuie să conecteze o tastatură USB, de exemplu. Dacă această casetă de selectare este bifată, este permisă utilizarea autentificării ce solicită intrarea de la tastatură înaintea încărcării sistemului. Recomandăm utilizarea acestei setări numai pentru dispozitivele care prezintă instrumente alternative pentru introducerea datelor înaintea încărcării sistemului, de exemplu o tastatură USB, în plus față de tastaturile de pe ecranul tactil. În cazul în care caseta de selectare este debifată, BitLocker Drive Encryption nu este posibilă pe tablete.
Utilizează criptare hardware (Windows 8 și versiunile ulterioare)	Dacă această casetă de selectare este bifată, aplicația folosește criptarea hardware. Acest lucru îți permite să crești viteza criptării și să folosești mai puțin resurse ale computerului.
Criptează doar spațiul de disc utilizat (Windows 8 și versiuni ulterioare)	Această casetă de selectare activează/dezactivează opțiunea care limitează zona de criptare la sectoarele ocupate de pe unitatea de hard disk. Această limită îți permite reducerea timpului necesar pentru criptare. Activarea sau dezactivarea caracteristicii **Criptează doar spațiu de disc utilizat (reduce durata criptării)** după pornirea criptării nu modifică această setare până când unitățile de hard disk nu sunt decriptate. Trebuie să bifezi sau să debifezi această casetă de selectare înainte de a începe criptarea. Dacă această casetă de selectare este bifată, sunt criptate numai poțiunile de pe unitatea de hard disk care sunt ocupate de fișiere. Kaspersky Endpoint Security criptează automat datele noi atunci când sunt adăugate. Dacă această casetă de selectare este debifată, va fi criptată întreaga unitate de hard disk, inclusiv fragmentele reziduale din fișiere șterse și modificate anterior. Această opțiune este recomandată pentru unități de hard disk noi, ale căror date nu au fost modificate sau șterse. Dacă aplici criptarea unei unități de hard disk aflate deja în uz, se recomandă să criptezi întreaga unitate de hard disk. Aceasta asigură protecția pentru toate datele, chiar și pentru datele șterse care pot fi eventual recuperate. În mod implicit, caseta de selectare este debifată.

Parametru	Descriere
Metoda de atentificare	**Doar parola (Windows 8 și versiunile ulterioare)** Dacă această opțiune este selectată, Kaspersky Endpoint Security solicită utilizatorului o parolă atunci când acesta încearcă să acceseze o unitate criptată. Această opțiune poate fi selectată atunci când nu este folosit un Trusted Platform Module (TPM). **Trusted Platform Module (TPM)** Dacă această opțiune este selectată, BitLocker folosește un Trusted Platform Module. Un *Trusted Platform Module* (TPM) este un microcip dezvoltat pentru a furniza funcții de bază legate de securitate (de exemplu, pentru stocarea cheilor de criptare). De obicei un Trusted Platform Module este instalat pe placa de bază a computerului și interacționează cu alte componente ale sistemului prin magistrala hardware. Pentru calculatoarele care execută Windows 7 sau Windows Server 2008 R2, este disponibilă numai criptarea folosind un modul TPM. Dacă nu este instalat un modul TPM, criptarea BitLocker nu este posibilă. Utilizarea unei parole pe aceste computere nu este acceptată. Un dispozitiv echipat cu un Trusted Platform Module poate crea chei de criptare care pot fi decriptate numai folosind dispozitivul respectiv. Un Trusted Platform Module criptează cheile de criptare folosind propria cheie de stocare pentru rădăcină. Cheia de stocare pentru rădăcină este stocată în Trusted Platform Module. Acest lucru oferă un nivel suplimentar de protecție împotriva încercărilor de compromitere a cheilor de criptare. Această acțiune este selectată în mod implicit. Poți seta o măsură suplimentară de protecție pentru acces la cheia de criptare și poți cripta cheia cu o parolă sau cu un PIN: • **Utilizează codul PIN pentru TPM**. Dacă această casetă de selectare este bifată, un utilizator poate utiliza un cod PIN pentru a obține acces la o cheie de criptare care este stocată pe un Trusted Platform Module (TPM). Dacă această casetă de selectare este debifată, utilizatorilor li se interzice utilizarea codurilor PIN. Pentru a accesa cheia de criptare, un utilizator trebuie să introducă parola. • **Trusted platform module (TPM) sau parola, dacă TPM este indisponibil**. Dacă este selectată această opțiune, utilizatorul poate folosi o parolă pentru a obține acces la cheile de criptare atunci când Trusted Platform Module (TPM) nu este disponibil. În cazul în care caseta de selectare este debifată și TPM nu este disponibil, criptarea completă a discului nu va începe. Metoda de autentificare selectată trebuie să fie configurată prin specificarea cerințelor privind parola sau codul PIN: • **Lungime minimă PIN (caractere)**. • **Lungime minimă parolă (caractere)**. • **Limitare perioada de valabilitate a parolei / PIN-ului pentru TPM (zile)**. • **Utilizează codul PIN îmbunătățit (litere și cifre)**. *Codul PIN îmbunătățit* permite utilizarea altor caractere în afară de cele numerice: litere latine majuscule și minuscule, caractere speciale și spații.
Recreați automat cheie de recuperare (zile)	Actualizează automat parola pentru a restabili accesul la o unitate protejată de BitLocker. Dacă este bifată caseta de selectare, specifică perioada de valabilitate a parolei cheii de recuperare. Acest lucru ajută la prevenirea reutilizării parolei cheii de recuperare.

Decriptarea unei unități de hard disk protejată de BitLocker

Utilizatorii pot decripta un disc folosind sistemul de operare (funcția *Dezactivare BitLocker*). După aceea, Kaspersky Endpoint Security va solicita utilizatorului să cripteze discul din nou. Kaspersky Endpoint Security vă va solicita să criptați discul, cu excepția cazului în care activați decriptarea discului în politică.

Cum se decriptează o unitate de hard disk protejată de BitLocker prin Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Criptare date → Full Disk Encryption**.
4. În lista verticală **Tehnologia de criptare**, selectează **BitLocker Drive Encryption**.

5. În lista verticală **Mod criptare**, selectează **Se decriptează toate unitățile de hard disk**.

6. Salvați-vă modificările.

Cum se decriptează o unitate de hard disk criptată cu BitLocker prin Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.
   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

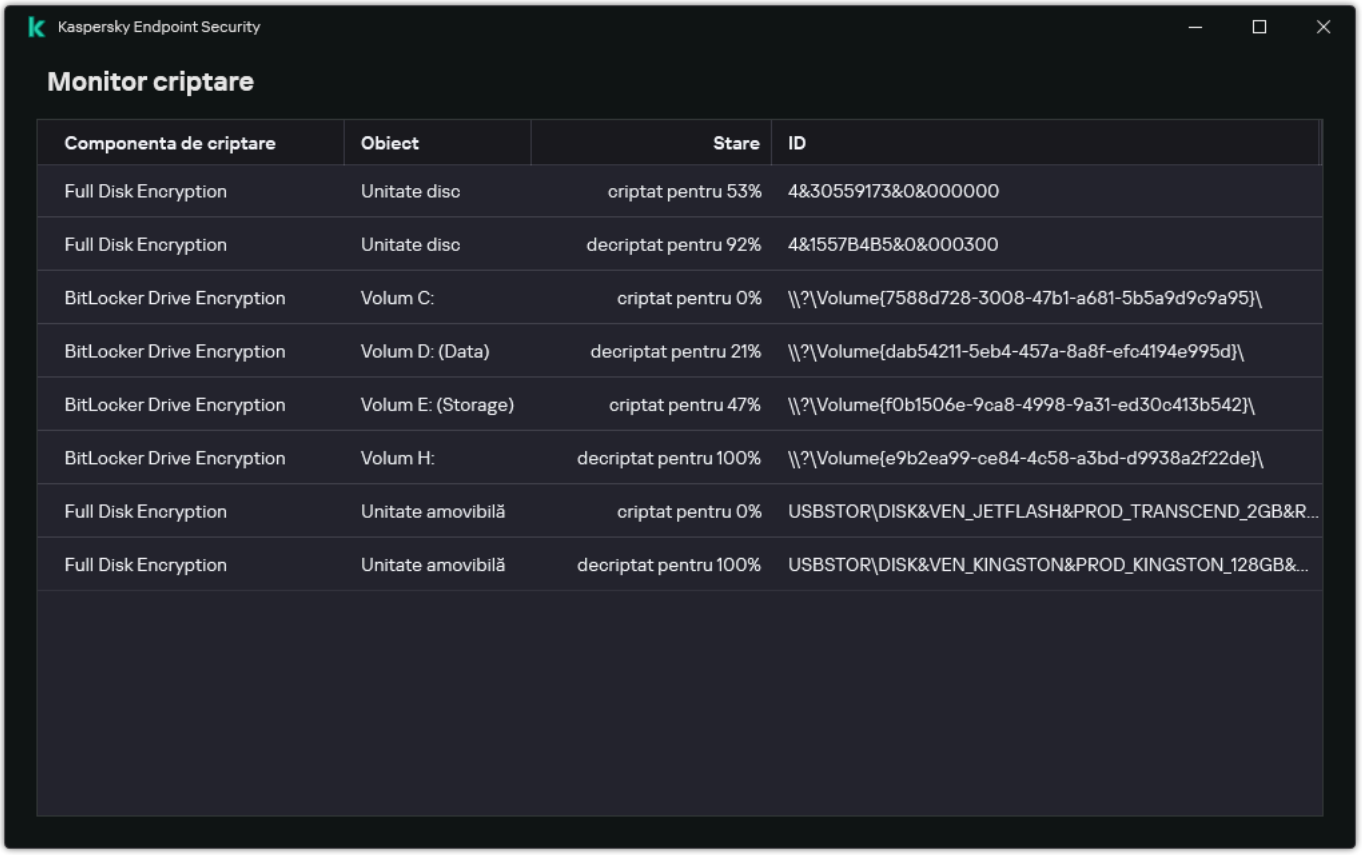
4. Accesați **Data Encryption** → **Full Disk Encryption**.

5. Selectează tehnologia **BitLocker Disk Encryption**.

6. În secțiunea **Action on devices**, selectați **Decrypt all hard drives**.

7. Salvați-vă modificările.

Puteți utiliza instrumentul Monitor criptare pentru controla procesul de criptare sau decriptare a discului de pe computerul unui utilizator. Puteți executa instrumentul Monitor criptare din fereastra principală a aplicației.



Monitor criptare

Restaurare acces la o unitate de hard disk protejată cu BitLocker

Dacă un utilizator a uitat parola pentru accesarea unei unități de hard disk criptată cu BitLocker, trebuie să începeți procedura de recuperare (Solicitare-Răspuns).

Dacă sistemul de operare al computerului are modul de compatibilitate cu standardul Federal Information Processing (FIPS), atunci în Windows 8 și versiunile anterioare fișierul cu cheia de recuperare este salvat pe unitatea amovibilă înainte de criptare. Pentru a restabili accesul la unitate, introduceți unitatea amovibilă și urmați instrucțiunile de pe ecran.

Restaurarea accesului la o unitate de hard disk criptată cu BitLocker constă în următorii pași:

1. Utilizatorul îi spune administratorului ID-ul cheii de recuperare (consultați figura de mai jos).
2. Administratorul verifică ID-ul cheii de recuperare din proprietățile computerului în Kaspersky Security Center. ID-ul furnizat de utilizator trebuie să se potrivească cu ID-ul afișat în proprietățile computerului.
3. Dacă ID-urile cheii de recuperare se potrivesc, administratorul îi oferă utilizatorului cheia de recuperare sau îi trimite un fișier cheie de recuperare.

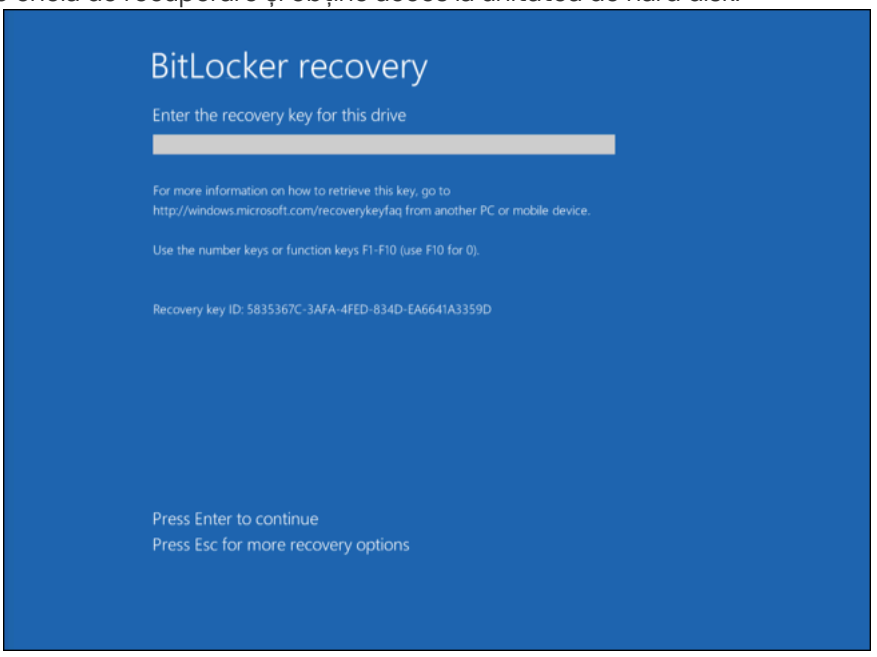
   Un fișier cheie de recuperare este utilizat pentru computerele care execută următoarele sisteme de operare:

   - Windows 7;
   - Windows 8;
   - Windows Server 2008;
   - Windows Server 2011;
   - Windows Server 2012;

   Pentru toate celelalte sisteme de operare, se folosește o cheie de recuperare.

   Pentru a preveni reutilizarea parolei cheii de recuperare, poți configura actualizarea automată a parolei în setările politicii.

4. Utilizatorul introduce cheia de recuperare și obține acces la unitatea de hard disk.



Restaurare acces la o unitate de hard disk criptată cu BitLocker

Restaurarea accesului la o unitate de sistem

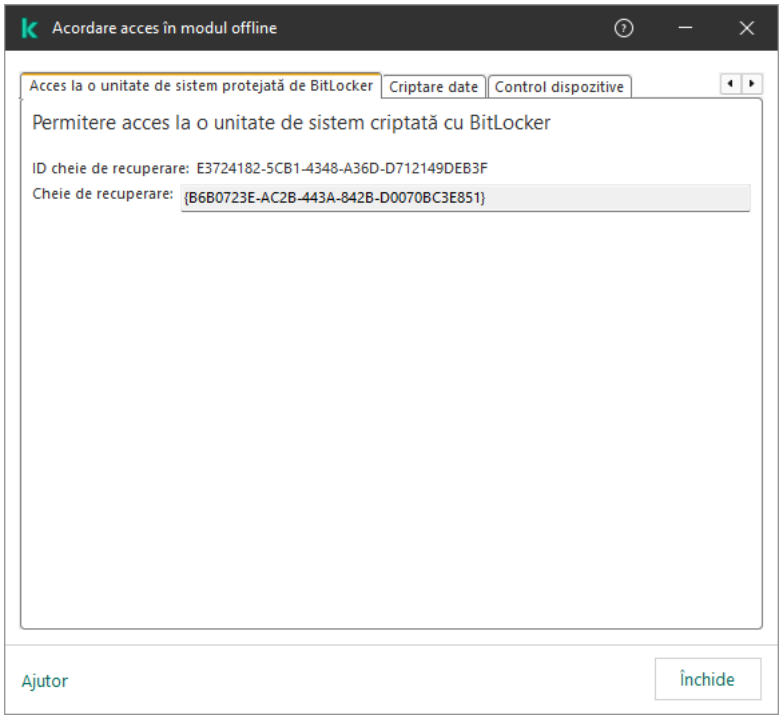
Pentru a începe procedura de recuperare, utilizatorul trebuie să apese tasta **Esc** în faza de autentificare preîncărcare.

Cum se vizualizează cheia de recuperare pentru o unitate de sistem criptată cu BitLocker în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați **Managed devices**.
3. În fila **Devices**, selectați computerul utilizatorului care solicită accesul la datele criptate și faceți clic dreapta pe el pentru a deschide meniul contextual.
4. În meniul contextual, selectați **Acordare acces în modul offline**.
5. Se deschide o fereastră; în acea fereastră, selectați fila **Acces la o unitate de sistem protejată de BitLocker**.
6. Solicită utilizatorului ID-ul cheii de recuperare, indicat în fereastra de introducere a parolei BitLocker, și compară-l cu ID-ul din câmpul **ID cheie de recuperare**.

   Dacă ID-urile nu corespund, această cheie nu este validă pentru restaurarea accesului la unitatea de sistem specificată. Asigură-te că numele computerului selectat corespunde cu numele computerului utilizatorului.

Drept urmare, veți avea acces la cheia de recuperare sau la fișierul cheii de recuperare, care va trebui transferat de utilizator.



Restaurarea accesului la o unitate criptată cu BitLocker

Cum se vizualizează cheia de recuperare pentru o unitate de sistem criptată cu BitLocker în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Assets (Devices)**.
2. Bifați caseta de selectare de lângă numele computerului la a cărui unitate doriți să restaurați accesul.
3. Fă clic pe **Grant access to the device in offline mode**.
4. În fereastra care se deschide, selectați secțiunea **BitLocker**.
5. Verificați Id-ul cheii de recuperare. ID-ul furnizat de utilizator trebuie să se potrivească cu ID-ul afișat în setările computerului.

   Dacă ID-urile nu corespund, această cheie nu este validă pentru restaurarea accesului la unitatea de sistem specificată. Asigură-te că numele computerului selectat corespunde cu numele computerului utilizatorului.

6. Fă clic pe **Receive key**.

Drept urmare, veți avea acces la cheia de recuperare sau la fișierul cheii de recuperare, care va trebui transferat de utilizator.

După încărcarea sistemului de operare, Kaspersky Endpoint Security îi solicită utilizatorului să schimbe parola sau codul PIN. După ce ai setat o parolă sau un cod PIN nou, BitLocker va crea o nouă cheie de recuperare și va trimite cheia către Kaspersky Security Center. Ca urmare, cheia de recuperare și fișierul cheie de recuperare vor fi actualizate. Dacă utilizatorul nu a schimbat parola, puteți utiliza cheia de recuperare veche data viitoare când se încarcă sistemul de operare.

Computerele care rulează Windows 7 nu permit schimbarea parolei sau a codului PIN. După introducerea cheii de recuperare și încărcarea sistemului, Kaspersky Endpoint Security nu îi solicită utilizatorului să schimbe parola sau codul PIN. Astfel, este imposibil să setați o nouă parolă sau un cod PIN. Această problemă apare din cauza particularităților sistemului de operare. Pentru a continua, trebuie să criptați din nou unitatea de disc.

Restaurarea accesului la o unitate care nu aparține sistemului

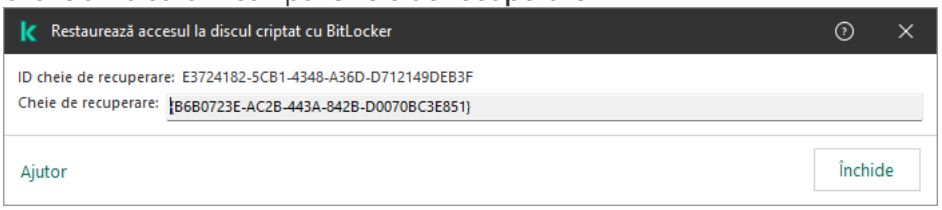
Pentru a începe procedura de recuperare, utilizatorul trebuie să facă clic pe butonul **Ți-ai uitat parola** din fereastra care asigură acces la unitate. După obținerea accesului la unitatea criptată, utilizatorul poate activa automat deblocarea unității în timpul autentificării Windows în setările BitLocker.

Cum se vizualizează cheia de recuperare pentru o unitate care nu aparține sistemului și este criptată cu BitLocker în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele Consolă de administrare, selectează directorul **Advanced** → **Data encryption and protection** → **Encrypted drives**.
3. În spațiul de lucru, selectați dispozitivul criptat pentru care doriți să creați un fișier cheie de acces și, în meniul contextual al dispozitivului, faceți clic pe **Obținere acces la dispozitiv în Kaspersky Endpoint Security**.
4. Solicită utilizatorului ID-ul cheii de recuperare, indicat în fereastra de introducere a parolei BitLocker, și compară-l cu ID-ul din câmpul **ID cheie de recuperare**.

   Dacă ID-urile nu corespund, această cheie nu este validă pentru restaurarea accesului la unitatea specificată. Asigură-te că numele computerului selectat corespunde cu numele computerului utilizatorului.

5. Trimite utilizatorului cheia indicată în câmpul **Cheie de recuperare**.



Restaurarea accesului la o unitate criptată cu BitLocker

Cum se vizualizează cheia de recuperare pentru o unitate care nu este de sistem criptată cu BitLocker în Web Console

1. În fereastra principală a componentei Web Console, selectați **Operations** → **Data encryption and protection** → **Encrypted drives**.
2. Bifați caseta de selectare de lângă numele computerului la a cărui unitate doriți să restaurați accesul.

3. Fă clic pe **Grant access to the device in offline mode**.

   Astfel, Expertul este pornit pentru permiterea accesului la un dispozitiv.

4. Urmați instrucțiunile din Expert pentru permiterea accesului la un dispozitiv:

   a. Selectează plug-in-ul **Kaspersky Endpoint Security for Windows**

   b. Verificați Id-ul cheii de recuperare. ID-ul furnizat de utilizator trebuie să se potrivească cu ID-ul afișat în setările computerului.

      > Dacă ID-urile nu corespund, această cheie nu este validă pentru restaurarea accesului la unitatea de sistem specificată. Asigură-te că numele computerului selectat corespunde cu numele computerului utilizatorului.

   c. Fă clic pe **Receive key**.

Drept urmare, veți avea acces la cheia de recuperare sau la fișierul cheii de recuperare, care va trebui transferat de utilizator.

Punerea în pauză a protecției BitLocker pentru actualizarea software-ului

Există o serie de considerații speciale pentru actualizarea sistemului de operare, instalarea pachetelor de actualizare pentru sistemul de operare sau actualizarea altor software-uri cu protecția BitLocker activată. Instalarea actualizărilor poate necesita repornirea computerului de mai multe ori. După fiecare repornire, utilizatorul trebuie să efectueze autentificarea BitLocker. Pentru a vă asigura că actualizările se instalează corect, puteți dezactiva temporar autentificarea BitLocker. În acest caz, discul rămâne criptat și utilizatorul are acces la date după ce se conectează la sistem. Pentru a gestiona autentificarea BitLocker, puteți utiliza activitatea *Gestionare protecție BitLocker*. Puteți utiliza această activitate pentru a specifica numărul de reporniri ale computerului care nu necesită autentificare BitLocker. În acest fel, după instalarea actualizărilor și finalizarea activității *Gestionare protecție BitLocker*, autentificarea BitLocker este activată automat. Puteți activa autentificarea BitLocker în orice moment.

Cum se pune în pauză protecția BitLocker utilizând Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **New task**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Selectarea tipului activității

Selectați **Kaspersky Endpoint Security for Windows (14.1)** → **Gestionare protecție BitLocker**.

Pasul 2. Gestionarea protecției BitLocker

Configurați autentificarea BitLocker. Pentru a pune în pauză protecția BitLocker, selectați **Permiteți omiterea temporară a autentificării BitLocker** și introduceți numărul de reporniri fără autentificare BitLocker (de 1 până la 15 ori). Dacă este necesar, introduceți o dată și o oră de expirare pentru activitate. La ora specificată, activitatea este dezactivată automat, iar utilizatorul trebuie să efectueze autentificarea BitLocker la repornirea computerului.

Pasul 3. Selectarea dispozitivelor cărora le va fi atribuită activitatea

Selectați computerele pe care se va efectua activitatea. Sunt disponibile următoarele opțiuni:

- Atribuirea activității unui grup de administrare. În acest caz, activitatea este atribuită computerelor incluse într-un grup de administrare creat anterior.
- Selectare computere detectate în rețea de Serverul de administrare: *dispozitive neatribuite*. Dispozitivele specifice pot include dispozitive din grupuri de administrare, precum și dispozitive neatribuite.
- Specificarea manuală a adreselor computerelor sau importarea adreselor dintr-o listă. Poți specifica nume NetBIOS, adrese IP și subrețele IP ale dispozitivelor cărora dorești să le atribui activitatea.

Pasul 4. Definirea numelui activității

Introduceți numele activității, de exemplu *Actualizare la Windows 10*.

Pasul 5. Finalizarea creării activității

Ieșiți din Expert. Dacă este necesar, bifați caseta de selectare **Run the task after the wizard finishes**. Puteți monitoriza progresul activității în proprietățile activității.

Cum se pune în pauză protecția BitLocker utilizând Web Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **Add**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Configurarea setările generale ale activității

Configurați setările generale pentru activitate:

1. În lista verticală **Application**, selectează **Kaspersky Endpoint Security**.
2. În lista verticală **Task type**, selectează **BitLocker Protection Management**.
3. În câmpul **Task name**, introduceți o descriere succintă, de exemplu *Actualizare la Windows 10*.
4. În blocul **Devices to which the task will be assigned**, selectați domeniul activității.

Pasul 2. Gestionarea protecției BitLocker

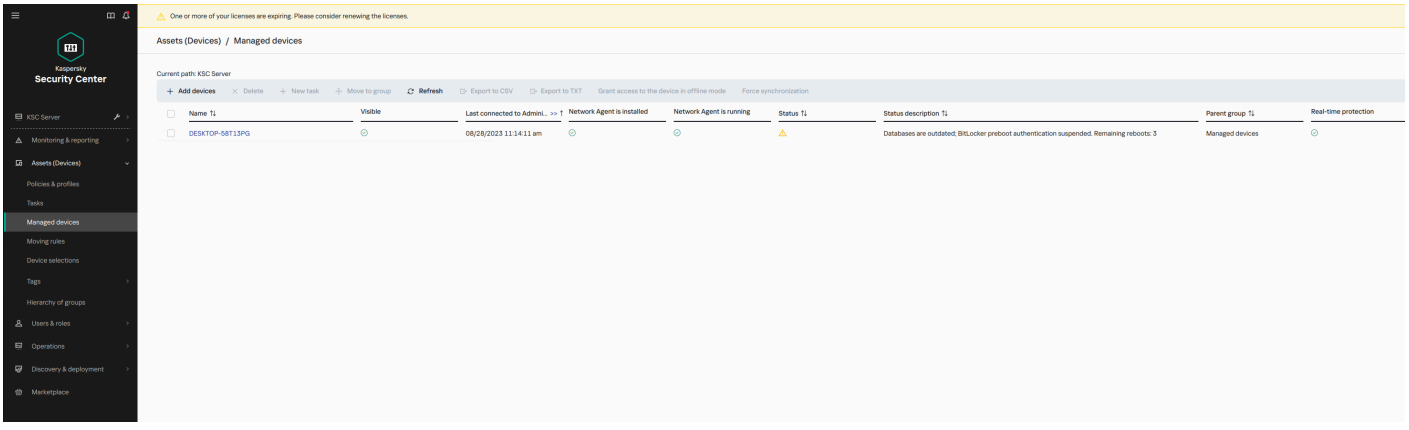
Configurați autentificarea BitLocker. Pentru a pune în pauză protecția BitLocker, selectați **Temporarily allow skipping BitLocker authentication** și introduceți numărul de reporniri fără autentificare BitLocker (de 1 până la 15 ori). Dacă este necesar, introduceți o dată și o oră de expirare pentru activitate. La ora specificată, activitatea este dezactivată automat, iar utilizatorul trebuie să efectueze autentificarea BitLocker la repornirea computerului.

Pasul 3. Finalizarea creării activității

Ieșiți din Expert. Se va afișa o activitate nouă în lista de activități.

Pentru a executa o activitate, bifează caseta de selectare de lângă activitate și fă clic pe butonul **Start**.

Ca rezultat, atunci când activitatea se execută, după următoarea repornire a computerului, BitLocker nu solicită utilizatorului autentificarea. După fiecare repornire a computerului fără autentificare BitLocker, Kaspersky Endpoint Security generează un eveniment corespunzător și înregistrează numărul de reporniri rămase. Kaspersky Endpoint Security trimite apoi evenimentul către Kaspersky Security Center pentru a fi monitorizat de administrator. De asemenea, puteți vizualiza numărul de reporniri rămase în directorul **Managed devices** al consolei Kaspersky Security Center din descrierea stării dispozitivului.



Lista dispozitivelor gestionate

Când se atinge numărul specificat de reporniri sau timpul de expirare al sarcinii, autentificarea BitLocker este activată automat. Pentru a avea acces la date, utilizatorul trebuie să efectueze autentificarea BitLocker.

Pe computerele pe care se execută Windows 7, BitLocker nu poate contoriza repornirile computerului. Contorizarea repornirilor pe computerele cu Windows 7 este gestionată de Kaspersky Endpoint Security. Astfel, pentru a activa automat autentificarea BitLocker după fiecare repornire, trebuie pornit Kaspersky Endpoint Security.

Pentru a activa autentificarea BitLocker din timp, deschideți proprietățile activității *Gestionare protecție BitLocker* și selectați opțiunea **Solicitați autentificarea de fiecare dată la pre-pornire**.

File Level Encryption pe unitățile locale ale computerului

Criptarea fișierelor nu este acceptată pe computerele bazate pe arhitectura Arm.

Această componentă este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Windows pentru stații de lucru. Această componentă nu este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Windows pentru servere.

Criptarea fișierelor are următoarele caracteristici speciale:

- Kaspersky Endpoint Security criptează/decriptează fișiere din directoare predefinite numai pentru profiluri de utilizatori locali de pe sistemul de operare. Kaspersky Endpoint Security nu criptează sau decriptează fișierele din directoarele predefinite ale profilurilor de utilizator în roaming, profilurilor de utilizator obligatorii, profilurilor de utilizator temporare sau directoarele redirecționate.

- Kaspersky Endpoint Security nu criptează fișiere a căror modificare ar putea afecta sistemul de operare și aplicațiile instalate. De exemplu, următoarele fișiere și directoare și toate directoarele imbricate se regăsesc pe lista de excluderi de la criptare:

  - %WINDIR%;

  - %PROGRAMFILES% și %PROGRAMFILES(X86)%;

  - Fișiere Windows registry.

  Lista de excluderi de la criptare nu poate fi vizualizată sau editată. Chiar dacă se pot adăuga în lista de criptare fișiere și directoare aflate în lista de excluderi de la criptare, acestea nu vor fi criptate în timpul activității de criptare a fișierelor.

Criptarea fișierelor de pe unitățile locale ale computerului

Kaspersky Endpoint Security nu criptează fișierele care se află în spațiul de stocare în cloud OneDrive sau în alte directoare care se numesc OneDrive. Kaspersky Endpoint Security blochează, de asemenea, copierea fișierelor criptate în directoarele OneDrive dacă acele fișiere nu sunt adăugate la regula de decriptare.

Pentru a cripta fișiere de pe unitățile locale:

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Data Encryption** → **File Level Encryption**.
4. În lista verticală **Mod criptare**, selectează **În conformitate cu regulile**.
5. În fila **Criptare**, faceți clic pe butonul **Adaugă** și, în lista verticală, selectați unul dintre elementele următoare:
   a. Selectați elementul **Directoare predefinite** pentru a adăuga la o regulă de criptare fișiere din directoare din profilurile utilizatorului local sugerate de experții Kaspersky.
      - **Documente**. Fișiere din directorul standard *Documente* al sistemului de operare și subdirectoarele sale.
      - **Favorite**. Fișiere din directorul standard *Favorite* al sistemului de operare și subdirectoarele sale.
      - **Desktop**. Fișiere din directorul standard *Desktop* al sistemului de operare și subdirectoarele sale.
      - **Fișiere temporare**. Fișiere temporare legate de funcționarea aplicațiilor instalate pe computer. De exemplu, aplicațiile Microsoft Office creează fișiere temporare care conțin copii de rezervă ale documentelor.

        Nu este recomandat să criptați fișierele temporare, deoarece acest lucru poate provoca pierderi de date. De exemplu, Microsoft Word creează fișiere temporare atunci când procesează un document. Dacă fișierele temporare sunt criptate, dar fișierul original nu este, utilizatorul poate primi o eroare *Acces refuzat* când încercați să salvați documentul. În plus, Microsoft Word ar putea salva fișierul, dar nu va fi posibil să deschideți documentul data viitoare, adică datele se vor pierde.

      - **Fișiere Outlook**. Fișiere legate de funcționarea clientului de e-mail Outlook: fișiere de date (PST), fișiere de date offline (OST), fișiere offline address book (OAB) și fișiere personal address book (PAB).

   b. Selectați elementul **Director personalizat** pentru a adăuga o cale de director introdusă manual la o regulă de criptare.

      Când adăugați o cale către director, respectați următoarele reguli:

      - Utilizați o variabilă de mediu (de exemplu, `%FOLDER%\UserFolder\`). Puteți utiliza o variabilă de mediu o singură dată și numai la începutul căii.
      - Nu folosiți căi relative.

- Nu folosiți caracterele `*` și `?`.
- Nu folosiți căi UNC.
- Utilizați `;` sau `,` drept caracter separator.

c. Selectați elementul **Fișiere după extensie** pentru a adăuga extensii individuale de fișier la o regulă de criptare. Kaspersky Endpoint Security criptează fișierele cu extensiile specificate de pe toate unitățile locale ale computerului.

d. Selectați elementul **Fișiere după grupuri de extensii** pentru a adăuga grupuri de extensii de fișiere la o regulă de criptare (de exemplu, *Documente Microsoft Office*). Kaspersky Endpoint Security criptează fișierele care au extensiile listate în grupurile de extensii de pe toate unitățile locale ale computerului.

6. Salvați-vă modificările.

Imediat după aplicarea politicii, Kaspersky Endpoint Security criptează fișierele care sunt incluse în regula de criptare și care nu sunt incluse în regula de decriptare.

Criptarea fișierelor are următoarele caracteristici speciale:

- Dacă se adaugă același fișier atât la o regulă de criptare, cât și la o regulă de decriptare, atunci Kaspersky Endpoint Security efectuează următoarele acțiuni:
  - Dacă fișierul nu este criptat, Kaspersky Endpoint Security nu criptează acest fișier.
  - Dacă fișierul este criptat, Kaspersky Endpoint Security decriptează acest fișier.
- Kaspersky Endpoint Security continuă să cripteze noi fișiere dacă aceste fișiere îndeplinesc criteriile regulii de criptare. De exemplu, atunci când modificați proprietățile unui fișier necriptat (calea sau extensia), fișierul respectă apoi criteriile regulii de criptare. Kaspersky Endpoint Security criptează acest fișier.
- Atunci când utilizatorul creează un fișier nou ale cărui proprietăți îndeplinesc criteriile regulii de criptare, Kaspersky Endpoint Security criptează fișierul imediat ce acesta este deschis.
- Kaspersky Endpoint Security amână criptarea fișierelor deschise până când acestea sunt închise.
- Dacă muți un fișier criptat într-un alt director de pe unitatea locală, fișierul rămâne criptat indiferent dacă acest director este inclus sau nu în regula de criptare.
- Dacă decriptați un fișier și îl copiați în alt director local care nu este inclus în regula de decriptare, o copie a fișierului poate fi criptată. Pentru a împiedica fișierul copiat să fie criptat, creați o regulă de decriptare pentru directorul țintă.

Crearea regulilor de acces la fișiere criptate pentru aplicații

În mod implicit, toate aplicațiile funcționează cu fișiere criptate într-o stare decriptată. Dacă utilizezi des anumite aplicații (de exemplu, browsere sau editoare de text), poți crea reguli de acces la fișiere criptate pentru a proteja informațiile.

Îți recomandăm să creezi o regulă de acces la fișiere criptate pentru browserele Microsoft Internet Explorer și Microsoft Edge. Datorită modului în care funcționează aceste browsere, dacă încarci un fișier criptat pe un site web (de exemplu, în spațiul de stocare în cloud), fișierul este decriptat automat. Acest lucru poate provoca o scurgere de date. Nu este posibil să încarci un fișier criptat folosind aceste browsere. Îți recomandăm să configurezi regula **Acordare acces la fișiere criptate numai sub formă de text cifrat**. Nu trebuie să creezi o regulă pentru alte browsere (cum ar fi Google Chrome).

Pentru a crea reguli de acces la fișiere criptate pentru aplicații:

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Data Encryption → File Level Encryption**.
4. În lista verticală **Mod criptare**, selectează **În conformitate cu regulile**.

   Regulile de acces sunt aplicate doar în modul **În conformitate cu regulile**. După aplicarea regulilor de acces în modul **În conformitate cu regulile**, dacă treceți la modul **Lasă nemodificat**, Kaspersky Endpoint Security va ignora toate regulile de acces. Toate aplicațiilor vor avea acces la toate fișierele criptate.

5. În partea dreaptă a ferestrei, selectați fila **Reguli pentru aplicații**.
6. Dacă dorești să selectezi aplicații exclusiv din lista Kaspersky Security Center, apasă pe butonul **Adaugă** și, în lista verticală, selectați elementul **Aplicații din lista Kaspersky Security Center**.
   a. Specifică filtrele pentru a restrânge lista de aplicații din tabel. Pentru aceasta, specifică valorile pentru parametrii **Aplicație**, **Vânzător** și **Perioadă adăugată** și toate casetele de selectare din secțiunea **Grup**.
   b. Fă clic pe **Împrospătează**.
   c. Tabelul listează aplicații care corespund filtrelor aplicate.
   d. În coloana **Aplicație**, bifați casetele de selectare de lângă aplicațiile pentru care dorești să creezi reguli de acces la fișiere criptate.
   e. În lista verticală **Regulă pentru aplicații**, selectați regula care va determina accesul aplicațiilor la fișiere criptate.
   f. În lista verticală **Acțiuni pentru aplicațiile selectate anterior**, selectați acțiunea care trebuie efectuată de Kaspersky Endpoint Security pentru regulile de acces la fișiere criptate create anterior pentru aceste aplicații.

Detaliile unei reguli de acces la fișiere criptate pentru aplicații apar în tabelul din fila **Reguli pentru aplicații**.

7. Dacă dorești să selectezi manual aplicații, faceți clic pe butonul **Adaugă** și, în lista verticală, selectați elementul **Aplicații personalizate**.

   a. În câmpul de introducere, tastează numele sau lista de nume de fișiere executabile ale aplicațiilor, inclusiv extensiile lor.

      Mai poți adăuga numele fișierelor executabile ale aplicațiilor din lista Kaspersky Security Center făcând clic pe butonul **Adaugă din lista Kaspersky Security Center**.

   b. Dacă este necesar, în câmpul **Descriere**, introdu o descriere a listei de aplicații.

   c. În lista verticală **Regulă pentru aplicații**, selectați regula care va determina accesul aplicațiilor la fișiere criptate.

   Detaliile unei reguli de acces la fișiere criptate pentru aplicații apar în tabelul din fila **Reguli pentru aplicații**.

8. Salvați-vă modificările.

Criptarea fișierelor create sau modificate de aplicații specifice

Poți crea o regulă prin care Kaspersky Endpoint Security va cripta toate fișierele create sau modificate de către aplicațiile specificate în regulă.

> Fișierele care au fost create sau modificate de către aplicațiile specificate înainte de aplicarea regulii de criptare nu vor fi criptate.

Pentru a configura criptarea fișierelor create sau modificate de aplicații specifice:

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Data Encryption → File Level Encryption**.
4. În lista verticală **Mod criptare**, selectează **În conformitate cu regulile**.

   > Regulile de criptare sunt aplicate doar în modul **În conformitate cu regulile**. După aplicarea regulilor de criptare în modul **În conformitate cu regulile**, dacă treceți la modul **Lasă nemodificat**, Kaspersky Endpoint Security va ignora toate regulile de criptare. Fișierele criptate anterior vor rămâne criptate.

5. În partea dreaptă a ferestrei, selectați fila **Reguli pentru aplicații**.
6. Dacă dorești să selectezi aplicații exclusiv din lista Kaspersky Security Center, apasă pe butonul **Adaugă** și, în lista verticală, selectați elementul **Aplicații din lista Kaspersky Security Center**.

   a. Specifică filtrele pentru a restrânge lista de aplicații din tabel. Pentru aceasta, specifică valorile pentru parametrii **Aplicație**, **Vânzător** și **Perioadă adăugată** și toate casetele de selectare din secțiunea **Grup**.

   b. Fă clic pe **Împrospătează**.

      Tabelul listează aplicații care corespund filtrelor aplicate.

c. În coloana **Aplicație**, bifați casetele de selectare de lângă aplicațiile ale căror fișiere create doriți să le criptați.

d. În lista verticală **Regulă pentru aplicații**, selectează **Criptează toate fișierele create**.

e. În lista verticală **Acțiuni pentru aplicațiile selectate anterior**, selectați acțiunea care va fi efectuată de Kaspersky Endpoint Security pentru regulile de criptare fișiere care au fost formate anterior pentru aceste aplicații.

Informațiile despre regula de criptare pentru fișierele create sau modificate de aplicațiile selectate sunt afișate în tabelul din fila **Reguli pentru aplicații**.

7. Dacă dorești să selectezi manual aplicații, faceți clic pe butonul **Adaugă** și, în lista verticală, selectați elementul **Aplicații personalizate**.

a. În câmpul de introducere, tastează numele sau lista de nume de fișiere executabile ale aplicațiilor, inclusiv extensiile lor.

Mai poți adăuga numele fișierelor executabile ale aplicațiilor din lista Kaspersky Security Center făcând clic pe butonul **Adaugă din lista Kaspersky Security Center**.

b. Dacă este necesar, în câmpul **Descriere**, introdu o descriere a listei de aplicații.

c. În lista verticală **Regulă pentru aplicații**, selectează **Criptează toate fișierele create**.

Informațiile despre regula de criptare pentru fișierele create sau modificate de aplicațiile selectate sunt afișate în tabelul din fila **Reguli pentru aplicații**.

8. Salvați-vă modificările.

Generarea unei reguli de decriptare

Pentru a genera o regulă de decriptare:

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.

2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

3. În fereastra politicii, selectați **Data Encryption → File Level Encryption**.

4. În lista verticală **Mod criptare**, selectează **În conformitate cu regulile**.

5. În fila **Decriptare**, faceți clic pe butonul **Adaugă** și, în lista verticală, selectați unul dintre elementele următoare:

a. Selectați elementul **Directoare predefinite** pentru a adăuga la o regulă de decriptare fișiere din directoare din profilurile utilizatorului local sugerate de experții Kaspersky.

b. Selectați elementul **Director personalizat** pentru a adăuga o cale de director introdusă manual la o regulă de decriptare.

c. Selectați elementul **Fișiere după extensie** pentru a adăuga extensii individuale de fișier la o regulă de decriptare. Kaspersky Endpoint Security nu criptează fișierele cu extensiile specificate de pe toate unitățile locale ale computerului.

d. Selectați elementul **Fișiere după grupuri de extensii** pentru a adăuga grupuri de extensii de fișiere la o regulă de decriptare (de exemplu, *Documente Microsoft Office*). Kaspersky Endpoint Security nu criptează fișierele care au extensiile listate în grupurile de extensii de pe toate unitățile locale ale computerului.

6. Salvați-vă modificările.

Dacă același fișier este adăugat a regula de criptare și al regula de decriptare, Kaspersky Endpoint Security nu criptează acest fișier dacă nu este criptat și îl decriptează dacă este criptat.

Decriptarea fișierelor de pe unitățile locale ale computerului

Pentru a decripta fișiere de pe unitățile locale:

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Data Encryption** → **File Level Encryption**.
4. În partea dreaptă a ferestrei, selectați fila **Criptare**.
5. Elimină fișierele și directoarele pe care dorești să le decriptezi din lista de criptare. Pentru aceasta, selectați fișierele și apoi selectați elementul **Ștergere regulă și decriptare fișiere** în meniul contextual al butonului **Șterge**.

   Fișierele și directoarele eliminate din lista de criptare sunt adăugate în mod automat în lista de decriptare.
6. Form a file decryption list.
7. Salvați-vă modificările.

Imediat ce politica este aplicată, Kaspersky Endpoint Security decriptează fișierele criptate care sunt adăugate la lista de decriptare.

Kaspersky Endpoint Security decriptează fișierele criptate dacă parametrii lor (cale fișier/nume fișier/extensie fișier) se modifică și corespund parametrilor obiectelor adăugate în lista de decriptare.

Kaspersky Endpoint Security amână decriptarea fișierelor deschise până când acestea sunt închise.

Crearea pachetelor criptate

Pentru a vă proteja datele când trimiteți fișiere către utilizatori din afara rețelei corporative, puteți utiliza pachete criptate. Pachetele criptate pot fi convenabile pentru transferul fișierelor mari pe unitățile amovibile, deoarece clienții de e-mail au restricții privind dimensiunea fișierului.

Înainte de a crea pachete criptate, Kaspersky Endpoint Security va solicita utilizatorului o parolă. Pentru a proteja în mod fiabil datele, puteți activa verificarea complexității parolei și să specificați cerințele privind complexitatea parolei. Acest lucru va împiedica utilizatorii să utilizeze parole scurte și simple, de exemplu, `1234`.

Cum se activează verificarea complexității parolei la crearea arhivelor criptate în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Criptare date → Setări de criptare comune**.
4. În blocul **Setări parolă**, fă clic pe butonul **Setări**.
5. Se deschide o fereastră; în acea fereastră, selectați fila **Pachete criptate**.
6. Configurați setările de complexitate a parolei atunci când creați pachete criptate.

Cum se activează verificarea complexității parolei la crearea arhivelor criptate în Consola Web

1. În fereastra principală a Web Console, selectați **Asset management → Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.
   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Data Encryption → File Level Encryption**.
5. În blocul **Encrypted package password settings**, configurați criteriul privind complexitatea parolei solicitat la crearea pachetelor criptate.

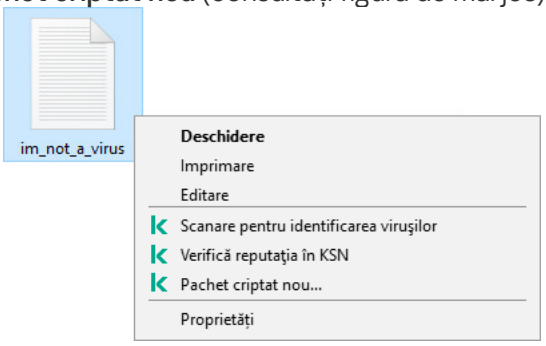
Puteți crea pachete criptate pe computere cu Kaspersky Endpoint Security instalat și pe care este disponibilă opțiunea File Level Encryption.

La adăugarea unui fișier la pachetul criptat al cărui conținut se află în spațiul de stocare în cloud OneDrive, Kaspersky Endpoint Security descarcă conținutul fișierului și execută criptarea.

Pentru a crea un pachet criptat:

1. În orice manager de fișiere, selectați fișierele sau directoarele pe care doriți să le adăugați la pachetul criptat. Faceți clic dreapta pentru a deschide meniul contextual.

2. În meniul contextual, selectați **Pachet criptat nou** (consultați figura de mai jos).



Crearea unui pachet criptat

3. În fereastra care se deschide, specificați parola și confirmați-o.

   Parola trebuie să îndeplinească criteriile de complexitate specificate în politică.

4. Fă clic pe **Creează**.

Începe procesul de creare a pachetului criptat. Kaspersky Endpoint Security nu efectuează nicio comprimare a fișierelor atunci când creează un pachet criptat. Când procesul se termină, un pachet criptat cu extragere automată protejat prin parolă (un fișier executabil cu extensia .exe -) este creat în directorul destinație selectat.

Pentru a accesa fișierele dintr-un pachet criptat, faceți dublu clic pe acesta pentru a porni Expertul de dezarhivare, apoi introduceți parola. Dacă v-ați uitat sau ați pierdut parola, nu este posibil să o recuperați și să accesați fișierele din pachetul criptat. Puteți recrea pachetul criptat.

Restaurarea accesului la fișierele criptate

Când fișierele sunt criptate, Kaspersky Endpoint Security primește o cheie de criptare necesară pentru accesarea directă a fișierelor criptate. Folosind această cheie de criptare, un utilizator care lucrează sub orice cont de utilizator Windows care era activ în cursul criptării fișierelor poate accesa direct fișierele criptate. Utilizatorii care lucrează sub conturi Windows care erau inactive în cursul criptării fișierelor trebuie să se conecteze la Kaspersky Security Center pentru a accesa fișierele criptate.

Fișierele criptate pot fi inaccesibile în următoarele situații:

- Computerul utilizatorului stochează chei de criptare, dar nu există o conexiune cu aplicația Kaspersky Security Center pentru gestionarea cheilor. În acest caz, utilizatorul trebuie să solicite accesul la fișierele criptate de la administratorul rețelei LAN.

  Dacă nu există acces la Kaspersky Security Center, trebuie să procedezi astfel:

  - Solicită o cheie de acces pentru accesul la fișiere criptate de pe unitățile de hard disk ale computerului.

  - Pentru a accesa fișiere criptate stocate pe unități amovibile, solicită chei de acces separate pentru fișierele criptate de pe fiecare unitate amovibilă.

- Componentele de criptare sunt șterse de pe computerul utilizatorului. În această situație, utilizatorul poate deschide fișiere criptate de pe discuri locale și amovibile, însă conținutul fișierelor respective va apărea criptat.

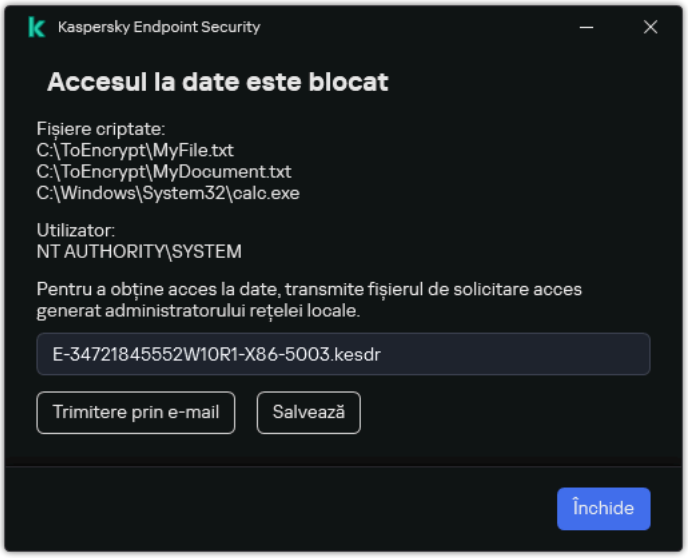
  Utilizatorul poate lucra cu fișiere criptate în următoarele situații:

  - Fișierele sunt plasate în pachete criptate create pe un computer cu aplicația Kaspersky Endpoint Security instalată.
  - Fișierele sunt stocate pe unități amovibile pe care a fost permis modul portabil.

Pentru a obține acces la fișierele criptate, utilizatorul trebuie să înceapă procedura de recuperare (Solicitare-Răspuns).

Recuperarea accesului la fișierele criptate constă în următorii pași:

1. Utilizatorul trimite administratorului un fișier de solicitare a accesului (consultați figura de mai jos).
2. Administratorul adaugă fișierul de solicitare a accesului în Kaspersky Security Center, creează un fișier cheie de acces și trimite fișierul către utilizator.
3. Utilizatorul adaugă fișierul cheie de acces la Kaspersky Endpoint Security și obține acces la fișiere.



Restaurarea accesului la fișierele criptate

Pentru a începe procedura de recuperare, utilizatorul trebuie să încerce să acceseze un fișier. Drept urmare, Kaspersky Endpoint Security va crea un fișier de solicitare a accesului (un fișier cu extensia KESDC), pe care utilizatorul trebuie să-l trimită administratorului, de exemplu, prin e-mail.

Kaspersky Endpoint Security generează un fișier de solicitare a accesului pentru accesarea tuturor fișierelor criptate stocate pe unitatea computerului (unitatea locală sau unitatea amovibilă).

Cum se obține un fișier cheie de acces la datele criptate în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați **Devices**.
3. În fila **Devices**, selectați computerul utilizatorului care solicită accesul la datele criptate și faceți clic dreapta pe el pentru a deschide meniul contextual.

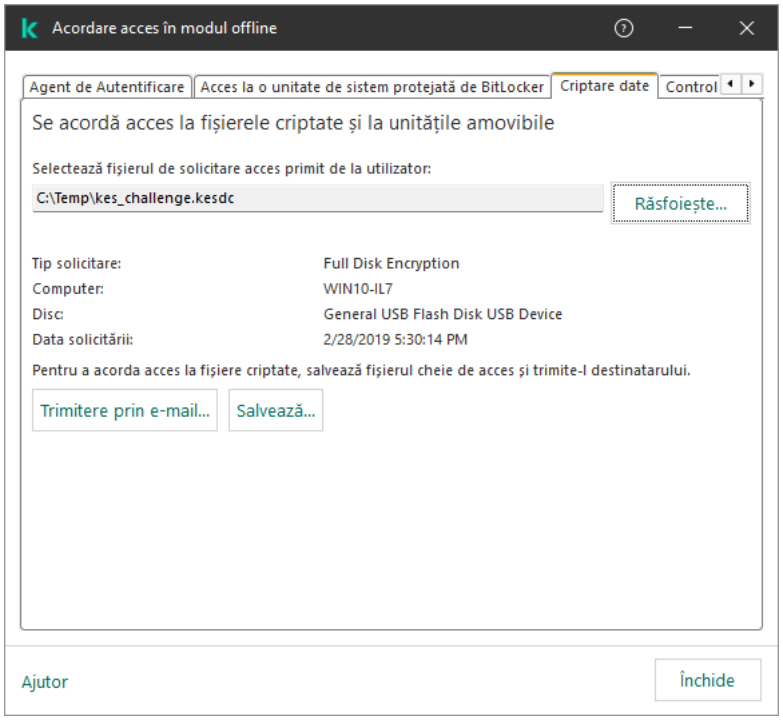
4. În meniul contextual, selectați **Acordare acces în modul offline**.

5. Se deschide o fereastră; în acea fereastră, selectați fila **Criptare date**.

6. În fila **Criptare date**, faceți clic pe butonul **Răsfoiește**.

7. În fereastra pentru selectarea unui fișier de solicitare a accesului, specificați calea către fișierul primit de la utilizator.

Veți vedea informații despre solicitarea utilizatorului. Kaspersky Security Center generează un fișier cheie. Trimiteți utilizatorului prin e-mail fișierul cheie de acces la date criptate generat. Sau salvați fișierul de acces și utilizați orice metodă disponibilă pentru a transfera fișierul.



Acordarea accesului în modul offline

Cum se obține un fișier cheie de acces la datele criptate în Web Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Assets (Devices)**.

2. Bifați caseta de selectare de lângă numele computerului la ale cărui date doriți să restaurați accesul.

3. Fă clic pe **Grant access to the device in offline mode**.

4. Selectați **Data Encryption**.

5. Faceți clic pe butonul **Select file** și selectați fișierul de solicitare a accesului pe care l-ați primit de la utilizator (un fișier cu extensia KESDC).

   Web Console va afișa informații despre solicitare. Acestea vor include numele computerului pe care utilizatorul solicită acces la fișier.

6. Faceți clic pe butonul **Save key** și selectați un director pentru a salva fișierul cheie de acces la datele criptate (un fișier cu extensia KESDR).

Drept urmare, veți putea obține cheia de acces la datele criptate, pe care va trebui să o transferați utilizatorului.

După ce a primit fișierul cu cheia de acces la datele criptate, utilizatorul trebuie să execute fișierul făcând dublu clic pe acesta. Drept urmare, Kaspersky Endpoint Security va acorda acces la toate fișierele criptate stocate pe unitate. Pentru a accesa fișierele criptate stocate pe alte unități, trebuie să obțineți un fișiercheie de acces separat pentru fiecare unitate.

Restaurarea accesului la date criptate după o eroare de sistem

Poți restabili accesul la date după o eroare de sistem numai pentru File Level Encryption (FLE). Nu poți restaura accesul la date dacă se folosește Full Disk Encryption (FDE).

Pentru a restaura accesul la date criptate după o eroare de sistem:

1. Reinstalează sistemul de operare, fără a formata unitatea de hard disk.
2. Instalează Kaspersky Endpoint Security.
3. Stabilește o conexiune între computer și Serverul de administrare Kaspersky Security Center care controla computerul atunci când au fost criptate datele.

   Accesul la datele criptate va fi acordat în aceleași condiții care erau valabile înainte de eroarea sistemului de operare.

Editarea șabloanelor de mesaje pentru acces la fișiere criptate

Pentru a edita șabloanele de mesaje pentru acces la fișiere criptate:

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Criptare date** → **Setări de criptare comune**.
4. În blocul **Șabloane**, fă clic pe butonul **Șabloane**.
5. În fereastra care se deschide, procedează după cum urmează:

   - Dacă dorești să editezi șablonul pentru mesajul utilizatorului, selectați fila **Mesajul utilizatorului**. Fereastra următoare se deschide atunci când utilizatorul încearcă să acceseze un fișier criptat când nu există pe computer nicio cheie disponibilă pentru accesul la fișierele criptate (vezi figura de mai jos). Făcând clic pe butonul **Trimitere prin e-mail**, se creează automat un mesaj de la utilizator. Acest mesaj este trimis administratorului rețelei LAN, împreună cu fișierul prin care se solicită accesul la fișiere criptate.

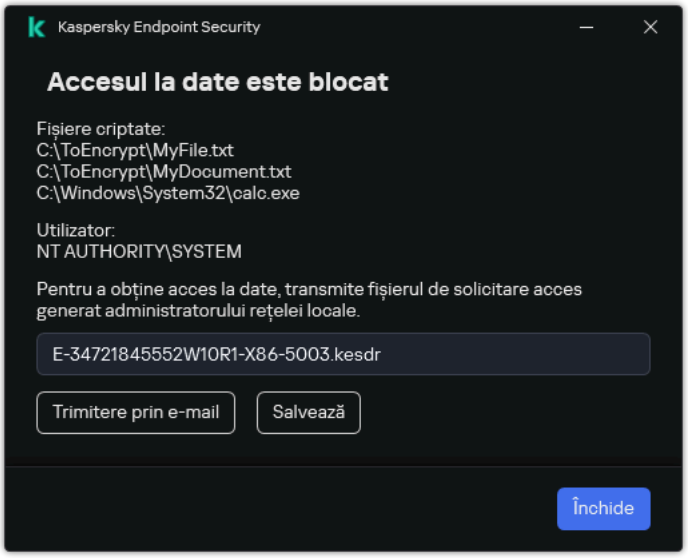
   - Dacă dorești să editezi șablonul pentru mesajul administratorului, selectați fila **Mesajul administratorului**. Utilizatorul primește acest mesaj după ce i se acordă acces la fișierele criptate.

6. Editează șabloanele de mesaje.

   Pentru a adăuga o variabilă la textul șablonului, plasează cursorul în poziția dorită, fă clic pe **Variabilă** și selectează variabila necesară din lista de opțiuni disponibile.

   De asemenea, poți restaura textul șablonului implicit utilizând butonul **În mod implicit**.

7. Salvați-vă modificările.



Restaurarea accesului la fișierele criptate

Criptare unități amovibile

Criptarea unităților amovibile nu este acceptată pe computerele bazate pe arhitectura Arm.

Această componentă este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Windows pentru stații de lucru. Această componentă nu este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Windows pentru servere.

Kaspersky Endpoint Security acceptă criptare de fișiere din sisteme de fișiere FAT32 și NTFS. Dacă o unitate amovibilă cu un sistem de fișiere neacceptat este conectată la computer, activitatea de criptare pentru această unitate amovibilă se termină cu o eroare și Kaspersky Endpoint Security atribuie unității amovibile starea numai în citire.

Pentru a proteja datele de pe unitățile amovibile, puteți utiliza următoarele tipuri de criptare:

- Full Disk Encryption (FDE).

  Criptarea întregii unități amovibile, inclusiv a sistemului de fișiere.

  Nu este posibilă accesarea datelor criptate în afara rețelei corporative. De asemenea, este imposibil să accesați date criptate din rețeaua corporativă în cazul în care computerul nu este conectat la Kaspersky Security Center (de ex. pe un computer „invitat”).

- File Level Encryption (FLE).

  Criptarea numai a fișierelor de pe o unitate amovibilă. Sistemul de fișiere rămâne neschimbat.

Criptarea fișierelor de pe unitățile amovibile oferă capacitatea de a accesa date din afara rețelei corporative folosind un mod special numit *mod portabil*.

În timpul criptării, Kaspersky Endpoint Security creează o cheie principală. Kaspersky Endpoint Security salvează cheia principală în următoarele depozite:

- Kaspersky Security Center.
- Computerul utilizatorului.

  Cheia principală este criptată cu cheia secretă a utilizatorului.
- Unitatea amovibilă.

  Cheia principală este criptată cu cheia publică a Kaspersky Security Center.

După finalizarea criptării, datele de pe unitatea amovibilă sunt accesibile în rețeaua corporativă ca și cum ați utiliza o unitate amovibilă convențională necriptată.

Accesarea datelor criptate

Când este conectată o unitate amovibilă cu date criptate, Kaspersky Endpoint Security efectuează următoarele acțiuni:

1. Verifică o cheie principală în spațiul de stocare local de pe computerul utilizatorului.

   Dacă se găsește cheia principală, utilizatorul obține acces la datele de pe unitatea amovibilă.

   Dacă nu se găsește cheia principală, Kaspersky Endpoint Security efectuează următoarele acțiuni:

   a. Trimite o solicitare către Kaspersky Security Center.

      După primirea solicitării, Kaspersky Security Center trimite un răspuns care conține cheia principală.

   b. Kaspersky Endpoint Security salvează cheia principală în stocarea locală de pe computerul utilizatorului pentru operațiunile ulterioare cu unitatea amovibilă criptată.
2. Decriptează datele.

Caracteristicile speciale ale criptării unității amovibile

Criptarea unităților amovibile are următoarele caracteristici speciale:

- Politica cu setările implicite pentru criptarea unității amovibile este concepută pentru un grup specific de computere gestionate. Prin urmare, rezultatul aplicării politicii Kaspersky Security Center configurate pentru criptarea/decriptarea unităților amovibile depinde de computerul la care este conectată unitatea amovibilă.
- Kaspersky Endpoint Security nu criptează/decriptează fișiere care au permisiunea Doar citire și care sunt stocate pe unități amovibile.

- Următoarele tipuri de dispozitive sunt acceptate ca unități amovibile:
  - Medii de date conectate prin magistrala USB
  - Unități de hard disk conectate prin magistralele USB și FireWire
  - Unități SSD conectate prin magistralele USB și FireWire

Lansarea criptării unităților amovibile

Puteți utiliza o politică pentru a decripta o unitate amovibilă. O politică cu setări definite pentru criptarea unității amovibile este generată pentru un anumit grup de administrare. Prin urmare, rezultatul decriptării datelor de pe unități amovibile depinde de computerul la care este conectată unitatea amovibilă.

Kaspersky Endpoint Security acceptă criptare de fișiere din sisteme de fișiere FAT32 și NTFS. Dacă o unitate amovibilă cu un sistem de fișiere neacceptat este conectată la computer, activitatea de criptare pentru această unitate amovibilă se termină cu o eroare și Kaspersky Endpoint Security atribuie unității amovibile starea numai în citire.

Înainte de a cripta fișierele de pe o unitate amovibilă, asigurați-vă că este formatată și că nu există partiții ascunse (cum ar fi o partiție de sistem EFI). Dacă unitatea conține partiții neformatate sau ascunse, criptarea fișierelor poate eșua cu o eroare.

Pentru a cripta unități amovibile:

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Criptare date** → **Criptare unități amovibile**.
4. În lista verticală **Mod criptare**, selectați acțiunea implicită pe care doriți ca Kaspersky Endpoint Security să o efectueze pe unitățile amovibile:
   - **Criptează unitate amovibilă în întregime** (FDE). Kaspersky Endpoint Security criptează conținutul unei unități amovibile sector cu sector. Prin urmare, aplicația criptează nu numai fișierele stocate pe unitatea amovibilă, ci și sistemele sale de fișiere, inclusiv numele fișierelor și structurile directoarelor de pe unitatea amovibilă.
   - **Criptează toate fișierele** (FLE). Kaspersky Endpoint Security criptează toate fișierele care sunt stocate pe unități amovibile. Aplicația nu criptează sistemele de fișiere ale unităților amovibile, inclusiv numele fișierelor și structurile directoarelor.
   - **Criptează numai fișiere noi** (FLE). Kaspersky Endpoint Security criptează numai acele fișiere care au fost adăugate pe unitățile amovibile sau care au fost stocate pe unitățile amovibile și au fost modificate după ce politica Kaspersky Security Center a fost aplicată ultima dată.

   Kaspersky Endpoint Security nu criptează o unitate amovibilă care este deja criptată.

5. Dacă doriți să utilizați modul portabil pentru criptarea unităților amovibile, selectați caseta de selectare **Mod portabil**.

   Portable mode este un mod de criptare a fișierelor (FLE) pe unitățile amovibile care oferă posibilitatea de a accesa date din afara unei rețele corporative. Modul portabil vă permite, de asemenea, să lucrați cu date criptate pe computere care nu au instalat Kaspersky Endpoint Security.

6. Dacă doriți să criptați o nouă unitate amovibilă, este recomandat să bifați caseta de selectare **Criptează doar spațiul de disc utilizat**. În cazul în care caseta de selectare este debifată, Kaspersky Endpoint Security va cripta toate fișierele, inclusiv fragmentele reziduale ale fișierelor șterse sau modificate.

7. Dacă doriți să configurați criptarea pentru unități amovibile individuale, definiți regulile de criptare.

8. Dacă doriți să utilizați criptarea Full Disk Encryption a unităților amovibile în modul offline, bifați caseta de selectare **Permiteți criptarea unităților amovibile în modul offline**.

   Offline encryption mode se referă la criptarea unităților amovibile (FDE) atunci când nu există nicio conexiune la Kaspersky Security Center. În timpul criptării, Kaspersky Endpoint Security salvează cheia principală doar pe computerul utilizatorului. Kaspersky Endpoint Security va trimite cheia principală către Kaspersky Security Center în timpul următoarei sincronizări.

   > În cazul în care computerul pe care este salvată cheia principală este corupt și datele nu sunt trimise către Kaspersky Security Center, nu este posibil să obțineți acces la unitatea amovibilă.

   În cazul în care caseta de selectare **Permiteți criptarea unităților amovibile în modul offline** este debifată și nu există nicio conexiune la Kaspersky Security Center, nu este posibilă criptarea unității amovibile.

9. Salvați-vă modificările.

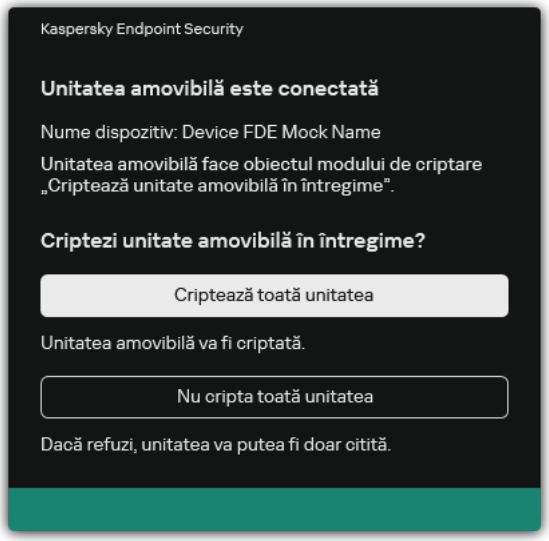
După aplicarea politicii, atunci când utilizatorul conectează o unitate amovibilă sau dacă o unitate amovibilă este deja conectată, Kaspersky Endpoint Security solicită utilizatorului confirmarea efectuării operației de criptare (consultați figura de mai jos).

Aplicația vă permite să efectuați următoarele acțiuni:

- Dacă utilizatorul confirmă solicitarea de criptare, Kaspersky Endpoint Security criptează datele.
- Dacă utilizatorul refuză cererea de criptare, Kaspersky Endpoint Security lasă datele neschimbate și atribuie acces numai în citire pentru această unitate amovibilă.
- Dacă utilizatorul nu răspunde la cererea de criptare, Kaspersky Endpoint Security lasă datele neschimbate și atribuie acces numai în citire pentru această unitate amovibilă. Aplicația solicită din nou confirmarea atunci când aplicați ulterior o politică sau data viitoare când este conectată această unitate amovibilă.

Dacă utilizatorul inițiază eliminarea în siguranță a unei unități amovibile în timpul criptării datelor, Kaspersky Endpoint Security întrerupe procesul de criptare a datelor și permite eliminarea unității amovibile înainte de finalizarea procesului de criptare. Criptarea datelor va fi continuată data viitoare când unitatea amovibilă este conectată la acest computer.

În cazul în care criptarea unei unități amovibile a eșuat, vizualizați raportul **Criptare date** în interfața Kaspersky Endpoint Security. Accesul la fișiere poate fi blocat de o altă aplicație. În acest caz, încercați să deconectați unitatea amovibilă de la computer și să o conectați din nou.



Solicitare de criptare a unității amovibile

Adăugarea unei reguli de criptare pentru unități amovibile

Pentru a adăuga o regulă de criptare pentru unități amovibile:

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Criptare date** → **Criptare unități amovibile**.
4. Faceți clic pe butonul **Adaugă** în lista verticală și selectați unul dintre elementele următoare:
   - Dacă dorești să adaugi reguli de criptare pentru unități amovibile care se găsesc în lista de dispozitive de încredere din componenta Control dispozitive, selectați **Din lista de dispozitive de încredere a acestei politici**.
   - Dacă dorești să adaugi reguli de criptare pentru unitățile amovibile care sunt în lista Kaspersky Security Center, selectează **Din lista de dispozitive a Kaspersky Security Center**.
5. În lista verticală **Mod de criptare pentru dispozitivele selectate**, selectează acțiunea care va fi efectuată de către Kaspersky Endpoint Security asupra fișierelor stocate pe unitățile amovibile selectate.

6. Bifează caseta de selectare **Mod portabil** dacă dorești ca aplicația Kaspersky Endpoint Security să pregătească unitățile amovibile înainte de criptare, făcând posibilă utilizarea fișierelor criptate stocate pe ele în modul portabil.

   Modul portabil îți permite să folosești fișiere criptate stocate pe unități amovibile care sunt conectate la computere fără funcționalitatea de criptare.

7. Bifați caseta de selectare **Criptează doar spațiul de disc utilizat** dacă dorești ca aplicația Kaspersky Endpoint Security să cripteze doar acele sectoare de disc care sunt ocupate de fișiere.

   Dacă aplici criptarea unei unități aflate deja în uz, se recomandă să criptezi întreaga unitate. Astfel se asigură protecția tuturor datelor – chiar și a datelor șterse care pot conține informații ce pot fi recuperate. Funcția **Criptează doar spațiul de disc utilizat** este recomandată pentru unități noi care nu au fost folosite anterior.

   Dacă un dispozitiv a fost criptat anterior folosind funcția **Criptează doar spațiul de disc utilizat**, după aplicarea unei politici în modul **Criptează unitate amovibilă în întregime**, sectoarele care nu sunt ocupate de fișiere în continuare nu vor fi criptate.

8. În lista verticală **Acțiuni pentru dispozitive selectate anterior**, selectați acțiunea care va fi efectuată de Kaspersky Endpoint Security în conformitate cu regulile de criptare care au fost definite anterior pentru unități amovibile:

   - Dacă dorești ca regula de criptare creată anterior să rămână neschimbată, selectați **Omite**.
   - Dacă doriți ca regula de criptare creată anterior pentru unitatea amovibilă să fie înlocuită de noua regulă, selectați **Împrospătează**.

9. Salvați-vă modificările.

Regulile de criptare adăugate pentru unitățile amovibile vor fi aplicate unităților amovibile conectate la orice computere din organizație.

Exportul și importul unei liste de reguli de criptare pentru unitățile amovibile

Puteți exporta lista de reguli pentru criptarea unităților amovibile într-un fișier XML. Apoi, puteți modifica fișierul pentru a adăuga, de exemplu, un număr mare de reguli pentru același tip de unități amovibile. De asemenea, puteți utiliza funcția de export/import pentru a face o copie de rezervă a listei de reguli sau pentru a migra regulile pe un alt server.

Cum se exportă și se importă o listă de reguli de criptare a unităților amovibile în Consola de administrare (MMC)

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.
4. Accesați **Data Encryption** → **Encryption of removable drives**.

5. În blocul **Encryption rules for selected devices**, faceți clic pe linkul **<N> rules**.

   Aceasta deschide o listă de reguli de criptare pentru unitățile amovibile.

6. Pentru a exporta lista de reguli de criptare a unităților amovibile:

   a. Selectați regulile pe care doriți să le exportați.

   b. Fă clic pe **Export**.

   c. Confirmați că doriți să exportați numai regulile selectate sau să exportați întreaga listă.

   d. Salvați fișierul.

      Kaspersky Endpoint Security exportă lista de reguli într-un fișier XML în directorul de descărcări implicit.

7. Pentru a importa lista de reguli:

   a. Faceți clic pe linkul **Import**.

      În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de reguli.

   b. Deschideți fișierul.

      În cazul în care computerul are deja o listă de reguli, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul XML.

8. Salvați-vă modificările.

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.

2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

3. În fereastra politicii, selectați **Criptare date** → **Criptare unități amovibile**.

4. Pentru a exporta lista de reguli de criptare a unităților amovibile:

   a. Selectați regulile pe care doriți să le exportați. Pentru a selecta mai multe porturi, utilizați tastele **CTRL** sau **SHIFT**.

      Dacă nu ați selectat nicio regulă, Kaspersky Endpoint Security va exporta toate regulile.

   b. Faceți clic pe linkul **Exportă**.

   c. În fereastra care se deschide, specificați numele fișierului XML în care doriți să exporți lista de reguli și selectați directorul în care doriți să salvați acest fișier.

   d. Salvați fișierul.

      Kaspersky Endpoint Security exportă lista de reguli în fișierul XML.

5. Pentru a importa o listă de reguli de criptare a unităților amovibile:

   a. Faceți clic pe linkul **Importă**.

      În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de reguli.

b. Deschideți fișierul.

În cazul în care computerul are deja o listă de reguli, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul XML.

6. Salvați-vă modificările.

Modul portabil pentru accesarea fișierelor criptate de pe unități amovibile

Portable mode este un mod de criptare a fișierelor (FLE) pe unitățile amovibile care oferă posibilitatea de a accesa date din afara unei rețele corporative. Modul portabil vă permite, de asemenea, să lucrați cu date criptate pe computere care nu au instalat Kaspersky Endpoint Security.

Modul portabil este convenabil de utilizat în următoarele cazuri:

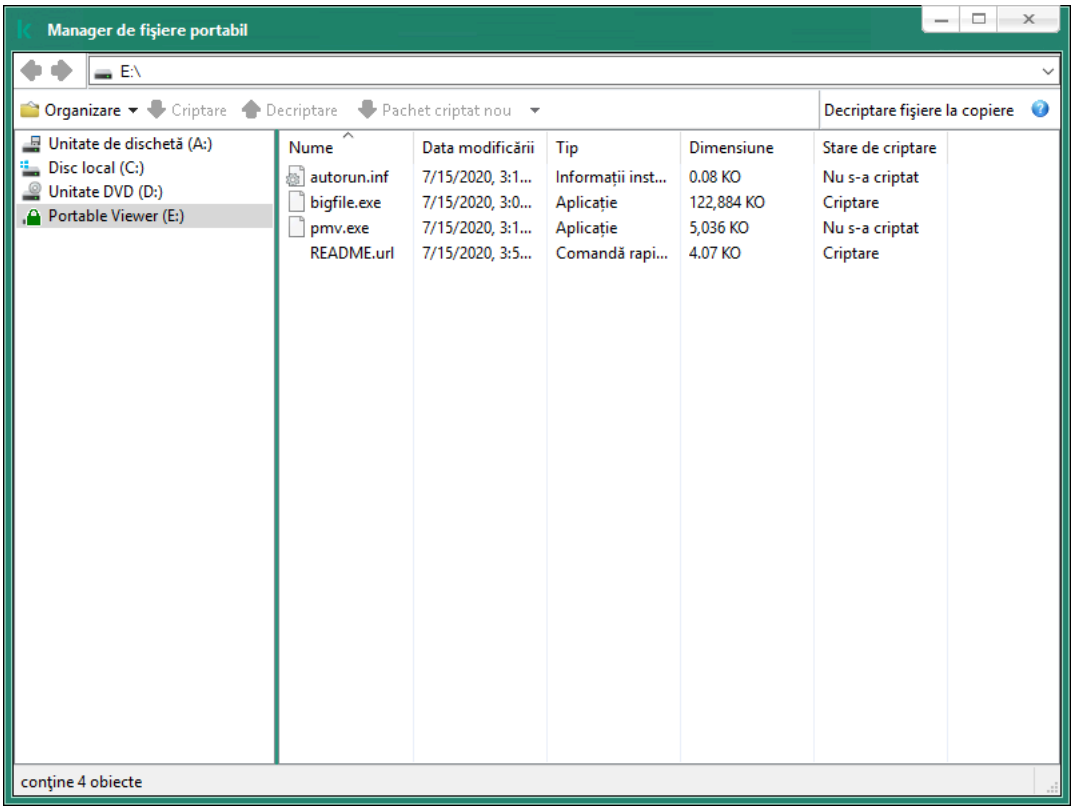
- Nu există nicio conexiune între computer și Serverul de administrare Kaspersky Security Center.
- Infrastructura s-a schimbat odată cu schimbarea Serverului de administrare Kaspersky Security Center.
- Kaspersky Endpoint Security nu este instalat pe computer.

Manager de fișiere portabil

Pentru a funcționa în modul portabil, Kaspersky Endpoint Security instalează un modul de criptare special numit *Manager de fișiere portabil* pe o unitate amovibilă. Managerul de fișiere portabil oferă o interfață pentru a lucra cu date criptate dacă Kaspersky Endpoint Security nu este instalat pe computer (consultați figura de mai jos). Dacă Kaspersky Endpoint Security este instalat pe computer, puteți lucra cu unități amovibile criptate folosind managerul dvs. de fișiere obișnuit (de exemplu, Explorer).

Managerul de fișiere portabil stochează o cheie pentru criptarea fișierelor pe o unitate amovibilă. Cheia este criptată cu parola utilizatorului. Utilizatorul setează o parolă înainte de criptarea fișierelor pe o unitate amovibilă.

Managerul de fișiere portabil pornește automat când o unitate amovibilă este conectată la un computer pe care Kaspersky Endpoint Security nu este instalat. Dacă pornirea automată a aplicațiilor este dezactivată pe computer, porniți manual Managerul de fișiere portabil. Pentru aceasta, executați fișierul numit pmv.exe care este stocat pe unitatea amovibilă.



Manager de fișiere portabil

Asistență pentru modul portabil pentru lucrul cu fișiere criptate

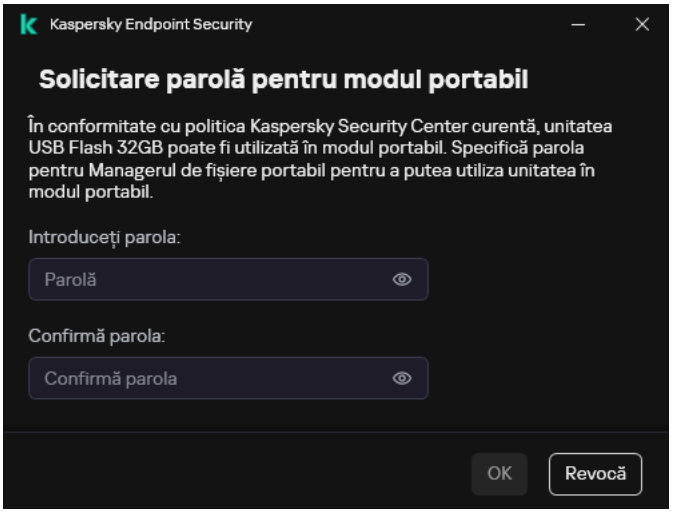
Cum să activați asistența pentru modul portabil pentru lucrul cu fișierele criptate pe unitățile amovibile în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Criptare date** → **Criptare unități amovibile**.
4. În lista verticală **Mod de criptare pentru dispozitivele selectate**, selectați **Criptează toate fișierele** sau **Criptează numai fișiere noi**.

   Modul portabil este disponibil numai cu File Level Encryption (FLE). Nu este posibilă activarea asistenței pentru modul portabil pentru Full Disk Encryption (FDE).

5. Bifați caseta de selectare **Mod portabil**.
6. Dacă este necesar, adăugați reguli de criptare pentru unitățile amovibile individuale.
7. Salvați-vă modificările.
8. După aplicarea politicii, conectați unitatea amovibilă la computer.
9. Confirmă funcționarea criptării unității amovibile.

Se deschide o fereastră în care puteți crea o parolă pentru Manager de fișiere portabil.



Solicitare parolă pentru modul portabil

10. Specifică o parolă care îndeplinește cerințele de complexitate și confirm-o.
11. Salvați-vă modificările.

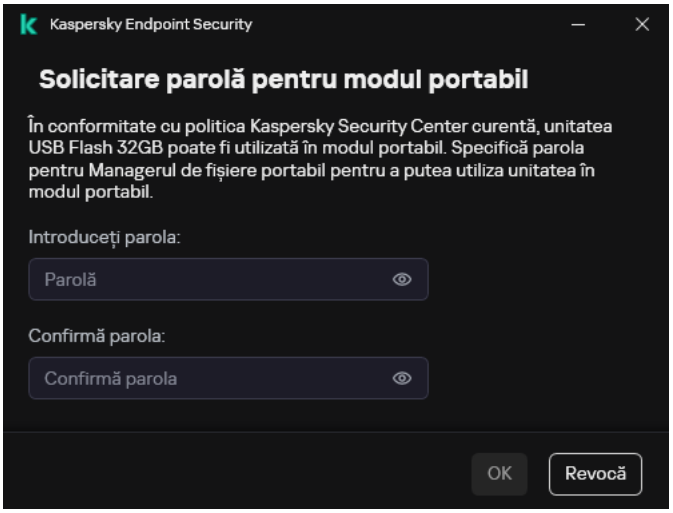
Cum să activați asistența pentru modul portabil pentru lucrul cu fișierele criptate pe unitățile amovibile în Web Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.
   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Data Encryption** → **Encryption of removable drives**.
5. În secțiunea **Default action**, selectați **Encrypt all files** sau **Encrypt new files only**.

   Modul portabil este disponibil numai cu File Level Encryption (FLE). Nu este posibilă activarea asistenței pentru modul portabil pentru Full Disk Encryption (FDE).

6. Bifați caseta de selectare **Portable mode**.
7. Dacă este necesar, adăugați reguli de criptare pentru unitățile amovibile individuale.
8. Salvați-vă modificările.
9. După aplicarea politicii, conectați unitatea amovibilă la computer.
10. Confirmă funcționarea criptării unității amovibile.

Se deschide o fereastră în care puteți crea o parolă pentru Manager de fișiere portabil.



Solicitare parolă pentru modul portabil

11. Specifică o parolă care îndeplinește cerințele de complexitate și confirm-o.

12. Salvați-vă modificările.

Kaspersky Endpoint Security va cripta fișierele de pe unitatea amovibilă. Aplicația Manager de fișiere portabil utilizată pentru lucrul cu fișiere criptate va fi și ea adăugată pe unitatea amovibilă. Dacă există deja fișiere criptate pe unitatea amovibilă, Kaspersky Endpoint Security le va cripta din nou folosind propria sa cheie. Acest lucru permite utilizatorului să acceseze toate fișierele de pe unitatea amovibilă în modul portabil.

Accesarea fișierelor criptate pe o unitate amovibilă

După criptarea fișierelor pe o unitate amovibilă cu asistență pentru modul portabil, sunt disponibile următoarele metode de accesare a fișierelor:

- Dacă Kaspersky Endpoint Security nu este instalat pe computer, aplicația Manager de fișiere portabil vă va solicita să introduceți o parolă. Va trebui să introduceți parola de fiecare dată când reporniți computerul sau reconectați unitatea amovibilă.

- În cazul în care computerul se află în afara rețelei corporative și Kaspersky Endpoint Security este instalat pe computer, aplicația vă va solicita să introduceți parola sau să trimiteți administratorului o solicitare pentru a accesa fișierele. După obținerea accesului la fișierele de pe o unitate amovibilă, Kaspersky Endpoint Security va salva cheia secretă în stocarea cheilor computerului. Acest lucru va permite accesul la fișiere în viitor fără a introduce o parolă sau a solicita administratorului (vezi figura de mai jos).

- În cazul în care computerul se află în rețeaua corporativă și Kaspersky Endpoint Security este instalat pe computer, veți avea acces la dispozitiv fără a introduce o parolă. Kaspersky Endpoint Security va primi cheia secretă de la Serverul de administrare Kaspersky Security Center la care este conectat computerul.



Accesarea fișierelor criptate pe o unitate amovibilă

Recuperarea parolei pentru lucrul în modul portabil

Dacă ați uitat parola pentru lucrul în modul portabil, trebuie să conectați unitatea amovibilă la un computer care are instalat Kaspersky Endpoint Security din rețeaua corporativă. Veți avea acces la fișiere, deoarece cheia secretă este stocată în stocarea pentru chei a computerului sau pe Serverul de administrare. Decriptați și criptați fișierele cu o nouă parolă.

Caracteristici ale modului portabil atunci când conectați o unitate amovibilă la un computer dintr-o altă rețea

În cazul în care computerul se află în afara rețelei corporative și Kaspersky Endpoint Security este instalat pe computer, puteți accesa fișierele în următoarele moduri:

- **Acces pe bază de parolă**

  După introducerea parolei, veți putea vizualiza, modifica și salva fișierele pe unitatea amovibilă (*acces transparent*). Kaspersky Endpoint Security poate seta un drept de acces numai de citire pentru o unitate detașabilă dacă următorii parametri sunt configurați în setările politicii pentru criptarea unităților amovibile:

  - Asistența în modul portabil este dezactivată.
  - Modul **Criptează toate fișierele** sau **Criptează numai fișiere noi** este selectat.

  În toate celelalte cazuri, veți avea acces complet la unitatea amovibilă (permisiunea de citire/scriere). Veți putea adăuga și șterge fișiere.

  Puteți modifica permisiunile de acces la unitățile amovibile chiar și în timp ce unitatea amovibilă este conectată la computer. Dacă se modifică permisiunile de acces la unitatea amovibilă, Kaspersky Endpoint Security va bloca accesul la fișiere și vă va solicita din nou parola.

  După introducerea parolei, nu puteți aplica setările politicii de criptare pentru unitatea amovibilă. În acest caz, este imposibil să decriptați sau să recriptați fișierele de pe unitatea amovibilă.

- **Solicită administratorului accesul la fișiere**

Dacă ați uitat parola pentru a lucra în modul portabil, cereți administratorului acces la fișiere. Pentru a accesa fișierele, utilizatorul trebuie să trimită administratorului un fișier de solicitare a accesului (un fișier cu extensia KESDC). Utilizatorul poate trimite fișierul de solicitare a accesului prin e-mail, de exemplu. Administratorul va trimite un fișier criptat de acces la date (un fișier cu extensia KESDR).

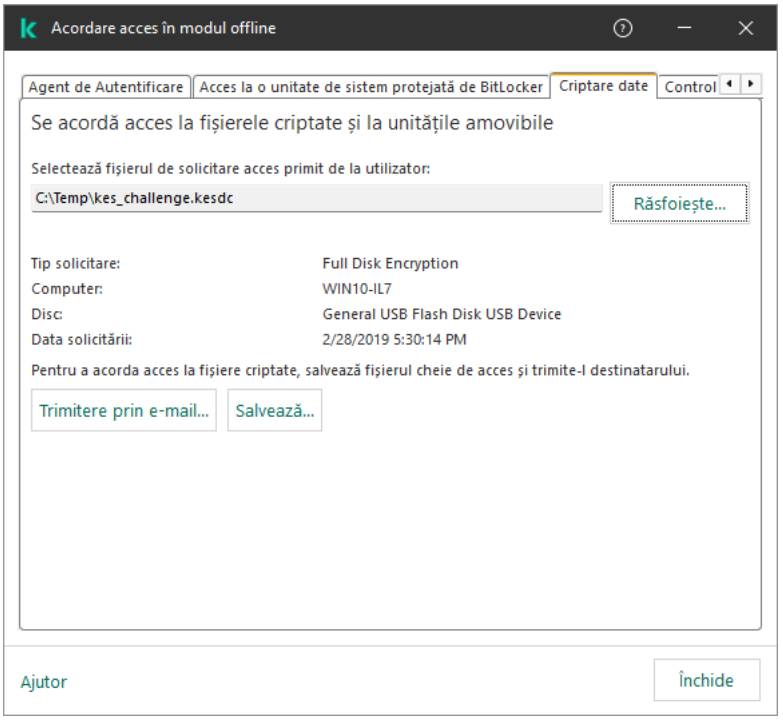
După ce finalizați procedura de recuperare a parolei Solicitare-Răspuns, veți primi acces transparent la fișierele de pe unitatea amovibilă și acces complet la unitatea amovibilă (permisiunea de citire/scriere).

Puteți aplica o politică de criptare a unității amovibile și decripta fișierele, de exemplu. După recuperarea parolei sau după actualizarea politicii, Kaspersky Endpoint Security vă va solicita să confirmați modificările.

Cum se obține un fișier criptat de acces la date în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați **Devices**.
3. În fila **Devices**, selectați computerul utilizatorului care solicită accesul la datele criptate și faceți clic dreapta pe el pentru a deschide meniul contextual.
4. În meniul contextual, selectați **Acordare acces în modul offline**.
5. Se deschide o fereastră; în acea fereastră, selectați fila **Criptare date**.
6. În fila **Criptare date**, faceți clic pe butonul **Răsfoiește**.
7. În fereastra pentru selectarea unui fișier de solicitare a accesului, specificați calea către fișierul primit de la utilizator.

Veți vedea informații despre solicitarea utilizatorului. Kaspersky Security Center generează un fișier cheie. Trimiteți utilizatorului prin e-mail fișierul cheie de acces la date criptate generat. Sau salvați fișierul de acces și utilizați orice metodă disponibilă pentru a transfera fișierul.



Acordarea accesului în modul offline

Cum se obține un fișier criptat de acces la date în Web Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Assets (Devices)**.
2. Bifați caseta de selectare de lângă numele computerului la ale cărui date doriți să restaurați accesul.
3. Fă clic pe **Grant access to the device in offline mode**.
4. Selectați **Data Encryption**.
5. Faceți clic pe butonul **Select file** și selectați fișierul de solicitare a accesului pe care l-ați primit de la utilizator (un fișier cu extensia KESDC).

   Web Console va afișa informații despre solicitare. Acestea vor include numele computerului pe care utilizatorul solicită acces la fișier.
6. Faceți clic pe butonul **Save key** și selectați un director pentru a salva fișierul cheie de acces la datele criptate (un fișier cu extensia KESDR).

Drept urmare, veți putea obține cheia de acces la datele criptate, pe care va trebui să o transferați utilizatorului.

Decriptarea unităților amovibile

Puteți utiliza o politică pentru a decripta o unitate amovibilă. O politică cu setări definite pentru criptarea unității amovibile este generată pentru un anumit grup de administrare. Prin urmare, rezultatul decriptării datelor de pe unități amovibile depinde de computerul la care este conectată unitatea amovibilă.

Pentru a decripta unități amovibile:

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Criptare date** → **Criptare unități amovibile**.
4. Dacă dorești să decriptezi toate fișierele criptate stocate pe unități amovibile, în lista verticală **Mod criptare** selectați **Decriptează unitate amovibilă în întregime**.

5. Pentru a decripta datele stocate pe unități amovibile individuale, editează regulile de criptare pentru unitățile amovibile ale căror date dorești să le decriptezi. Pentru aceasta:

   a. În lista de unități amovibile pentru care au fost configurate reguli de criptare, selectați o înregistrare care corespunde unității amovibile de care ai nevoie.

   b. Fă clic pe butonul **Setare regulă** pentru a edita regula de criptare pentru unitatea amovibilă selectată.

   c. În meniul contextual al butonului **Setare regulă**, selectează elementul **Decriptează unitate amovibilă în întregime**.

6. Salvați-vă modificările.

Drept urmare, dacă un utilizator conectează o unitate amovibilă sau dacă este deja conectată, Kaspersky Endpoint Security decriptează unitatea amovibilă. Aplicația îl avertizează pe utilizator că procesul de decriptare poate dura ceva timp. Dacă utilizatorul inițiază eliminarea în siguranță a unei unități amovibile în timpul decriptării datelor, Kaspersky Endpoint Security întrerupe procesul de decriptare a datelor și permite eliminarea unității amovibile înainte de finalizarea operațiunii de decriptare. Decriptarea datelor va fi continuată data viitoare când unitatea amovibilă este conectată la acest computer.

În cazul în care decriptarea unei unități amovibile a eșuat, vizualizați raportul **Criptare date** în interfața Kaspersky Endpoint Security. Accesul la fișiere poate fi blocat de o altă aplicație. În acest caz, încercați să deconectați unitatea amovibilă de la computer și să o conectați din nou.

Vizualizarea detaliilor de criptare date

Atunci când criptarea sau decriptarea este în curs, Kaspersky Endpoint Security transmite informații despre starea parametrilor de criptare aplicați computerelor client de Kaspersky Security Center.

Vizualizarea stării de criptare

Puteți privi starea pentru a monitoriza criptarea datelor. Kaspersky Endpoint Security atribuie următoarele stări de criptare:

- **Does not meet the policy; canceled by user**. Utilizatorul a revocat criptarea datelor.
- **Does not meet the policy due to an error**. Eroare de criptare a datelor, de exemplu, lipsește o licență.
- **Applying the policy; restart is required**. Criptarea datelor este în curs de desfășurare pe acest computer. Repornește computerul pentru a finaliza criptarea.
- **No encryption policy specified**. Criptarea datelor este dezactivată în setările politicii.
- **Not supported**. Componentele de criptare a datelor nu sunt instalate pe computer.
- **Applying the policy**. Criptarea și/sau decriptarea datelor este în curs pe acest computer.

Pentru a vedea starea de criptare a datelor computerului:

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați **Managed devices**.
3. În fila **Devices** din spațiul de lucru, defilează până la maximum dreapta baza de defilare. În cazul în care coloana **Encryption status** nu este afișată, adăugați această coloană în setările consolei Kaspersky Security Center.

   Coloana **Encryption status** afișează starea de criptare a datelor de pe computerele din grupul de administrare selectat. Această stare este definită în baza informațiilor despre criptarea fișierelor de pe unitățile locale ale computerului și a celor despre funcția Full Disk Encryption.
4. Dacă starea criptării datelor pentru computer este **Applying policy**, puteți monitoriza panoul de progres al criptării:
   a. Deschideți proprietățile computerului cu starea **Applying policy**, făcând dublu clic pe el.
   b. În fereastra cu proprietățile computerului, selectează secțiunea **Applications**.
   c. În lista de aplicații Kaspersky instalate pe computer, selectați **Kaspersky Endpoint Security for Windows**.
   d. Fă clic pe **Statistics**.
   e. În **Encryption of devices** puteți vedea progresul curent al criptării datelor ca procent.

Vizualizarea statisticilor de criptare pe tablourile de bord Kaspersky Security Center

Pentru a vizualiza starea de criptare pe tablourile de bord Kaspersky Security Center:

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați nodul **Administration Server**.
3. În spațiul de lucru din dreapta arborelui consolei de administrare, selectați fila **Statistics**.
4. Creează o pagină nouă cu panouri de detalii care conțin statistici de criptare a datelor. Pentru aceasta:
   a. În fila **Statistics**, faceți clic pe butonul **Customize view**.
   b. În fereastra care se deschide, faceți clic pe butonul **Add**.
   c. Se deschide o fereastră; în această fereastră, în secțiunea **General**, introduceți numele paginii.
   d. În secțiunea **Information panels**, faceți clic pe butonul **Add**.
   e. În fereastra care se deschide în grupul **Protection status**, selectează elementul **Encryption of devices**.
   f. Fă clic pe **OK**.
   g. Dacă este necesar, editați setările panoului de detalii. Pentru aceasta, folosește secțiunile **View** și **Devices**.

h. Fă clic pe **OK**.

i. Repetă pașii d – h din instrucțiuni, selectând elementul **Encryption of removable drives** din secțiunea **Protection status**.

Panourile de detalii adăugate apar în lista **Information panels**.

j. Fă clic pe **OK**.

Numele paginii cu panourile de detalii create în pașii anteriori apare în lista **Pages**.

k. Faceți clic pe butonul **Close**.

5. În fila **Statistics**, deschide pagina creată în pașii anteriori din aceste instrucțiuni.

Apar panourile de detalii, prezentând starea de criptare pentru computere și unități amovibile.

Vizualizarea erorile de criptare fișiere pe unitățile locale ale computerului

Pentru a vizualiza erorile de criptare fișiere pe unitățile locale ale computerului:

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați **Managed devices**.
3. În fila **Devices**, selectați numele computerului în listă și faceți clic dreapta pe el pentru a deschide meniul contextual.
4. În meniul contextual al computerului, selectați elementul **Properties**. În fereastra care se deschide, selectați secțiunea **Protection**.
5. Faceți clic pe linkul **View data encryption errors** pentru a deschide fereastra **Data encryption errors**.

Această fereastră afișează detalii despre erorile de criptare fișiere pe unitățile locale ale computerului. Atunci când o eroare este corectată, Kaspersky Security Center elimină detaliile erorii din fereastra **Data encryption errors**.

Vizualizarea raportului de criptare a datelor

Kaspersky Security Center vă permite să creați rapoarte de criptare a datelor:

- **Report on encryption status of managed devices**. Raportul include informații privind conformitatea stării de criptare a computerului cu politica de criptare.
- **Report on encryption status of mass storage devices**. Raportul include informații despre starea de criptare a dispozitivelor externe și a dispozitivelor de stocare.
- **Report on rights to access encrypted drives**. Raportul include informații despre starea conturilor care au acces la unități criptate.

- **Report on file encryption errors**. Raportul include informații despre erorile care au apărut în timpul executării sarcinilor de criptare sau de decriptare a datelor pe computere.
- **Report on blockage of access to encrypted files**. Raportul include informații despre aplicațiile care nu au acces la fișierele criptate.

Pentru a vizualiza raportul de criptare a datelor:

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În nodul **Administration Server** din arborele consolei de administrare, selectați fila **Reports**.
3. Faceți clic pe butonul **New report template**.

   Se lansează Expertul pentru șablon de raport nou.
4. Urmează instrucțiunile din Expertul pentru șablon de raport. În fereastra **Selecting the report template type**, în secțiunea **Other**, selectați unul dintrerapoartele de criptare:

   După ce ai finalizat Expertul pentru șablon de raport nou, un nou șablon de raport apare în tabelul din fila **Reports**.
5. Selectați șablonul de raport creat în pasul anterior al instrucțiunilor.
6. În meniul contextual al șablonului, selectați **Show report**.

Începe procesul de generare a raportului. Raportul este afișat într-o fereastră nouă.

Lucrul cu dispozitive criptate atunci când nu există acces la acestea

Obținerea accesului la dispozitive criptate

Este posibil ca un utilizator să trebuiască să solicite acces la dispozitive criptate în următoarele cazuri:

- Unitatea de hard disk a fost criptată pe alt computer.
- Cheia de criptare pentru un dispozitiv nu este pe computer (de exemplu, la prima încercare de a accesare a unității amovibile criptate pe computer) și computerul nu este conectat la Kaspersky Security Center.

  După ce utilizatorul a aplicat cheia de acces dispozitivului criptat, Kaspersky Endpoint Security salvează cheia de criptare pe computerul utilizatorului și permite accesul la acest dispozitiv la încercările de accesare ulterioare chiar dacă nu există conexiune la Kaspersky Security Center.

Accesul la dispozitive criptate poate fi obținut după cum urmează:

1. Utilizatorul folosește interfața aplicației Kaspersky Endpoint Security pentru a crea un fișier de solicitare a accesului cu extensia kesdc și-l trimite administratorului rețelei LAN a companiei.
2. Administratorul utilizează Kaspersky Security Center Administration Console pentru a crea un fișier cheie de acces cu extensia kesdr și-l trimite utilizatorului.
3. Utilizatorul aplică cheia de acces.

Restaurarea datelor pe dispozitive criptate

Un utilizator poate folosi Utilitarul de restaurare pentru dispozitive criptate (denumit în continuare Utilitarul de restaurare) pentru a lucra cu dispozitive criptate. Acest lucru este necesar în următoarele cazuri:

- Procedura pentru utilizarea unei chei de acces pentru obținerea accesului nu s-a finalizat cu succes.
- Componentele de criptare nu au fost instalate pe computer cu dispozitivul criptat.

Datele necesare pentru restaurarea accesului la dispozitive criptate utilizându-se Utilitarul de restaurare sunt rezidente de câtva timp în memoria computerului utilizatorului în formă necriptată. Pentru a reduce riscul de acces neautorizat la astfel de date, te sfătuim să restaurezi accesul la dispozitive criptate pe dispozitive de încredere.

Datele de pe dispozitive criptate pot fi restaurate după cum urmează:

1. Utilizatorul folosește Utilitarul de restaurare pentru a crea un fișier de solicitare a accesului cu extensia fdertc și-l trimite administratorului rețelei LAN a companiei.
2. Administratorul utilizează Kaspersky Security Center Administration Console pentru a crea un fișier cheie de acces cu extensia fdertr și-l trimite utilizatorului.
3. Utilizatorul aplică cheia de acces.

Pentru a restaura date pe unități de hard disk de sistem criptate, utilizatorul poate, de asemenea, să specifice acreditările pentru contul de Agent de Autentificare în Utilitarul de restaurare. Dacă metadatele contului de Agent de Autentificare au fost corupte, utilizatorul trebuie să finalizeze procedura de restaurare utilizând fișierul solicitare acces.

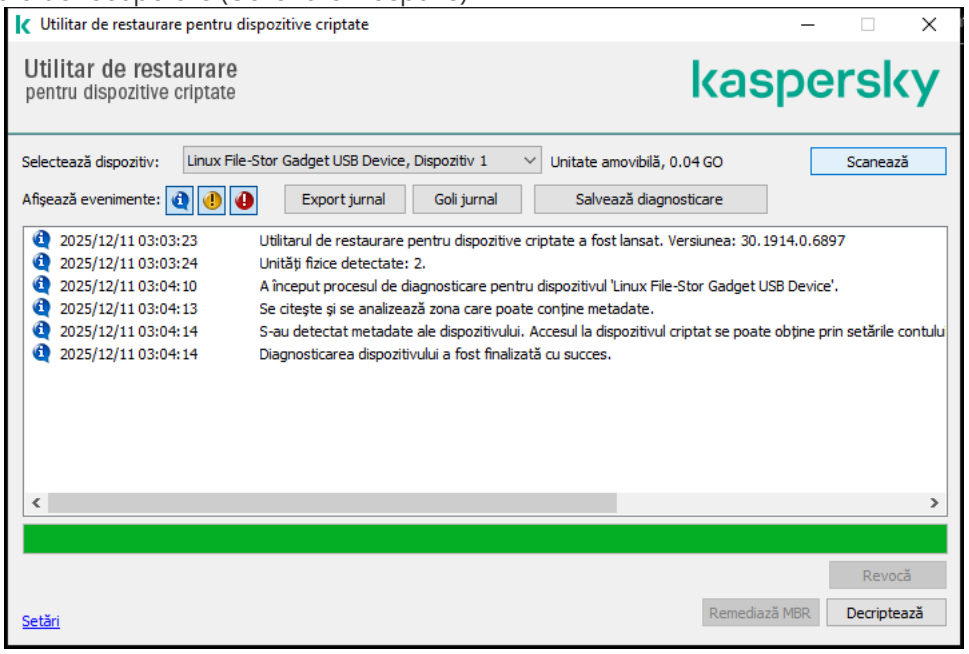
Înainte de a restaura datele pe dispozitive criptate, se recomandă să revoci politica aplicației Kaspersky Security Center sau să dezactivezi criptarea în setările politicii aplicației Kaspersky Security Center pe computerul pe care va fi efectuată operațiunea. Aceasta împiedică dispozitivul să fie criptat din nou.

Recuperarea datelor utilizând Utilitarul de restaurare FDERT

Dacă unitatea de hard disk dă eroare, sistemul de fișiere poate fi corupt. În acest caz, datele protejate de tehnologia Kaspersky Disk Encryption nu vor fi disponibile. Puteți să decriptași datele și să le copiați pe o unitate nouă.

Recuperarea datelor de pe o unitate protejată de tehnologia Kaspersky Disk Encryption constă în următorii pași:

1. Creați un Utilitar de restaurare independent (consultați figura de mai jos).
2. Conectați o unitate la un computer care nu are componente de criptare Kaspersky Endpoint Security instalate.
3. Rulați Utilitarul de restaurare și diagnosticați unitatea de hard disk.
4. Accesați datele de pe unitate. Pentru a face acest lucru, introduceți acreditările Agentului de Autentificare sau începeți procedura de recuperare (Solicitare-Răspuns).



Utilitarul de restaurare FDERT

Crearea unui utilitar de restaurare independent

Pentru a crea fișierul executabil al utilitarului Restaurare:

1. În fereastra principală a aplicației, faceți clic pe butonul .
2. În fereastra care se deschide, faceți clic pe butonul **Restaurare dispozitiv criptat**.

   Se lansează Utilitarul de restaurare pentru dispozitive criptate.
3. Faceți clic pe butonul **Creează Utilitar de restaurare independent** în fereastra utilitarului Restaurare.
4. Salvați Utilitarul de restaurare independent în memoria computerului.

Drept urmare, fișierul executabil al Utilitarului de restaurare (fdert.exe) va fi salvat în directorul specificat. Copiați Utilitarul de restaurare pe un computer care nu are componente de criptare Kaspersky Endpoint Security. Aceasta împiedică unitatea să fie criptată din nou.

Datele necesare pentru restaurarea accesului la dispozitive criptate utilizându-se Utilitarul de restaurare sunt rezidente de câtva timp în memoria computerului utilizatorului în formă necriptată. Pentru a reduce riscul de acces neautorizat la astfel de date, te sfătuim să restaurezi accesul la dispozitive criptate pe dispozitive de încredere.

Recuperarea datelor de pe o unitate de hard disk

Pentru a restaura accesul la un dispozitiv criptat folosind Utilitarul de restaurare:

1. Executați fișierul numit fdert.exe, care este fișierul executabil al Utilitarului de restaurare. Acest fișier este creat de Kaspersky Endpoint Security.

2. În fereastra Restore Utility, selectați dispozitivul criptat la care doriți să restaurați accesul.

3. Faceți clic pe butonul **Scanează** pentru a permite utilitarului să definească acțiunile care trebuie efectuate asupra dispozitivului: acesta trebuie deblocat sau decriptat.

   În cazul în care computerul are acces la funcționalitatea de criptare Kaspersky Endpoint Security, Utilitarul de restaurare îți solicită să deblochezi dispozitivul. Deblocarea unui dispozitiv nu este sinonimă cu decriptarea lui, dar dispozitivul devine accesibil direct ca urmare a acțiunii de deblocare. În cazul în care computerul nu are acces la funcționalitatea de criptare Kaspersky Endpoint Security, Utilitarul de restaurare îți solicită să decriptezi dispozitivul.

4. Dacă doriți să importați informațiile dignosticării, faceți clic pe butonul **Salvează diagnosticare**.

   Utilitarul va salva o arhivă cu fișierele care conțin informațiile diagnosticării.

5. Faceți clic pe butonul **Remediază MBR** dacă diagnosticarea unității de hard disk de sistem criptat a returnat un mesaj despre probleme cu înregistrarea master boot record (MBR) a dispozitivului.

   Remedierea înregistrării master boot record a dispozitivului poate accelera procesul de obținere a informațiilor necesare pentru deblocarea sau decriptarea dispozitivului.

6. Faceți clic pe butonul **Deblochează** sau **Decriptează** în funcție de rezultatele diagnosticării.

7. Dacă doriți să restaurați datele utilizând un cont Agent de Autentificare, selectați opțiunea **Utiliză setări cont Agent de Autentificare** și introduceți acreditările Agentului de Autentificare.

   Această metodă este posibilă numai la restaurarea datelor pe o unitate de hard disk de sistem. Dacă unitatea de hard disk de sistem a fost coruptă și datele contului Agent de Autentificare s-au pierdut, trebuie să obții o cheie de acces de la administratorul rețelei LAN a companiei pentru a restaura date pe un dispozitiv criptat.

8. Dacă doriți să începeți procedura de recuperare, procedați astfel:

   a. Selectați opțiunea **Specifică manuală cheie de acces pentru dispozitiv**.

   b. Faceți clic pe butonul **Primi cheie de acces** și salvați fișierul de solicitare a accesului în memoria computerului (un fișier cu extensia FDERTC).

   c. Trimite fișierul solicitare acces administratorului rețelei LAN a companiei.

   > Nu închide fereastra **Primi cheie de acces pentru dispozitiv** până când nu primești cheia de acces. Atunci când se deschide din nou această fereastră, nu mai poți aplica cheia de acces creată anterior de către administrator.

   d. Primiți și salvați fișierul de acces (un fișier cu extensia FDERTR) care a fost creat și v-a fost trimis de administratorul rețelei LAN corporative (consultați instrucțiunile de mai jos).

   e. Descărcați fișierul de acces în fereastra **Primi cheie de acces pentru dispozitiv**.

9. Dacă decriptați un dispozitiv, trebuie să configurați setările de decriptare suplimentare:

    - Specifică zona de decriptat:

        - Dacă dorești să decriptezi întregul dispozitiv, selectați opțiunea **Decriptare întregul dispozitiv**.

        - Dacă doriți să decriptați o parte din datele de pe un dispozitiv, selectați opțiunea **Decriptare zone individuale din dispozitiv** și specificați limitele zonei de decriptare.

    - Selectați locația pentru scrierea datelor decriptate:

        - Dacă dorești rescrierea datelor de pe dispozitivul original cu datele decriptate, debifați caseta de selectare **Decriptare în fișier imagine disc**.

        - Dacă dorești să salvezi date decriptate separat de datele criptate originale, bifați caseta de selectare **Decriptare în fișier imagine disc** și utilizează butonul **Răsfoiește** pentru a furniza calea către locația de salvare a fișierul VHD.

10. Fă clic pe **OK**.

Începe procesul de deblocare/decriptare.

Cum se creează un fișier de acces la datele criptate în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.

2. În arborele Consolă de administrare, selectează directorul **Advanced** → **Data encryption and protection** → **Encrypted drives**.

3. În spațiul de lucru, selectați dispozitivul criptat pentru care doriți să creați un fișier cheie de acces și, în meniul contextual al dispozitivului, faceți clic pe **Obținere acces la dispozitiv în Kaspersky Endpoint Security**.

    Dacă nu ești sigur pentru ce computer a fost generat fișierul de solicitare a accesului, în arborele Consolei de administrare selectează directorul **Advanced** → **Data encryption and protection** și, în spațiul de lucru, fă clic pe **Obținere cheie de criptare a dispozitivului în Kaspersky Endpoint Security**.

4. În fereastra care se deschide, selectați algoritmul de criptare pe care doriți să îl folosiți: AES256 sau AES56.

    Algoritmul de criptare a datelor depinde de biblioteca de criptare AES care este inclusă în pachetul de distribuție: *Strong encryption (AES256)* sau *Lite encryption (AES56)*. Biblioteca de criptare AES este instalată împreună cu aplicația.

5. Fă clic pe **Răsfoiește** pentru a deschide o fereastră; în această fereastră, specificați calea către fișierul de solicitare cu extensia fdertc care a fost primit de la utilizator.

6. Fă clic pe **Deblochează**.

Veți vedea informații despre solicitarea utilizatorului. Kaspersky Security Center generează un fișier cheie. Trimiteți utilizatorului prin e-mail fișierul cheie de acces la date criptate generat. Sau salvați fișierul de acces și utilizați orice metodă disponibilă pentru a transfera fișierul.

Cum se creează un fișier de acces la datele criptate în Web Console

1. În fereastra principală a componentei Web Console, selectați **Operations** → **Data encryption and protection** → **Encrypted drives**.

2. Bifați caseta de selectare de lângă numele computerului pe care doriți să recuperați datele.

3. Fă clic pe **Grant access to the device in offline mode**.

   Astfel, Expertul este pornit pentru permiterea accesului la un dispozitiv.

4. Urmați instrucțiunile din Expert pentru permiterea accesului la un dispozitiv:

   a. Selectează plug-inul Kaspersky Endpoint Security for Windows.

   b. Selectați algoritmul de criptare pe care doriți să îl urilizați: AES256 sau AES56.

      Algoritmul de criptare a datelor depinde de biblioteca de criptare AES care este inclusă în pachetul de distribuție: *Strong encryption (AES256)* sau *Lite encryption (AES56)*. Biblioteca de criptare AES este instalată împreună cu aplicația.

   c. Selectează fișierul de solicitare a accesului primit de la utilizator (un fișier cu extensia FDERTC).

   d. Selectează un director în care să salvezi fișierul cu cheia de acces la datele criptate (un fișier cu extensia FDERTR).

Drept urmare, veți putea obține cheia de acces la datele criptate, pe care va trebui să o transferați utilizatorului.

Crearea unui disc de recuperare pentru sistemul de operare

Discul de recuperare pentru sistemul de operare poate fi util atunci când nu se poate accesa o unitate de hard disk criptată dintr-un motiv oarecare sau atunci când sistemul de operare nu se poate încărca.

Poți încărca o imagine a sistemului de operare Windows folosind discul de recuperare și poți restaura accesul la unitatea de hard disk criptată folosind utilitarul Restaurare inclus în imaginea sistemului de operare.

Pentru a crea un disc de recuperare pentru sistemul de operare:

1. Creează un fișier executabil pentru Utilitarul de restaurare pentru dispozitive criptate.

2. Creează o imagine particularizată a mediului pre-boot Windows. Atunci când creezi o imagine particularizată a mediului pre-boot Windows, adaugă la imagine fișierul executabil al utilitarului Restaurare.

3. Salvează imaginea particularizată a mediului pre-instalare Windows pe un mediu bootabil, cum ar fi un CD sau o unitate amovibilă.

   Consultați fișierele de ajutor Microsoft pentru instrucțiuni referitoare la crearea unei imagini particularizate a mediului pre-boot Windows (de exemplu, în acest resurse Microsoft TechNet).

Soluțiile Detection and Response

Soluțiile Kaspersky Detection and Response sunt sisteme de securitate pentru detectarea amenințărilor avansate și a indicatorilor de atac la diferite niveluri ale infrastructurii unei organizații. Soluțiile Detection and Response oferă informații despre amenințarea detectată și permit gestionarea acțiunilor Răspuns la amenințare.

Astfel, soluția Detection and Response face următoarele:

- Primiți informații despre funcționarea unui computer, server sau a altor dispozitive (telemetrie).
- Analizați automat informațiile pentru a detecta amenințările.
- Generați detalii despre alerte sub formă de coloane ale lanțului de dezvoltare a amenințărilor pentru analiză și alegerea acțiunilor Răspuns la amenințare.
- Efectuați acțiuni Răspuns la amenințare (de exemplu, izolarea în rețea a computerului).

Kaspersky Endpoint Security acceptă soluțiile Detection and Response utilizând un agent încorporat. Agentul încorporat trimite telemetrie către serverele soluțiilor și efectuează acțiuni Răspuns la amenințare. Agentul încorporat acceptă:

- 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) versiunea 7.1 sau o versiune anterioară
  - Network Detection and Response (NDR)
  - KATA Sandbox
- Kaspersky Endpoint Detection and Response Expert (on-premises)
- Kaspersky Sandbox 2.0

Poți utiliza Kaspersky Endpoint Security cu soluția Detection and Response în diferite configurații, de exemplu, [EDR Optimum+MDR].

Licențiere MDR și EDR Optimum

Kaspersky Endpoint Security acceptă funcționarea soluțiilor Kaspersky Managed Detection and Response (MDR) și Kaspersky Endpoint Detection and Response Optimum (EDR Optimum). Puteți utiliza Kaspersky Endpoint Security cu aceste soluții în diferite configurații și puteți construi un sistem de protecție personalizat care să satisfacă cerințele dvs. specifice. Pentru aceasta, trebuie să achiziționați o licență pentru fiecare dintre soluții. Licența poate acoperi dreptul de a utiliza o singură soluție (de exemplu, doar suplimentul MDR) sau mai multe soluții, suplimentul [EDR Optimum+MDR].

MDR și EDR Optimum acceptă următoarele metode de licențiere:

- Funcționalitatea MDR sau EDR Optimum este acoperită de licența Kaspersky Endpoint Security for Windows.

  Funcționalitatea este disponibilă imediat după activarea Kaspersky Endpoint Security for Windows. Trebuie doar să adăugați o cheie.

- Licențe separate pentru MDR sau EDR Optimum (MDR Add-on, EDR Optimum Add-on, [EDR Optimum+MDR] Add-on).

  Funcționalitatea devine disponibilă după adăugarea unei chei separate pentru MDR Add-on, EDR Optimum Add-on sau [EDR Optimum+MDR] Add-on. Ca rezultat, sunt adăugate două chei pe computer: o cheie pentru Kaspersky Endpoint Security și o cheie pentru MDR sau EDR Optimum. Cheia Kaspersky Endpoint Security trebuie să fie adăugată prima.

Kaspersky Endpoint Security permite adăugarea unei singure *chei active* pentru licențierea soluțiilor MDR și EDR Optimum. Prin urmare, dacă trebuie să activați ambele soluții, trebuie să adăugați o cheie [EDR Optimum+MDR] Add-on Add-on în loc de o cheie separată pentru fiecare soluție. De asemenea, puteți adăuga o *chei de rezervă*.

Dacă ați folosit un fișier BLOB la implementarea soluției MDR, nu aveți nevoie de o cheie separată pentru a activa soluția MDR. Fișierul BLOB conține deja informații despre licență.

Licențierea inițială a soluțiilor

La prima implementare a soluțiilor MDR și EDR Optimum, acestea sunt activate în același mod ca aplicația Kaspersky Endpoint Security. Puteți adăuga o cheie folosind activitatea *Adaugă cheie* sau puteți utiliza funcționalitatea de distribuție automată a cheilor. Cheia de licență este adăugată la aplicație ca a doua cheie activă sau ca cheie de rezervă dacă bifați caseta de selectare corespunzătoare.

Comutarea de la o licență la alta

Dacă organizația dvs. are deja implementată una dintre aceste soluții și cheia corespunzătoare a fost adăugată la aplicație, există câteva considerații speciale implicate în acordarea licenței noii configurații. Când comutați la o altă licență, aplicația nu adaugă noua cheie în aplicație, ci înlocuiește cheia curentă cu noua cheie. Motivul acestui lucru este restricția care permite aplicației să adauge o singură cheie pentru a activa soluțiile MDR și EDR Optimum.

De exemplu, să presupunem că organizația dvs. are soluția [[EDR Optimum+MDR] implementată și ați decis să comutați la configurația MDR Add-on. Pentru a comuta la noua configurație, trebuie să înlocuiți cheia [EDR Optimum+MDR] Add-on cu cheia MDR Add-on.

O licență separată pentru EDR Optimum și MDR ([EDR Optimum+MDR] Add-on) nu mai este disponibilă. Dacă doriți să utilizați ambele soluții, trebuie să activați soluția MDR folosind un fișier BLOB și EDR Optimum cu o cheie de licență.

Cu funcția de distribuire automată a cheilor, aplicația respinge cheile de licență care acoperă același număr de soluții. Adică, dacă ați adăugat o cheie EDR Optimum Add-on, nu puteți înlocui această cheie cu o cheie MDR Add-on. Cu toate acestea, puteți înlocui cheia EDR Optimum Add-on cu o cheie [EDR Optimum+MDR] Add-on. Aplicația respinge, de asemenea, cheile dacă încercați să înlocuiți o cheie MDR Add-on cu o cheie EDR Add-on. Pentru a înlocui o cheie, puteți executa activitatea *Adaugă cheie*. Activitatea *Adaugă cheie* permite înlocuirea cheilor de licență cu orice număr de soluții.

Dacă ai adăugat o cheie de rezervă [EDR Optimum+MDR] Add-on, pentru a adăuga corect o cheie activă pentru EDR Optimum Add-on sau MDR Add-on, trebuie mai întâi să înlocuiești cheia de rezervă cu o cheie EDR Optimum Add-on sau MDR Add-on sau, alternativ, să elimini cheia de rezervă și apoi să înlocuiești cheia activă.

Compatibilitatea cu soluțiile EDR terțe

Puteți utiliza Kaspersky Endpoint Security pentru a proteja stațiile de lucru și serverele împreună cu soluții EDR terțe. Pentru a elimina alertele false, vă recomandăm să adăugați fișierele executabile ale Kaspersky Endpoint Security și Network Agent în zona de încredere a soluției EDR terțe.

Zonă de încredere pentru compatibilitatea cu soluțiile EDR terțe

	Kaspersky Endpoint Security for Windows	Kaspersky Security Center Network Agent
Director de lucru	`C:\Program Files (x86)\Kaspersky Lab\KES.14.1.0`	`C:\Program Files (x86)\Kaspersky Lab\NetworkAgent`

Fișiere executabile	`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 acceptă interacțiunea dintre aplicație și alte soluții Kaspersky pentru detectarea amenințărilor avansate (de ex. Kaspersky Sandbox). Soluțiile Kaspersky sunt compatibile cu versiunile specifice ale Kaspersky Endpoint Agent.

Pentru a utiliza Kaspersky Endpoint Agent ca parte a soluțiilor Kaspersky, trebuie să activați acele soluții cu o cheie de licență corespunzătoare.

Pentru informații complete despre componenta Kaspersky Endpoint Agent inclusă în soluția software pe care o utilizați și pentru informații complete despre soluțiile independente, consultați Ghidul de ajutor al produsului relevant:

- Ajutor pentru Kaspersky Anti Targeted Attack Platform
- Ajutor pentru Kaspersky Sandbox
- Ghid de ajutor Endpoint Detection and Response Optimum
- Ghid de ajutor Kaspersky Managed Detection and Response

Kitul de distribuție pentru versiunile Kaspersky Endpoint Security versiunile 11.2.0 – 11.8.0 include Kaspersky Endpoint Agent. Puteți selecta Kaspersky Endpoint Agent în timpul instalării Kaspersky Endpoint Security for Windows. Ca rezultat, două aplicații vor fi instalate pe computer: KEA și KES. În Kaspersky Endpoint Security 11.9.0, pachetul de distribuție Kaspersky Endpoint Agent nu mai face parte din kitul de distribuție al Kaspersky Endpoint Security.

Corespondența versiunilor KEA (ca parte a KES) cu versiunile KES

Kaspersky Endpoint Security for 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 comută toate soluțiile Detection and Response pentru a funcționa cu agentul încorporat Kaspersky Endpoint Security în loc de Kaspersky Endpoint Agent. Kaspersky adaugă treptat suport pentru aceste soluții și elimină treptat Kaspersky Endpoint Agent (vezi tabelul de mai jos). Începând cu versiunea 12.1, aplicația acceptă toate soluțiile Detection and Response. În plus, începând cu versiunea 12.1, aplicația nu mai este compatibilă cu Kaspersky Endpoint Agent, iar instalarea ambelor aplicații pe același computer nu mai este posibilă.

Versiunea Kaspersky Endpoint Security	Kaspersky Managed Detection and Response	Kaspersky Sandbox	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Endpoint Detection and Response Expert	Kaspersky Anti Targeted Attack Platform (componenta Endpoint Detection and Response)	Kaspersky Anti Targeted Attack Platform (componenta Network Detection and Response)
11.5.0	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.6.0	**Agent încorporat**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.7.0	**Agent încorporat**	**Agent încorporat**	**Agent încorporat**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.8.0	**Agent încorporat**	**Agent încorporat**	**Agent încorporat**	**Agent încorporat**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.9.0	**Agent încorporat**	**Agent încorporat**	**Agent încorporat**	**Agent încorporat**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.10.0	**Agent încorporat**	**Agent încorporat**	**Agent încorporat**	**Agent încorporat**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.11.0	**Agent încorporat**	**Agent încorporat**	**Agent încorporat**	**Agent încorporat**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12	**Agent încorporat**	**Agent încorporat**	**Agent încorporat**	**Agent încorporat**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12.1	**Agent încorporat**	**Agent încorporat**	**Agent încorporat**	**Agent încorporat**	**Agent încorporat**	Kaspersky Endpoint Agent
12.6	**Agent încorporat**	**Agent încorporat**	**Agent încorporat**	**Agent încorporat**	**Agent încorporat**	**Agent încorporat**

Migrarea configurării [KES+KEA] la [KES+built-in agent]

Kaspersky Endpoint Security include un agent încorporat pentru lucrul cu soluțiile Detection and Response. Nu mai aveți nevoie de aplicația Kaspersky Endpoint Agent pentru a utiliza aceste soluții. Când implementați Kaspersky Endpoint Security pe computere care au instalat Kaspersky Endpoint Agent, soluțiile Detection and Response vor continua să funcționeze cu Kaspersky Endpoint Security. În plus, Kaspersky Endpoint Agent va fi eliminat din computer.

Kitul de distribuție pentru versiunile Kaspersky Endpoint Security versiunile 11.2.0 – 11.8.0 include Kaspersky Endpoint Agent. Puteți selecta Kaspersky Endpoint Agent în timpul instalării Kaspersky Endpoint Security for Windows. Ca rezultat, două aplicații vor fi instalate pe computer: KEA și KES. În Kaspersky Endpoint Security 11.9.0, pachetul de distribuție Kaspersky Endpoint Agent nu mai face parte din kitul de distribuție al Kaspersky Endpoint Security.

Migrarea configurației [KES+KEA] la [KES+agent încorporat] implică pașii următori:

1. **Efectuarea upgrade-ului Kaspersky Security Center**

   Faceți upgrade pentru toate componentele Kaspersky Security Center la versiunea 13.2 sau la o versiune ulterioară, inclusiv Agentul de rețea pe computerele utilizatorului și în Web Console.

2. **Se face upgrade pentru plug-in-ul web Kaspersky Endpoint Security**

   În Kaspersky Security Center Web Console, faceți upgrade pentru plug-in-ul web Kaspersky Endpoint Security la versiunea 11.7.0 sau la o versiune ulterioară. Pentru a gestiona componentele EDR Optimum și Kaspersky Sandbox, trebuie să utilizați componenta Web Console.

Pentru a utiliza Kaspersky Anti Targeted Attack Platform (EDR), veți avea nevoie de un plug-in web pentru Kaspersky Endpoint Security versiunea 12.1 sau o versiune ulterioară.

Pentru a utiliza Kaspersky Anti Targeted Attack Platform (NDR), veți avea nevoie de un plug-in web pentru Kaspersky Endpoint Security versiunea 12.7 sau o versiune ulterioară.

3. **Migrarea politicii și a activităților**

Utilizați Expertul pentru politici și activități al Kaspersky Endpoint Agent pentru a migra setările Kaspersky Endpoint Agent la Kaspersky Endpoint Security for Windows.

Aceasta creează o nouă politică Kaspersky Endpoint Security. Noua politică are starea *Inactive*. Pentru a aplica politica, deschideți proprietățile politicii, acceptați Declarația Kaspersky Security Network și setați-i starea la *Active*.

4. **Funcționalitatea de licențiere**

Dacă folosiți o licență obișnuită Kaspersky Endpoint Detection and Response Optimum sau Kaspersky Optimum Security pentru a activa Kaspersky Endpoint Security for Windows și Kaspersky Endpoint Agent, funcționalitatea EDR Optimum va fi activată automat după efectuarea upgrade-ului aplicației la versiunea 11.7.0. Nu trebuie să faceți nimic.

Dacă folosiți o licență independentă Kaspersky Endpoint Detection and Response Optimum Add-on pentru a activa funcționalitatea EDR Optimum, trebuie să vă asigurați că cheia EDR Optimum Add-on este adăugată la depozitul Kaspersky Security Center și că funcționalitatea de distribuire automată a cheii licenței este activată. După efectuarea upgrade-ului aplicației la versiunea 11.7.0, funcționalitatea EDR Optimum este activată automat.

Dacă folosiți o licență Kaspersky Endpoint Detection and Response Optimum sau Kaspersky Optimum Security pentru a activa Kaspersky Endpoint Agent și o licență diferită pentru a activa Kaspersky Endpoint Security for Windows, trebuie să înlocuiți cheia pentru Kaspersky Endpoint Security for Windows cu o cheie Kaspersky Endpoint Detection and Response Optimum sau Kaspersky Optimum Security. Puteți înlocui cheia utilizând activitatea *Add key*.

Nu trebuie să activați funcționalitatea Kaspersky Sandbox. Funcționalitatea Kaspersky Sandbox va fi disponibilă imediat după efectuarea upgrade-ului și activarea Kaspersky Endpoint Security for Windows.

Numai licența Kaspersky Anti Targeted Attack Platform poate fi utilizată pentru a activa Kaspersky Endpoint Security ca parte a soluției Kaspersky Anti Targeted Attack Platform. După efectuarea upgrade-ului aplicației la versiunea 12.1, funcționalitatea EDR (KATA) este activată automat. Nu trebuie să faceți nimic.

5. **Efectuarea upgrade-ului aplicației Kaspersky Endpoint Security**

> Pentru a efectua upgrade-ul aplicației și a migra funcționalitățile EDR Optimum și Kaspersky Sandbox, este recomandată o activitate de instalare la distanță.

Pentru a efectua upgrade-ul aplicației utilizând o activitate de instalare la distanță, trebuie să editați următoarele setări:

- Selectați componentele pentru soluțiile Detection and Response în setările pachetului de instalare.
- Excludeți componenta Kaspersky Endpoint Agent din setările pachetului de instalare (pentru versiunile Kaspersky Endpoint Security for Windows 11.2.0 – 11.8.0).
- Dacă Protecția prin parolă este activată pentru a restricționa accesul la Kaspersky Endpoint Agent, introduceți parola pentru dezinstalarea aplicației în setările sarcinii *Install application remotely*. Puteți introduce parola de dezinstalare începând cu Kaspersky Security Center Linux 15.1.

De asemenea, puteți face upgrade aplicației utilizând următoarele metode:

- Utilizând serviciul de actualizare Kaspersky (Actualizare fără probleme – SMU).
- Local, folosind Expertul de configurare.

Kaspersky Endpoint Security acceptă selectarea automată a componentelor atunci când se face upgrade-ul unei aplicații pe un computer pe care este instalată aplicația Kaspersky Endpoint Agent. Selectarea automată a componentelor depinde de permisiunile contului de utilizator care face upgrade-ul aplicației.

Dacă faceți upgrade pentru Kaspersky Endpoint Security utilizând fișierul EXE sau MSI din contul de sistem (SYSTEM), Kaspersky Endpoint Security obține acces la licențele curente ale soluțiilor Kaspersky. Prin urmare, dacă pe computer este instalat, de exemplu, Kaspersky Endpoint Agent și soluția EDR Optimum este activată, programul de instalare Kaspersky Endpoint Security configurează automat setul de componente și selectează componenta EDR Optimum. Acest lucru determină componenta Kaspersky Endpoint Security să treacă la utilizarea agentului încorporat și elimină Kaspersky Endpoint Agent. Executarea programului de instalare MSI din contul de sistem (SYSTEM) este efectuată, de obicei, atunci când se face upgrade prin intermediul sistemului de actualizare Kaspersky (SMU) sau când se implementează un pachet de instalare prin Kaspersky Security Center.

Dacă faceți upgrade pentru Kaspersky Endpoint Security utilizând un fișier MSI dintr-un cont de utilizator fără privilegii, Kaspersky Endpoint Security nu obține acces la licențele curente ale soluțiilor Kaspersky. În acest caz, Kaspersky Endpoint Security selectează automat componentele pe baza configurației Kaspersky Endpoint Agent. Ulterior, componenta Kaspersky Endpoint Security comută la utilizarea agentului încorporat și elimină Kaspersky Endpoint Agent.

6. **Repornire computer**

   Reporniți computerul pentru a finaliza actualizarea aplicației cu agentul încorporat. La efectuarea upgrade-ului aplicației, programul de instalare elimină Kaspersky Endpoint Agent înainte de repornirea computerului. După ce computerul este repornit, programul de instalare adaugă agentul încorporat. Aceasta înseamnă că Kaspersky Endpoint Security nu îndeplinește funcțiile EDR și Kaspersky Sandbox până când computerul este repornit.

7. **Verificarea stării componentelor Kaspersky Endpoint Detection and Response Optimum și Kaspersky Sandbox**

   Dacă după upgrade componenta are starea *Critical* în consola Kaspersky Security Center:

   - asigurați-vă că Agentul de rețea versiunea 13.2 sau o versiune ulterioară este instalată pe computer.
   - Verificați starea de funcționare a agentului încorporat, vizualizând *Report on status of application components*. Dacă o componentă are starea *Not installed*, instalați componenta, utilizând activitatea *Change application components*.
   - Asigurați-vă că acceptați Declarația Kaspersky Security Network în noua politică a Kaspersky Endpoint Security for Windows.

   - Asigurați-vă că funcționalitatea EDR Optimum este activată utilizând *Report on status of application components*. Dacă o componentă are starea *Nu este acoperită de licență*, asigurați-vă că funcționalitatea de distribuire automată a cheii de licență a componentei EDR Optimum este activată.

Migrarea politicilor și activităților pentru Kaspersky Endpoint Agent

Kaspersky Endpoint Security include acum un expert pentru migrarea de la Kaspersky Endpoint Agent la Kaspersky Endpoint Security. Puteți migra setările politicii și sarcinilor pentru următoarele soluții:

- Kaspersky Sandbox
- Kaspersky Endpoint Detection and Response Optimum (EDR Optimum)
- Kaspersky Anti Targeted Attack Platform

Un expert pentru migrarea de la Kaspersky Endpoint Agent la Kaspersky Endpoint Security funcționează numai în Web Console și Cloud Console. În Consola de administrare (MMC), poți doar să migrezi setările pentru soluția Kaspersky Anti Targeted Attack Platform (EDR) utilizând expertul de migrare standard pentru politicile și activitățile Kaspersky Security Center.

Este recomandat să începeți cu migrarea Kaspersky Endpoint Agent la Kaspersky Endpoint Security pe un singur computer, apoi să o faceți pe un grup de computere și apoi să finalizați migrarea pe toate computerele organizației.

Pentru a migra setările politicilor și ale activităților de la Kaspersky Endpoint Agent la Kaspersky Endpoint Security,

În fereastra principală a Web Console, selectați **Operations** → **Migration from Kaspersky Endpoint Agent**.

Aceasta execută Expertul de migrare a politicilor și activităților. Urmează instrucțiunile din expert.

Pasul 1. Migrarea politicii

Expertul de migrare creează o nouă politică ce combină setările politicilor Kaspersky Endpoint Security și Kaspersky Endpoint Agent. În lista de politici, selectați politicile Kaspersky Endpoint Agent ale căror setări doriți să le îmbinați cu politica Kaspersky Endpoint Security. Faceți clic pe politica Kaspersky Endpoint Agent pentru a selecta Kaspersky Endpoint Security cu care doriți să îmbinați setările. Asigurați-vă că ați selectat politicile corecte și treceți la pasul următor.

Pasul 2. Migrarea activităților

Expertul pentru migrare creează noi activități pentru Kaspersky Endpoint Security. În lista de activități, selectați activitățile Kaspersky Endpoint Agent pe care doriți să le creați pentru politica Kaspersky Endpoint Security. Expertul acceptă activități pentru soluțiile Kaspersky Endpoint Detection and Response și Kaspersky Sandbox. Mergeți la pasul următor.

Pasul 3. Finalizarea expertului

Ieșiți din Expert. Ca rezultat, expertul efectuează următoarele acțiuni:

- Creează o nouă politică Kaspersky Endpoint Security.

  Politica va combina setările de la Kaspersky Endpoint Security și Kaspersky Endpoint Agent. Politica se numește *<Kaspersky Endpoint Security policy name> & <Kaspersky Endpoint Agent policy name>*. Noua politică are starea *Inactive*. Pentru a continua, modificați stările politicilor Kaspersky Endpoint Agent și Kaspersky Endpoint Security în *Inactive* și activați noua politică îmbinată.

  După migrarea de la Kaspersky Endpoint Agent la Kaspersky Endpoint Security for Windows, asigurați-vă că noua politică are setarea funcționalitatea pentru transferul datelor către Serverul de administrare (date despre fișierul carantină și date despre lanțul de dezvoltare a amenințării). Valorile parametrului pentru transferul de date nu sunt migrate dintr-o politică Kaspersky Endpoint Agent.

  Când se realizează migrarea de la Kaspersky Endpoint Agent la Kaspersky Endpoint Security pentru soluția Kaspersky Anti Targeted Attack Platform (EDR), este posibil să întâmpinați erori atunci când conectați computerul la serverele Central Node. Motivul îl constituie faptul că expertul de migrare Web Console omite următoarele setări ale politicii și nu le migrează:

  - Interzicerea modificării setărilor **Connection to KATA servers** („lacăt").

    În mod implicit, setările pot fi modificate („lacătul" este deschis). Prin urmare, setările nu sunt aplicate pe computer. Trebuie să interziceți modificarea setărilor și să închideți „lacătul".

  - Crypto-container.

    Dacă utilizați autentificarea mutuală pentru conectarea la serverele Central Node, trebuie să adăugați din nou cripto-containerul. Expertul de migrare migrează corect certificatul TLS pe server.

  Expertul de migrare a politicii și activității în Consola de administrare (MMC) migrează toate setările pentru soluția Kaspersky Anti Targeted Attack Platform (EDR).

- Creează noi activități de Kaspersky Endpoint Security.

  Activitățile noi sunt copii ale activităților Kaspersky Endpoint Agent pentru soluțiile Kaspersky Endpoint Detection and Response și Kaspersky Sandbox. În același timp, Expertul lasă activitățile componentei Kaspersky Endpoint Agent neschimbate.

Cum se migrează setările politicii și ale activității de la Kaspersky Endpoint Agent la Kaspersky Endpoint Security în Consola de administrare (MMC) (numai pentru KATA (EDR))

1. În Consola de administrare, selectați Server de administrare și faceți clic dreapta pentru a deschide meniul contextual.
2. Selectați **All tasks** → **Policies and tasks batch conversion wizard**.

Expertul de conversie în loturi a politicilor și activităților va începe. Urmează instrucțiunile din expert.

Pasul 1. Selectarea aplicației pentru care doriți să convertiți politicile și activităților

La acest pas, trebuie să selectați Kaspersky Endpoint Security for Windows. Mergeți la pasul următor.

Pasul 2. Conversia politicilor

Expertul de migrare creează o nouă politică Kaspersky Endpoint Security în care vor fi migrate setările politicii Kaspersky Endpoint Agent. În lista de politici, selectați politicile Kaspersky Endpoint Agent ale căror setări doriți să le transferați în politica Kaspersky Endpoint Security. Mergeți la pasul următor.

Expertul de migrare va începe apoi să efectueze conversia politicilor. În timpul conversiei politicii, Expertul de migrare vă solicită să acceptați Declarația Kaspersky Security Network. Noile politici vor fi denumite *<Nume politică> (convertită)*.

Pasul 3. Conversia activităților

Sari peste acest pas. Expertul acceptă activități pentru soluțiile Kaspersky Endpoint Detection and Response Optimum și Kaspersky Sandbox. Gestionarea acestor componente este disponibilă numai în Web Console. Mergeți la pasul următor.

Pasul 4. Finalizarea expertului

Ieșiți din Expert. În urma utilizării expertului, va fi creată o nouă politică Kaspersky Endpoint Security.

Endpoint Detection and Response Agent (EDR Agent)

Începând cu Kaspersky Endpoint Security 12.3 for Windows, aplicația include configurația Endpoint Detection and Response Agent (EDR Agent). *Endpoint Detection and Response Agent* este o aplicație care este instalată pe stațiile de lucru și pe serverele individuale din infrastructura IT a organizației pentru a susține următoarele soluții Detection and Response de la Kaspersky:

- Kaspersky Managed Detection and Response
- Kaspersky Anti Targeted Attack Platform (EDR)
- Kaspersky Unified Monitoring and Analysis Platform (KUMA) (începând cu versiunea 12.6)

- Kaspersky Anti Targeted Attack Platform (NDR) (începând cu versiunea 12.7)
- Kaspersky Endpoint Detection and Response Expert (on-premises) (începând cu versiunea 12.11)

EDR Agent nu acceptă integrarea cu soluția Kaspersky Endpoint Detection and Response Expert (cloud).

EDR Agent monitorizează continuu procesele care execută pe aceste computere, conexiunile de rețea deschise și fișierele modificate. Componentele de protecție și control ale aplicației nu sunt disponibile pentru EDR Agent.

EDR Agent este compatibil cu aplicațiile EPP terțe. Acest lucru vă permite să utilizați instrumente de securitate ale infrastructurii terțe alături de Detection and Response de la Kaspersky.

Pentru a implementa EDR Agent, computerul trebuie să aibă instalat Agentul de rețea, iar computerul trebuie adăugat în consola Kaspersky Security Center. Pentru a activa interacțiunea EDR Agent cu Kaspersky Security Center, trebuie să instalați plug-inul de gestionare Kaspersky Endpoint Security for Windows. Puteți specifica setările EDR Agent utilizând o politică de grup. Pentru a integra EDR Agent, trebuie să configurați integrarea în secțiunile corespunzătoare ale politicii.

Următoarele aplicații Kaspersky trebuie instalate pe infrastructură pentru a accepta soluțiile Kaspersky Detection and Response:

	• Agent de rețea • EDR Agent
Endpoint	
	Plug-inul de gestionare Kaspersky Endpoint Security for Windows
Kaspersky Security Center	
	
Soluțiile Detection and Response: MDR, KATA (EDR), KATA (NDR), KUMA, EDR Expert (on-premises)	

Instalarea EDR Agent

Kaspersky Endpoint Security în configurația Endpoint Detection and Response Agent (EDR Agent) pentru soluțiile Kaspersky Detection and Response se instalează în același mod.

EDR Agent poate fi instalat pe un computer în unul dintre următoarele moduri:

- De la distanță, folosind Kaspersky Security Center.
- Local, folosind Expertul de configurare.
- Local, în linia de comandă (doar pentru KATA (EDR) și EDR Expert (on-premises)).

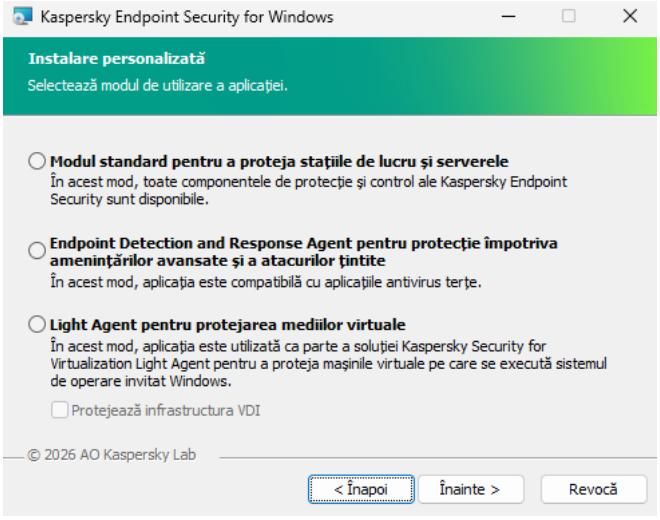
Pentru a instala EDR Agent, trebuie să selectați configurația corespunzătoare în setările pachetului de instalare sau în Expertul de configurare.

Cum se instalează EDR Agent utilizând Expertul de configurare

1. Copiați folderul kitului de distribuire pe computerul utilizatorului.
2. Rulați setup_kes.exe.

   Expertul de instalare pornește.

Configurarea Kaspersky Endpoint Security



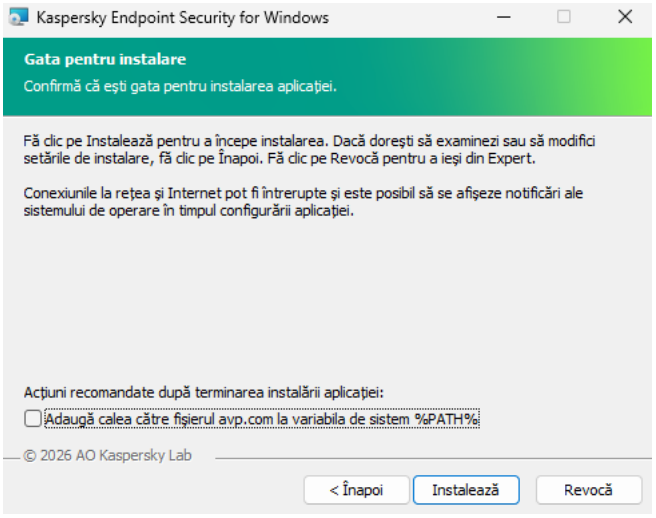
Alegerea configurației aplicației

Selectați configurația **Endpoint Detection and Response Agent**. În această configurație, puteți instala doar componentele care oferă suport pentru soluțiile Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), precum și KUMA. Această configurație este necesară dacă o platformă Endpoint Protection Platform (EPP) terță este implementată în organizație împreună cu soluția Kaspersky Detection and Response. Acest lucru face ca Kaspersky Endpoint Security în configurația Endpoint Detection and Response Agent să fie compatibil cu aplicațiile EPP terțe.

Componentele Kaspersky Endpoint Security

Selectați componentele pe care doriți să le instalați. Puteți schimba componentele disponibile ale aplicației după instalarea aplicației. Pentru a face acest lucru, trebuie să executați din nou Expertul de configurare și să alegeți să schimbați componentele disponibile.

Setări avansate



Setări avansate pentru instalarea aplicației

Protejează procesul de instalare a aplicației. Protejarea instalării include protecția împotriva înlocuirii pachetului de distribuție cu aplicații rău intenționate, blocarea accesului la directorul de instalare al aplicației Kaspersky Endpoint Security și blocarea accesului la secțiunea de registre a sistemului care conține cheile aplicației. Cu toate acestea, dacă aplicația nu poate fi instalată (de exemplu, atunci când se execută o instalare la distanță cu ajutorul Windows Remote Desktop), te sfătuim să dezactivezi protecția procesului de instalare.

Asigură compatibilitatea cu Citrix PVS. Poți activa suportul pentru Citrix Provisioning Services pentru a instala aplicația Kaspersky Endpoint Security pe o mașină virtuală.

Adaugă calea către fișierul avp.com la variabila de sistem %PATH%. Poți adăuga calea de instalare la variabila %PATH% pentru utilizarea comodă a interfeței liniei de comandă.

Cum se instalează EDR Agent în linia de comandă (numai pentru KATA (EDR) și EDR Expert (on-premises))

1. Executați interpretorul de linii de comandă (cmd.exe) ca administrator.
2. Deschide directorul în care se află pachetul de distribuție pentru Kaspersky Endpoint Security.
3. Execută următoare comandă:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pSTANDALONEMODE=1 [/s]
```

sau

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 STANDALONEMODE=1 [/qn]
```

Drept urmare, aplicația EDR Agent pentru integrarea cu Kaspersky Anti Targeted Attack Platform (EDR) sau Kaspersky Endpoint Detection and Response Expert (on-premises) este instalată pe computer. Poți confirma faptul că aplicația este instalată și să verifici setările aplicației inițiind comanda `status`.

Cum se instalează EDR Agent utilizând Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectează directorul **Advanced** → **Remote installation** → **Installation packages**.

   Aceasta deschide o listă cu pachetele de instalare care au fost descărcate în Kaspersky Security Center.
3. Deschideți proprietățile pachetului de instalare.

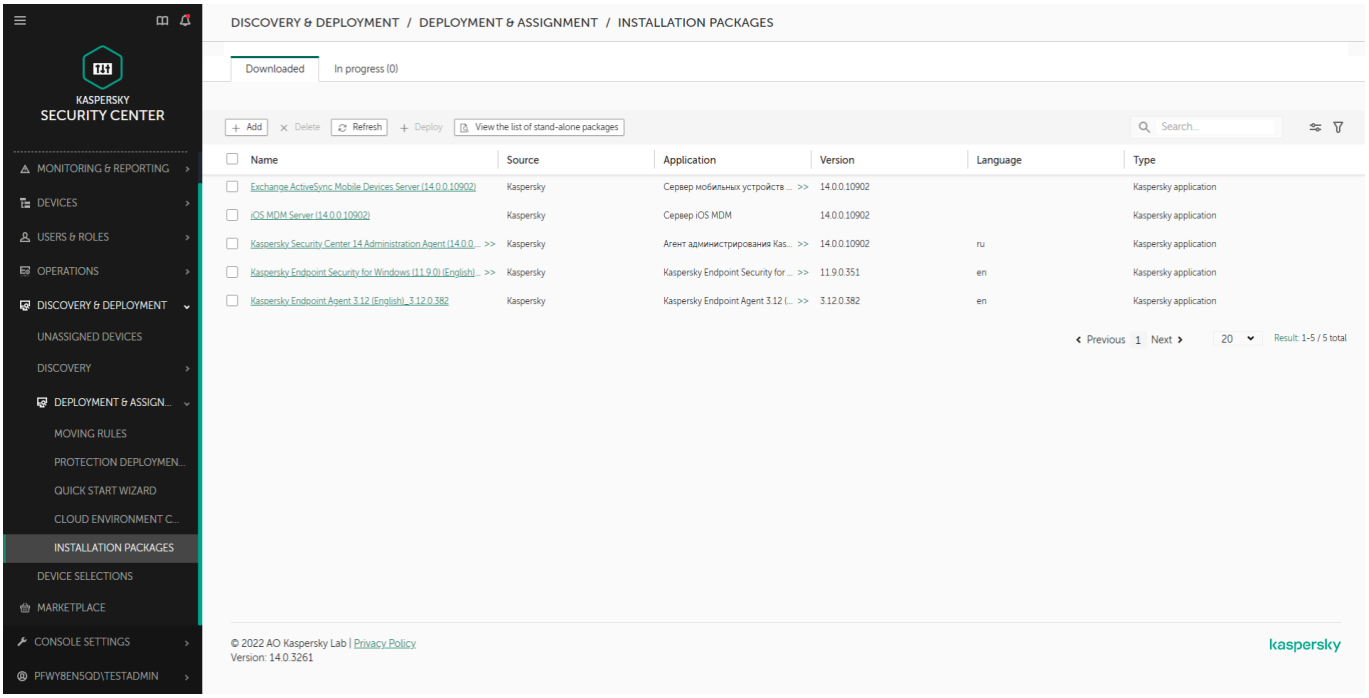
   Daca este necesar, creați un nou pachet de instalare.
4. Accesează secțiunea **Protection components**.
5. Selectați configurația **Endpoint Detection and Response Agent pentru protecție împotriva amenințărilor avansate și a atacurilor țintite**. În această configurație, puteți instala doar componentele care oferă suport pentru soluțiile Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), precum și KUMA. Această configurație este necesară dacă o platformă Endpoint Protection Platform (EPP) terță este implementată în organizație împreună cu soluția Kaspersky Detection and Response. Acest lucru face ca Kaspersky Endpoint Security în configurația Endpoint Detection and Response Agent să fie compatibil cu aplicațiile EPP terțe.
6. Selectați componentele pe care doriți să le instalați.

   Puteți schimba componentele disponibile ale aplicației după instalarea aplicației.
7. Salvați-vă modificările.
8. Creați unui pachet de instalare la distanță. În proprietățile activității, selectați pachetul de instalare pe care l-ați creat.

Cum se instalează EDR Agent utilizând Web Console

1. În fereastra principală a componentei Web Console, selectați **Discovery & deployment** → **Deployment & assignment** → **Installation packages**.

   Aceasta deschide o listă cu pachetele de instalare care au fost descărcate în Kaspersky Security Center.



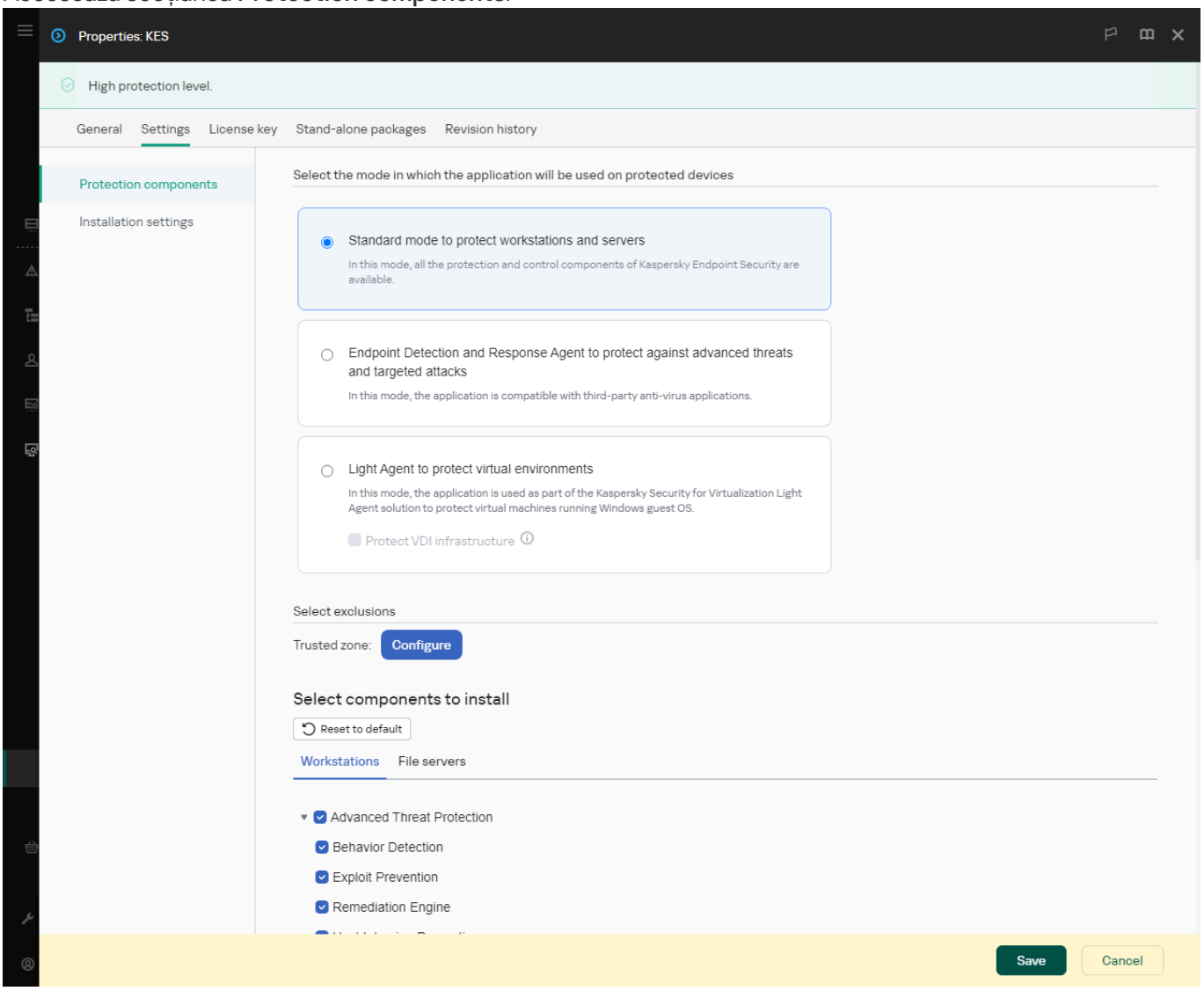
Lista pachetelor de instalare

2. Deschideți proprietățile pachetului de instalare.

   Daca este necesar, creați un nou pachet de instalare.

3. Selectați fila **Settings**.

4. Accesează secțiunea **Protection components**.



Componente incluse în pachetul de instalare

5. Selectați configurația **Endpoint Detection and Response Agent to protect against advanced threats and targeted attacks**. În această configurație, puteți instala doar componentele care oferă suport pentru soluțiile Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), precum și KUMA. Această configurație este necesară dacă o platformă Endpoint Protection Platform (EPP) terță este implementată în organizație împreună cu soluția Kaspersky Detection and Response. Acest lucru face ca Kaspersky Endpoint Security în configurația Endpoint Detection and Response Agent să fie compatibil cu aplicațiile EPP terțe.

6. Selectați componentele pe care doriți să le instalați.

   Puteți schimba componentele disponibile ale aplicației după instalarea aplicației.

7. Salvați-vă modificările.

8. Creați unui pachet de instalare la distanță. În proprietățile activității, selectați pachetul de instalare pe care l-ați creat.

Drept rezultat, EDR Agent este instalat pe computerul utilizatorului. Puteți utiliza interfața aplicației și o pictogramă a aplicației este afișată în zona de notificare .

În Kaspersky Security Center, computerul cu aplicația instalată în configurația EDR Agent are starea *Critical* - . Computerul are această stare deoarece componenta File Threat Protection lipsește. Nu trebuie să întreprindeți nicio acțiune.

Dacă nu ați putut instala EDR Agent pe un computer cu o aplicație EPP terță, deoarece programul de instalare a găsit un software incompatibil pe computer, puteți sări peste verificarea software-ului incompatibil.



Fereastra principală a EDR Agent

Acum trebuie să configurați integrarea cu soluția Kaspersky Managed Detection and Response, Kaspersky Anti Targeted Attack (EDR) sau cu Kaspersky Anti Targeted Attack (NDR). De asemenea, puteți specifica setări avansate ale aplicației și, de exemplu, puteți crea o zonă de încredere sau puteți ascunde interfața aplicației. Sunt disponibile setările din următoarele secțiuni:

- Kaspersky Security Network
- Setări aplicație
- Setări rețea
- Excluderi
- Rapoarte

- Interfață
- Gestionare setări

Integrarea EDR Agent cu MDR

EDR Agent este instalat pe stațiile de lucru și serverele din infrastructura IT a organizației. EDR Agent procesează datele și le trimite prin fluxurile Kaspersky Security Network către Kaspersky Managed Detection and Response.

Pentru funcționarea Kaspersky Managed Detection and Response cu Serverul de administrare prin intermediul Kaspersky Security Center Web Console, trebuie să stabilești o nouă conexiune securizată, o *conexiune în fundal*. Kaspersky Managed Detection and Response vă solicită să stabiliți o conexiune de fundal atunci când implementați soluția. Asigurați-vă că este stabilită conexiunea de fundal.

Stabilirea unei conexiuni de fundal în Consola Web

1. În fereastra principală a Web Console, selectați **Settings** → **Integration**.
2. Accesează secțiunea **Integration**.
3. Duceți comutatorul **Background connection for integration Enabled** la poziția activat.
4. Salvați-vă modificările.

Integrarea cu Kaspersky Managed Detection and Response constă în următorii pași:

1. **Instalarea componentei Managed Detection and Response**

   Poți selecta componenta MDR în timpul instalării sau efectuării upgrade-ului, precum și utilizând activitatea *Modificare componente ale aplicației*.

   > Pentru a instala componenta Managed Detection and Response fără a reporni computerul utilizând activitatea *Modificare componente ale aplicației*, trebuie să dezactivezi opțiunea **Verifică aplicațiile terțe incompatibile** în setările activității.

2. **Configurarea Kaspersky Private Security Network**

   > Omiteți acest pas dacă utilizați Kaspersky Security Center Cloud Console. Kaspersky Security Center Cloud Console configurează automat componenta Kaspersky Private Security Network când se instalează plug-in-ul MDR.

   Kaspersky Private Security Network (KPSN) este o soluție care permite utilizatorilor de computere care găzduiesc Kaspersky Endpoint Security sau alte aplicații Kaspersky să obțină acces la bazele de date privind reputația ale Kaspersky și la alte date statistice, fără a trimite date către Kaspersky de la propriile lor computere.

   Încărcați fișierul de configurare Kaspersky Security Network în proprietățile Serverului de administrare. Fișierul de configurare al Kaspersky Security Network se află în arhiva ZIP a fișierului de configurare MDR. Puteți obține arhiva ZIP în Consola Kaspersky Managed Detection and Response. Pentru detalii privind configurarea componentei Kaspersky Private Security Network, consultați Ajutor pentru Kaspersky Security Center. De asemenea, puteți încărca un fișier de configurare Kaspersky Security Network în computer, din linia de comandă (consultați instrucțiunile de mai jos).

Cum se configurează Kaspersky Private Security Network din linia de comandă

1. Executați interpretorul de linii de comandă (cmd.exe) ca administrator.
2. Deschideți directorul în care se află fișierul executabil Kaspersky Endpoint Security.
3. Execută următoare comandă:

```
avp.com KSN /private <file name>
```

unde `<file name>` este numele fișierului de configurare care conține setările componentei Kaspersky Private Security Network (format fișier PKCS7 sau PEM).

Exemplu:
`avp.com KSN /private C:\kpsn_config.pkcs7`

Ca rezultat, Kaspersky Endpoint Security va utiliza componenta Kaspersky Private Security Network pentru a determina reputația fișierelor, aplicațiilor și site-urilor web. Secțiunea **Kaspersky Security Network** din setările politicii va afișa următoarea stare de funcționare: *Infrastructură: Kaspersky Private Security Network*.

Trebuie să activați modul KSN extins pentru ca Managed Detection and Response să funcționeze.

3 Activarea funcționalității Kaspersky Managed Detection and Response

Începând cu Kaspersky Endpoint Security for Windows 12.10, pentru a activa funcționalitatea Managed Detection and Response, ca alternativă la uno cod de activare, poți folosi și un fișier cheie.

Trebuie să achiziționezi o licență separată pentru MDR (suplimentul Kaspersky Managed Detection and Response).

Funcționalitatea devine disponibilă după adăugarea unei chei separate pentru suplimentul Kaspersky Managed Detection and Response. Licențierea funcționalității autonome Managed Detection and Response se realizează la fel ca licențierea componentei Kaspersky Endpoint Security.

Asigurați-vă că funcționalitatea componentei MDR este inclusă în licență și că aceasta funcționează în interfața locală a aplicației.

4 Activarea componentei Managed Detection and Response

Încărcați fișierul de configurare BLOB în politica Kaspersky Endpoint Security (consultați instrucțiunile de mai jos). Fișierul BLOB conține Id-ul clientului și informații despre licența pentru componenta Kaspersky Managed Detection and Response. Fișierul BLOB se află în arhiva ZIP a fișierului de configurare MDR. Puteți obține arhiva ZIP în Consola Kaspersky Managed Detection and Response. Pentru informații detaliate despre un fișier BLOB, consultați Ajutorul Kaspersky Managed Detection and Response.

Începând cu Kaspersky Endpoint Security 12.6 for Windows, adăugarea unui fișier BLOB este opțională pentru Kaspersky Managed Detection and Response fără entități găzduite, dacă aveți o licență actuală.

Cum se activează componenta Managed Detection and Response în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Detection and Response → Managed Detection and Response (Industrial CyberSecurity)**.
4. Bifați caseta de selectare **Managed Detection and Response (Industrial CyberSecurity)**.

5. În blocul **Setări**, faceți clic pe **Încărcare** și selectați fișierul BLOB primit în Kaspersky Managed Detection and Response Console. Fișierul are extensia P7.

   În mod implicit, utilizatorului i se permite să gestioneze setările aplicației („lacătul" este deschis). Pentru a aplica politica pe computere, închide lacătele.

6. Salvați-vă modificările.

Cum se activează componenta Managed Detection and Response în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.
4. Accesați **Built-in Agents Configuration** → **Managed Detection and Response**.
5. Duceți comutatorul **Managed Detection and Response ENABLED** la poziția activat.
6. Faceți clic pe **Upload** și selectați fișierul BLOB care a fost obținut în Kaspersky Managed Detection and Response Console. Fișierul are extensia P7.

   În mod implicit, utilizatorului i se permite să gestioneze setările politicii („lacătul" este deschis). Pentru a aplica politica pe computere, închide lacătele.

7. Salvați-vă modificările.

Cum se activează componenta Managed Detection and Response din linia de comandă

1. Executați interpretorul de linii de comandă (cmd.exe) ca administrator.
2. Deschideți directorul în care se află fișierul executabil Kaspersky Endpoint Security.
3. Execută următoare comandă:

```
avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>
```

Pentru a executa această comandă, funcția Protecție prin parolă trebuie activată. Utilizatorul trebuie să aibă permisiunea **Configurează setările aplicației**.

Ca rezultat, Kaspersky Endpoint Security va verifica fișierul BLOB. Verificarea fișierului BLOB include verificarea semnăturii digitale și a termenilor licenței. Dacă fișierul BLOB este verificat cu succes, Kaspersky Endpoint Security va descărca fișierul și îl va trimite către computer în timpul următoarei sincronizări cu Kaspersky Security Center. Verificați starea de funcționare a componentei, vizualizând *Report on status of application components*. De asemenea, puteți vizualiza starea de funcționare a unei componente în rapoarte, în interfața locală a Kaspersky Endpoint Security. Componenta **Managed Detection and Response** va fi adăugată la lista componentelor Kaspersky Endpoint Security.

5 **Configurarea altor componente ale aplicației pentru a primi telemetrie**

Trebuie să activați următoarele componente pentru ca Managed Detection and Response să funcționeze:

- Kaspersky Security Network (modul extins);
- Behavior Detection.
- Exploit Prevention.
- Web Threat Protection.
- Mail Threat Protection.
- File Threat Protection.
- Network Threat Protection.
- Firewall.
- Protecție AMSI.
- Scanare în fundal.

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.
   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Built-in Agents Configuration** → **Managed Detection and Response**.
5. Duceți comutatorul **Managed Detection and Response ENABLED** la poziția activat.
6. Salvați-vă modificările.

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)**.
4. Bifați caseta de selectare **Managed Detection and Response (Industrial CyberSecurity)**.
5. Salvați-vă modificările.

Integrarea EDR Agent cu EDR (KATA)

EDR Agent este instalat pe stațiile de lucru și serverele din infrastructura IT a organizației. Pe aceste computere, EDR Agent monitorizează continuu procesele, conexiunile de rețea deschise și fișierele care sunt modificate și trimite datele de monitorizare către serverul cu componenta Central Node.

Pentru integrarea cu EDR (KATA), trebuie să activați componenta Endpoint Detection and Response (KATA) și să configurați EDR Agent.

Trebuie îndeplinite următoarele condiții pentru ca Endpoint Detection and Response (KATA) să funcționeze:

- Kaspersky Anti Targeted Attack Platform versiunile 5.0–7.1.
- Kaspersky Security Center versiunea 14.2 sau o versiune ulterioară. În versiunile anterioare ale Kaspersky Security Center, este imposibil de activat caracteristica Endpoint Detection and Response (KATA).

https://www.youtube.com/watch?v=cZzgtBoeC7k

Integrarea cu Kaspersky Endpoint Detection and Response (KATA) presupune următorii pași:

1. **Activarea componentei Endpoint Detection and Response (KATA)**

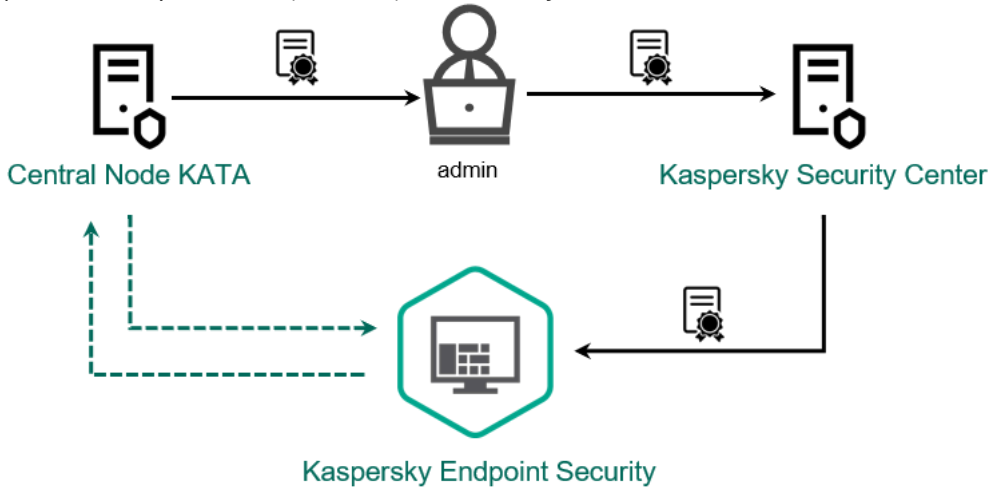
   Trebuie să achiziționați o licență separată pentru EDR (KATA) (suplimentul Kaspersky Endpoint Detection and Response (KATA)).

   Funcționalitatea devine disponibilă după adăugarea unei chei separate pentru Kaspersky Endpoint Detection and Response (KATA). Licențierea funcționalității individuale Endpoint Detection and Response (KATA) se realizează la fel ca licențierea componentei Kaspersky Endpoint Security.

   Asigurați-vă că funcționalitatea componentei EDR (KATA) este inclusă în licență și că aceasta se execută în interfața locală a aplicației.

2. **Conectarea la Central Node**

   Kaspersky Anti Targeted Attack Platform necesită stabilirea unei conexiuni de încredere între Kaspersky Endpoint Security și componenta Central Node. Pentru a configura o conexiune de încredere, trebuie să utilizați un certificat TLS. Puteți obține un certificat TLS în consola Kaspersky Anti Targeted Attack Platform (consultați instrucțiunile din Ajutor Kaspersky Anti Targeted Attack Platform). Apoi, trebuie să adăugați certificatul TLS la Kaspersky Endpoint Security (consultați instrucțiunile de mai jos).



Adăugarea unui certificat TLS la Kaspersky Endpoint Security

În mod implicit, Kaspersky Endpoint Security verifică doar certificatul TLS al componentei Central Node. Pentru a face conexiunea mai sigură, puteți activa suplimentar verificarea computerului în Central Node (autentificare mutuală). Pentru a activa această verificare, trebuie să activați autentificarea mutuală în setările Central Node și Kaspersky Endpoint Security. Pentru a utiliza autentificarea mutuală, veți avea nevoie și de un cripto-container. Un *cripto-container* este o arhivă PFX cu un certificat și o cheie privată. Puteți obține un cripto-container în consola Kaspersky Anti Targeted Attack Platform (consultați instrucțiunile din Ajutor Kaspersky Anti Targeted Attack Platform).

Cum conectați un computer Kaspersky Endpoint Security la Central Node utilizând Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați **Policies**.
3. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
4. În fereastra politicii, selectați **Detection and Response → Endpoint Detection and Response Expert (on-premises)**.
5. Bifați caseta de selectare **Endpoint Detection and Response Expert (on-premises)**.
6. Fă clic pe **Setări conectare server**.
7. Configurați conexiunea la server:
   - **Expirare (sec)**. Expirarea timpului maxim de răspuns al serverului Central Node. Când timpul de expirare se termină, Kaspersky Endpoint Security încearcă să se conecteze la un alt server Central Node.
   - **Certificat TLS server**. Certificat TLS pentru stabilirea unei conexiuni de încredere cu serverul Central Node. Puteți obține un certificat TLS în consola Kaspersky Anti Targeted Attack Platform (consultați instrucțiunile din Ajutor Kaspersky Anti Targeted Attack Platform).
   - **Utilizează autentificarea mutuală**. Autentificare mutuală la stabilirea unei conexiuni securizate între Kaspersky Endpoint Security și serverul Central Node. Pentru a utiliza autentificarea mutuală, trebuie să activezi autentificarea mutuală în setările serverului Central Node, apoi să obții un container crypto și să setezi o parolă pentru a proteja containerul crypto. Un *cripto-container* este o arhivă PFX cu un certificat și o cheie privată. Puteți obține un cripto-container în consola Kaspersky Anti Targeted Attack Platform (consultați instrucțiunile din Ajutor Kaspersky Anti Targeted Attack Platform). După configurarea setărilor Central Node, trebuie să activați și autentificarea mutuală în setările Kaspersky Endpoint Security și să încărcați un container crypto protejat prin parolă.

     Criptocontainerul trebuie să fie protejat prin parolă. Nu este posibil să adăugați un criptocontainer cu o parolă necompletată.
8. Fă clic pe **OK**.
9. Adăugați servere Central Node. Pentru a face acest lucru, specificați adresa serverului (IPv4, IPv6) și portul de conectare la server.

   Poți adăuga mai multe adrese de server Central Node. Kaspersky Endpoint Security încearcă să se conecteze la server la prima adresă IP. Dacă nu se poate stabili o conexiune, Kaspersky Endpoint Security încearcă să se conecteze la a doua adresă IP din listă și așa mai departe.

10. Dacă este necesar, configurează telemetria.

11. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum conectați un computer Kaspersky Endpoint Security la Central Node utilizând Web Console

1. În fereastra principală a Web Console, selectați fila **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (on-premises)**.

5. Duceți comutatorul **Endpoint Detection and Response Expert (on-premises) ENABLED** la poziția activat.

6. Pentru a configura EDR (KATA), selectează **Endpoint Detection and Response Expert (version 7.1 or earlier)** din lista de soluții.

7. Fă clic pe **Connection settings**.

8. Configurați conexiunea la server:

   - **Timeout (sec)**. Expirarea timpului maxim de răspuns al serverului Central Node. Când timpul de expirare se termină, Kaspersky Endpoint Security încearcă să se conecteze la un alt server Central Node.

   - **Server certificate**. Certificat TLS pentru stabilirea unei conexiuni de încredere cu serverul Central Node. Puteți obține un certificat TLS în consola Kaspersky Anti Targeted Attack Platform (consultați instrucțiunile din Ajutor Kaspersky Anti Targeted Attack Platform).

   - **Use two-way authentication**. Autentificare mutuală la stabilirea unei conexiuni securizate între Kaspersky Endpoint Security și serverul Central Node. Pentru a utiliza autentificarea mutuală, trebuie să activezi autentificarea mutuală în setările serverului Central Node, apoi să obții un container crypto și să setezi o parolă pentru a proteja containerul crypto. Un *cripto-container* este o arhivă PFX cu un certificat și o cheie privată. Puteți obține un cripto-container în consola Kaspersky Anti Targeted Attack Platform (consultați instrucțiunile din Ajutor Kaspersky Anti Targeted Attack Platform). După configurarea setărilor Central Node, trebuie să activați și autentificarea mutuală în setările Kaspersky Endpoint Security și să încărcați un container crypto protejat prin parolă.

     Criptocontainerul trebuie să fie protejat prin parolă. Nu este posibil să adăugați un criptocontainer cu o parolă necompletată.

9. Fă clic pe **OK**.

10. Adăugați servere Central Node. Pentru a face acest lucru, specificați adresa serverului (IPv4, IPv6) și portul de conectare la server.

    Poți adăuga mai multe adrese de server Central Node. Kaspersky Endpoint Security încearcă să se conecteze la server la prima adresă IP. Dacă nu se poate stabili o conexiune, Kaspersky Endpoint Security încearcă să se conecteze la a doua adresă IP din listă și așa mai departe.

11. Dacă este necesar, configurează telemetria.

12. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Ca rezultat, computerul este adăugat în consola Kaspersky Anti Targeted Attack Platform. Verificați starea de funcționare a componentei, vizualizând *Report on status of application components*. De asemenea, puteți vizualiza starea de funcționare a unei componente în rapoarte, în interfața locală a Kaspersky Endpoint Security. Componenta **Endpoint Detection and Response Expert (on-premises)** va fi adăugată la lista componentelor Kaspersky Endpoint Security.

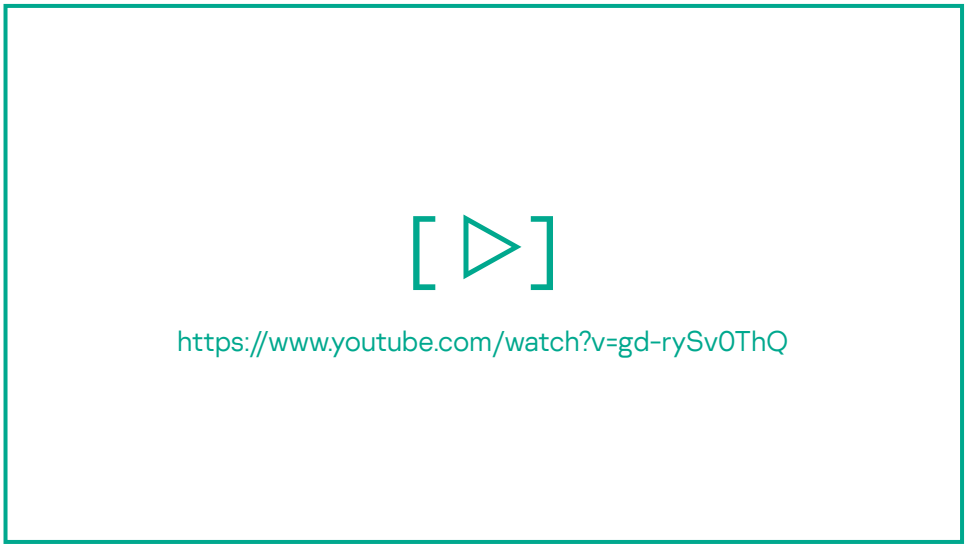
Integrarea EDR Agent cu NDR (KATA)

EDR Agent este instalat pe stațiile de lucru și serverele din infrastructura IT a organizației. Pe aceste computere, EDR Agent monitorizează continuu procesele, conexiunile de rețea deschise și fișierele care sunt modificate și trimite datele de monitorizare către serverul cu componenta Central Node.

Pentru integrarea cu NDR (KATA), trebuie să activați componenta Network Detection and Response (KATA) și să configurați EDR Agent.

Trebuie îndeplinite următoarele condiții pentru ca Network Detection and Response (KATA) să funcționeze:

- Kaspersky Anti Targeted Attack Platform versiunea 7.0 sau o versiune ulterioară.
- Kaspersky Security Center versiunea 14.2 sau o versiune ulterioară. În versiunile anterioare ale Kaspersky Security Center, este imposibil de activat caracteristica Network Detection and Response (KATA).



Integrarea cu Kaspersky Network Detection and Response (KATA) presupune următorii pași:

1. **Activarea componentei Network Detection and Response (KATA)**

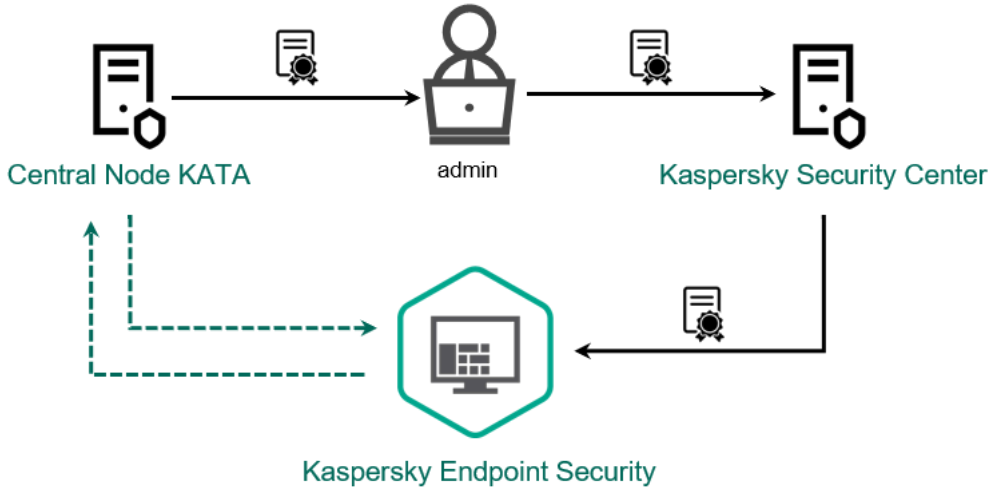
   Trebuie să achiziționați o licență separată pentru NDR (KATA) (suplimentul Kaspersky Network Detection and Response (KATA)).

   Funcționalitatea devine disponibilă după adăugarea unei chei separate pentru Kaspersky Network Detection and Response (KATA). Licențierea funcționalității individuale Network Detection and Response (KATA) se realizează la fel ca licențierea componentei Kaspersky Endpoint Security.

   Asigurați-vă că funcționalitatea componentei NDR (KATA) este inclusă în licență și că aceasta se execută în interfața locală a aplicației.

2. **Conectarea la Central Node**

Kaspersky Anti Targeted Attack Platform necesită stabilirea unei conexiuni de încredere între Kaspersky Endpoint Security și componenta Central Node. Pentru a configura o conexiune de încredere, trebuie să utilizați un certificat TLS. Puteți obține un certificat TLS în consola Kaspersky Anti Targeted Attack Platform (consultați instrucțiunile din Ajutor Kaspersky Anti Targeted Attack Platform). Apoi, trebuie să adăugați certificatul TLS la Kaspersky Endpoint Security (consultați instrucțiunile de mai jos).



Adăugarea unui certificat TLS la Kaspersky Endpoint Security

În mod implicit, Kaspersky Endpoint Security verifică doar certificatul TLS al componentei Central Node. Pentru a face conexiunea mai sigură, puteți activa suplimentar verificarea computerului în Central Node (autentificare mutuală). Pentru a activa această verificare, trebuie să activați autentificarea mutuală în setările Central Node și Kaspersky Endpoint Security. Pentru a utiliza autentificarea mutuală, veți avea nevoie și de un cripto-container. Un *cripto-container* este o arhivă PFX cu un certificat și o cheie privată. Puteți obține un cripto-container în consola Kaspersky Anti Targeted Attack Platform (consultați instrucțiunile din Ajutor Kaspersky Anti Targeted Attack Platform).

Cum conectați un computer Kaspersky Endpoint Security la Central Node utilizând Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Detection and Response** → **Network Detection and Response (KATA)**.
4. Bifați caseta de selectare **Network Detection and Response (KATA)**.
5. Fă clic pe **Connection settings**.
6. Configurați conexiunea la server:

   - **Timeout (sec)**. Expirarea timpului maxim de răspuns al serverului Central Node. Când timpul de expirare se termină, Kaspersky Endpoint Security încearcă să se conecteze la un alt server Central Node.
   - **Server certificate**. Certificat TLS pentru stabilirea unei conexiuni de încredere cu serverul Central Node. Puteți obține un certificat TLS în consola Kaspersky Anti Targeted Attack Platform (consultați instrucțiunile din Ajutor Kaspersky Anti Targeted Attack Platform).

- **Use two-way authentication**. Autentificare mutuală la stabilirea unei conexiuni securizate între Kaspersky Endpoint Security și serverul Central Node. Pentru a utiliza autentificarea mutuală, trebuie să activezi autentificarea mutuală în setările serverului Central Node, apoi să obții un container crypto și să setezi o parolă pentru a proteja containerul crypto. Un *cripto-container* este o arhivă PFX cu un certificat și o cheie privată. Puteți obține un cripto-container în consola Kaspersky Anti Targeted Attack Platform (consultați instrucțiunile din Ajutor Kaspersky Anti Targeted Attack Platform). După configurarea setărilor Central Node, trebuie să activați și autentificarea mutuală în setările Kaspersky Endpoint Security și să încărcați un container crypto protejat prin parolă.

  Criptocontainerul trebuie să fie protejat prin parolă. Nu este posibil să adăugați un criptocontainer cu o parolă necompletată.

7. Fă clic pe **OK**.
8. Adăugați servere Central Node. Pentru a face acest lucru, specificați adresa serverului (IPv4, IPv6) și portul de conectare la server.
9. Poți adăuga mai multe adrese de server Central Node. Kaspersky Endpoint Security încearcă să se conecteze la server la prima adresă IP. Dacă nu se poate stabili o conexiune, Kaspersky Endpoint Security încearcă să se conecteze la a doua adresă IP din listă și așa mai departe.
10. Dacă este necesar, configurează telemetria.
11. Salvați-vă modificările.

Cum conectați un computer Kaspersky Endpoint Security la Central Node utilizând Web Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Built-in Agents Configuration** → **Network Detection and Response (KATA)**.
5. Duceți comutatorul **Network Detection and Response (KATA) ENABLED** la poziția activat.
6. Fă clic pe **Connection settings**.
7. Configurați conexiunea la server:

   - **Timeout (sec)**. Expirarea timpului maxim de răspuns al serverului Central Node. Când timpul de expirare se termină, Kaspersky Endpoint Security încearcă să se conecteze la un alt server Central Node.
   - **Server certificate**. Certificat TLS pentru stabilirea unei conexiuni de încredere cu serverul Central Node. Puteți obține un certificat TLS în consola Kaspersky Anti Targeted Attack Platform (consultați instrucțiunile din Ajutor Kaspersky Anti Targeted Attack Platform).

- **Use two-way authentication**. Autentificare mutuală la stabilirea unei conexiuni securizate între Kaspersky Endpoint Security și serverul Central Node. Pentru a utiliza autentificarea mutuală, trebuie să activezi autentificarea mutuală în setările serverului Central Node, apoi să obții un container crypto și să setezi o parolă pentru a proteja containerul crypto. Un *cripto-container* este o arhivă PFX cu un certificat și o cheie privată. Puteți obține un cripto-container în consola Kaspersky Anti Targeted Attack Platform (consultați instrucțiunile din Ajutor Kaspersky Anti Targeted Attack Platform). După configurarea setărilor Central Node, trebuie să activați și autentificarea mutuală în setările Kaspersky Endpoint Security și să încărcați un container crypto protejat prin parolă.

  Criptocontainerul trebuie să fie protejat prin parolă. Nu este posibil să adăugați un criptocontainer cu o parolă necompletată.

8. Fă clic pe **OK**.
9. Adăugați servere Central Node. Pentru a face acest lucru, specificați adresa serverului (IPv4, IPv6) și portul de conectare la server.
10. Poți adăuga mai multe adrese de server Central Node. Kaspersky Endpoint Security încearcă să se conecteze la server la prima adresă IP. Dacă nu se poate stabili o conexiune, Kaspersky Endpoint Security încearcă să se conecteze la a doua adresă IP din listă și așa mai departe.
11. Dacă este necesar, configurează telemetria.
12. Salvați-vă modificările.

Ca rezultat, computerul este adăugat în consola Kaspersky Anti Targeted Attack Platform. Verificați starea de funcționare a componentei, vizualizând *Report on status of application components*. De asemenea, puteți vizualiza starea de funcționare a unei componente în rapoarte, în interfața locală a Kaspersky Endpoint Security. Componenta **Network Detection and Response (KATA)** va fi adăugată la lista componentelor Kaspersky Endpoint Security.

Integrarea EDR Agent cu EDR Expert (on-premises)

EDR Agent este instalat pe stațiile de lucru și serverele din infrastructura IT a organizației. Pe aceste computere, EDR Agent monitorizează continuu procesele, conexiunile la rețea deschise și fișierele care sunt modificate și trimite datele de monitorizare către serverul EDR Expert (on-premises).

Pentru integrarea cu EDR Expert (on-premises), trebuie să activezi componenta Endpoint Detection and Response Expert (on-premises) și să configurezi EDR Agent.

Integrarea cu Kaspersky Endpoint Detection and Response Expert (on-premises) presupune următorii pași:

1. **Activarea Kaspersky Endpoint Detection and Response Expert (on-premises)**

   Trebuie să achiziționezi o licență separată pentru EDR Expert (on-premises) (suplimentul Kaspersky Endpoint Detection and Response Expert (on-premises)).

   Funcționalitatea devine disponibilă după adăugarea unei chei separate pentru Kaspersky Endpoint Detection and Response Expert (on-premises). Licențierea funcționalității individuale Endpoint Detection and Response Expert (on-premises) se realizează la fel ca licențierea componentei Kaspersky Endpoint Security.

   Asigură-te că funcționalitatea componentei EDR Expert (on-premises) este inclusă în licență și că aceasta se execută în interfața locală a aplicației.

2. **Conectarea la serverul de colectare a telemetriei și la serverul de răspuns**

Kaspersky Endpoint Detection and Response Expert (on-premises) necesită o conexiune de încredere între Kaspersky Endpoint Security și două servere:

- Un *server de colectare a telemetriei* este un server care face parte dintr-o soluție SIEM și care colectează, normalizează, corelează, analizează și stochează informații despre evenimentele care au loc pe computer.
- Un *server de răspuns* este un server pentru primirea și scanarea datelor, studierea comportamentului obiectelor și publicarea rezultatelor acestor studii.

Pentru a configura o conexiune de încredere, trebuie să utilizați un certificat TLS. Poți obține un certificat TLS pe Open Single Management Platform (consultă instrucțiunile din Ajutor pentru Kaspersky Endpoint Detection and Response Expert (on-premises)). Apoi, trebuie să adăugați certificatul TLS la Kaspersky Endpoint Security (consultați instrucțiunile de mai jos).

În mod implicit, Kaspersky Endpoint Security verifică doar certificatul TLS al serverelor. Pentru a face conexiunea mai sigură, poți activa suplimentar verificarea computerului pe server (autentificare mutuală). Pentru a activa această verificare, trebuie să activezi autentificarea mutuală în setările serverului și ale Kaspersky Endpoint Security. Pentru a utiliza autentificarea mutuală, veți avea nevoie și de un cripto-container. Un *cripto-container* este o arhivă PFX cu un certificat și o cheie privată. Poți obține un container crypto pe Open Single Management Platform (consultă instrucțiunile din Ajutor pentru Kaspersky Endpoint Detection and Response Expert (on-premises)).

Cum conectezi un computer Kaspersky Endpoint Security la EDR Expert (on-premises) utilizând Web Console

1. În fereastra principală a Web Console, selectați fila **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (on-premises)**.
5. Duceți comutatorul **Endpoint Detection and Response Expert (on-premises) ENABLED** la poziția activat.
6. Pentru a configura EDR Expert (on-premises), selectează **Endpoint Detection and Response Expert (version 8.0 or later)** din lista de soluții.
7. Configurează conexiunea la *serverele de colectare a telemetriei*:

   a. În blocul **Connection to telemetry collection servers**, faceți clic pe linkul **Connection settings**.

   b. Configurează conexiunea la serverele de colectare a telemetriei:

   - **Timeout (sec)**. Expirarea timpului maxim de răspuns al serverului. Când timpul de expirare se termină, Kaspersky Endpoint Security încearcă să se conecteze la un alt server.
   - **Server certificate**. Certificat TLS pentru stabilirea unei conexiuni de încredere cu serverul. Poți obține un certificat TLS pe Open Single Management Platform (consultă instrucțiunile din Ajutor pentru Kaspersky Endpoint Detection and Response Expert (on-premises)).

- **Use two-way authentication**. Autentificare mutuală la stabilirea unei conexiuni securizate între Kaspersky Endpoint Security și server. Pentru a utiliza autentificarea mutuală, trebuie să activezi autentificarea mutuală în setările serverului, apoi să obții un container crypto și să setezi o parolă pentru a proteja containerul crypto. Un *cripto-container* este o arhivă PFX cu un certificat și o cheie privată. Poți obține un container crypto pe Open Single Management Platform (consultă instrucțiunile din Ajutor pentru Kaspersky Endpoint Detection and Response Expert (on-premises)). După configurarea setărilor serverului, trebuie să activezi autentificarea mutuală și în setările Kaspersky Endpoint Security și să încarci un container crypto protejat prin parolă.

  Criptocontainerul trebuie să fie protejat prin parolă. Nu este posibil să adăugați un criptocontainer cu o parolă necompletată.

c. Fă clic pe **OK**.

d. Adaugă servere de colectare a telemetriei. Pentru a face acest lucru, specificați adresa serverului (IPv4, IPv6) și portul de conectare la server.

Poți adăuga mai multe adrese de server de colectare a datelor de telemetrie. Kaspersky Endpoint Security încearcă să se conecteze la server la prima adresă IP. Dacă nu se poate stabili o conexiune, Kaspersky Endpoint Security încearcă să se conecteze la a doua adresă IP din listă și așa mai departe.

e. Dacă este necesar, configurează telemetria.

8. Configurează conexiunea la *serverele de răspuns*:

a. În blocul **Connection to response servers**, configurează setările pentru **Send sync request to server every (min)**. Frecvența solicitărilor de sincronizare trimise către serverul. În timpul sincronizării, Kaspersky Endpoint Security primește sarcini de răspuns la amenințări și trimite rezultatele sarcinilor.

b. Faceți clic pe linkul **Connection settings**.

c. Configurează conexiunea la serverele de răspuns:

- **Timeout (sec)**. Expirarea timpului maxim de răspuns al serverului. Când timpul de expirare se termină, Kaspersky Endpoint Security încearcă să se conecteze la un alt server.

- **Server certificate**. Certificat TLS pentru stabilirea unei conexiuni de încredere cu serverul. Poți obține un certificat TLS pe Open Single Management Platform (consultă instrucțiunile din Ajutor pentru Kaspersky Endpoint Detection and Response Expert (on-premises)).

- **Use two-way authentication**. Autentificare mutuală la stabilirea unei conexiuni securizate între Kaspersky Endpoint Security și server. Pentru a utiliza autentificarea mutuală, trebuie să activezi autentificarea mutuală în setările serverului, apoi să obții un container crypto și să setezi o parolă pentru a proteja containerul crypto. Un *cripto-container* este o arhivă PFX cu un certificat și o cheie privată. Poți obține un container crypto pe Open Single Management Platform (consultă instrucțiunile din Ajutor pentru Kaspersky Endpoint Detection and Response Expert (on-premises)). După configurarea setărilor serverului, trebuie să activezi autentificarea mutuală și în setările Kaspersky Endpoint Security și să încarci un container crypto protejat prin parolă.

  Criptocontainerul trebuie să fie protejat prin parolă. Nu este posibil să adăugați un criptocontainer cu o parolă necompletată.

d. Fă clic pe **OK**.

e. Adaugă servere de răspuns. Pentru a face acest lucru, specificați adresa serverului (IPv4, IPv6) și portul de conectare la server.

Poți adăuga mai multe adrese de servere de răspuns. Kaspersky Endpoint Security încearcă să se conecteze la server la prima adresă IP. Dacă nu se poate stabili o conexiune, Kaspersky Endpoint Security încearcă să se conecteze la a doua adresă IP din listă și așa mai departe.

9. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Drept urmare, computerul este adăugat pe Open Single Management Platform (OSMP). Verificați starea de funcționare a componentei, vizualizând *Report on status of application components*. De asemenea, puteți vizualiza starea de funcționare a unei componente în rapoarte, în interfața locală a Kaspersky Endpoint Security. Componenta **Endpoint Detection and Response Expert (on-premises)** va fi adăugată la lista componentelor Kaspersky Endpoint Security.

Compatibilitatea cu aplicațiile EPP terțe

EDR Agent acceptă funcționalitatea soluțiilor Kaspersky Detection and Response. Componentele de protecție și control nu sunt disponibile pentru EDR Agent. Această configurație permite instalarea de aplicații EPP terțe și implementarea soluțiilor Kaspersky Detection and Response în infrastructura organizației. EDR Agent acceptă lucrul cu Kaspersky Managed Detection and Response, Kaspersky Anti Targeted Attack Platform (EDR) și Kaspersky Anti Targeted Attack Platform (NDR).

EDR Agent este compatibil cu aplicațiile EPP de la următorii furnizori:

- **Dr.Web**

  EDR Agent este compatibil cu Dr.Web Agent pentru Windows versiunea 13.0.1 sau o versiune ulterioară și Dr.Web Server (x64) 13.0.0.10200.

- **Dallas Lock**

  EDR Agent este compatibil cu Dallas Lock 8.0-C versiunea 11.4.2.843 sau o versiune ulterioară.

  Pentru ca EDR Agent să se execute pe un computer pe care este instalat software-ul Dallas Lock, trebuie să permiți conectarea la serviciile externe Kaspersky în setările modulului Firewall.Pentru ca agentul EDR să se execute pe un computer pe care este instalat software-ul Dallas Lock, trebuie să permiți conectarea la serviciile externe Kaspersky în setările modulului Firewall.

- **Secret Net Studio**

  EDR Agent este compatibil cu Secret Net Studio versiunea 8.11 sau o versiune ulterioară.

  Aplicația nu poate fi instalată pe un computer unde Secret Net Studio este implementat cu componenta Antivirus. Pentru a face posibilă interoperabilitatea, trebuie să elimini componenta Antivirus din Secret Net Studio.

- **Trend Micro**

  EDR Agent este compatibil cu Trend Micro Apex One versiunea 14.0.12994 sau o versiune ulterioară (inclusiv Security Agent).

  EDR Agent este compatibil cu Trend Micro Deep Security versiunea 20.0.2-4960 sau o versiune ulterioară (inclusiv Security Agent).

- **Windows Defender**

- **Sophos**

  EDR Agent este compatibil cu Sophos Intercept X versiunea 2024.1.2 sau o versiune ulterioară (inclusiv Endpoint Agent) și Sophos Core Agent versiunea 2024.3.2.3.

- **Bitdefender**

  EDR Agent este compatibil cu Bitdefender Endpoint Security Tools versiunea 7.9.21.523 sau o versiune ulterioară.

- **ESET**

  EDR Agent este compatibil cu ESET Endpoint Security versiunea 12.0.2049.0 sau o versiune ulterioară și ESET Management Agent versiunea 12.0 sau o versiune ulterioară.

Pe computerele pe care se execută Windows 11 pentru Arm64, Agentul EDR nu este compatibil cu Bitdefender Endpoint Security Tools.

Aplicațiile trebuie instalate în următoarea ordine: mai întâi, instalați aplicația EPP, apoi Agentul de rețea Kaspersky Security Center, apoi EDR Agent. Acest lucru este necesar deoarece programul de instalare a aplicației EPP poate detecta EDR Agent și Agentul de rețea ca software incompatibil și le poate elimina. Funcționarea EDR Agent și a Agentului de rețea trebuie verificată și după actualizarea aplicației EPP terțe, deoarece programul său de instalare poate scana din nou computerul pentru software incompatibil și poate elimina aplicațiile.

Dacă nu ați putut instala EDR Agent pe un computer cu o aplicație EPP terță, deoarece programul de instalare a găsit un software incompatibil pe computer, puteți sări peste verificarea software-ului incompatibil.

Managed Detection and Response



Kaspersky Endpoint Security for Windows acceptă integrarea cu soluția Managed Detection and Response. Soluția *Kaspersky Managed Detection and Response (MDR)* detectează și analizează automat incidentele de securitate din infrastructura dvs. Pentru aceasta, MDR folosește date de telemetrie primite de la puncte finale și învățarea programată. MDR trimite datele incidentelor către experții Kaspersky. Experții pot procesa apoi incidentul și, de exemplu, pot adăuga o nouă intrare în bazele de date antivirus. Alternativ, experții pot emite recomandări privind procesarea incidentului și, de exemplu, pot sugera izolarea computerului de rețea. Pentru informații detaliate despre modul în care funcționează soluțiile, consultați pagina Ajutor Kaspersky Managed Detection and Response.

Configurații ale Kaspersky Endpoint Security pentru integrarea cu MDR

Următoarele configurații pot fi utilizate pentru a lucra cu MDR:

- **[KES+agent încorporat]**. În această configurație, Kaspersky Endpoint Security acționează atât ca aplicație care asigură securitatea computerului, cât și ca aplicație pentru lucrul cu MDR. Agentul încorporat este disponibil în Kaspersky Endpoint Security 11.6.0 for Windows sau o versiune ulterioară.

- **[EPP terță+agent EPP+EDR]**. În această configurație, securitatea infrastructurii IT este asigurată de platforma de Endpoint Protection Platform (EPP) terță. Interacțiunea cu MDR este asigurată de Kaspersky Endpoint Security în configurația Endpoint Detection and Response Agent (Agent EDR). În această configurație, EDR Agent este compatibil cu aplicațiile EPP terțe. EDR Agent este disponibil în Kaspersky Endpoint Security 12.3 for Windows sau o versiune ulterioară.

Suport pentru versiunile anterioare ale Kaspersky Endpoint Security

Kaspersky Endpoint Security versiunea 11 și versiunile ulterioare acceptă soluția MDR. Kaspersky Endpoint Security versiunile 11 – 11.5.0 doar trimit date de telemetrie către Kaspersky Managed Detection and Response, pentru a permite detectarea amenințărilor. Kaspersky Endpoint Security versiunea 11.6.0 deține toate funcționalitățile agentului încorporat (Kaspersky Endpoint Agent).

Dacă utilizați Kaspersky Endpoint Security 11 – 11.5.0, trebuie să actualizați bazele de date la cea mai recentă versiune pentru a funcționa cu soluția MDR. Trebuie să instalați Kaspersky Endpoint Agent.

Dacă utilizezi Kaspersky Endpoint Security 11.6.0 sau o versiune ulterioară, nu este necesar să instalezi Kaspersky Endpoint Agent pentru a utiliza soluția MDR.

Dacă politica Kaspersky Endpoint Security se aplică și computerelor pe care nu este instalat Kaspersky Endpoint Security 11 – 11.5.0, mai întâi trebuie să creați o politică Kaspersky Endpoint Agent separată pentru acele computere. În noua politică, configurați integrarea cu Kaspersky Managed Detection and Response.

Integrarea agentului încorporat cu MDR

Pentru a configura integrarea cu Kaspersky Managed Detection and Response, trebuie să activați componenta Managed Detection and Response și să configurați Kaspersky Endpoint Security.

Pentru funcționarea Kaspersky Managed Detection and Response cu Serverul de administrare prin intermediul Kaspersky Security Center Web Console, trebuie să stabilești o nouă conexiune securizată, o *conexiune în fundal*. Kaspersky Managed Detection and Response vă solicită să stabiliți o conexiune de fundal atunci când implementați soluția. Asigurați-vă că este stabilită conexiunea de fundal.

Stabilirea unei conexiuni de fundal în Consola Web

1. În fereastra principală a Web Console, selectați **Settings** → **Integration**.
2. Accesează secțiunea **Integration**.
3. Duceți comutatorul **Background connection for integration Enabled** la poziția activat.
4. Salvați-vă modificările.

Integrarea cu Kaspersky Managed Detection and Response constă în următorii pași:

1. **Instalarea componentei Managed Detection and Response**

   Poți selecta componenta MDR în timpul instalării sau efectuării upgrade-ului, precum și utilizând activitatea *Modificare componente ale aplicației*.

   Pentru a instala componenta Managed Detection and Response fără a reporni computerul utilizând activitatea *Modificare componente ale aplicației*, trebuie să dezactivezi opțiunea **Verifică aplicațiile terțe incompatibile** în setările activității.

2. **Configurarea Kaspersky Private Security Network**

Omiteți acest pas dacă utilizați Kaspersky Security Center Cloud Console. Kaspersky Security Center Cloud Console configurează automat componenta Kaspersky Private Security Network când se instalează plug-in-ul MDR.

Kaspersky Private Security Network (KPSN) este o soluție care permite utilizatorilor de computere care găzduiesc Kaspersky Endpoint Security sau alte aplicații Kaspersky să obțină acces la bazele de date privind reputația ale Kaspersky și la alte date statistice, fără a trimite date către Kaspersky de la propriile lor computere.

Încărcați fișierul de configurare Kaspersky Security Network în proprietățile Serverului de administrare. Fișierul de configurare al Kaspersky Security Network se află în arhiva ZIP a fișierului de configurare MDR. Puteți obține arhiva ZIP în Consola Kaspersky Managed Detection and Response. Pentru detalii privind configurarea componentei Kaspersky Private Security Network, consultați Ajutor pentru Kaspersky Security Center. De asemenea, puteți încărca un fișier de configurare Kaspersky Security Network în computer, din linia de comandă (consultați instrucțiunile de mai jos).

Cum se configurează Kaspersky Private Security Network din linia de comandă

1. Executați interpretorul de linii de comandă (cmd.exe) ca administrator.
2. Deschideți directorul în care se află fișierul executabil Kaspersky Endpoint Security.
3. Execută următoare comandă:

   ```
   avp.com KSN /private <file name>
   ```

   unde `<file name>` este numele fișierului de configurare care conține setările componentei Kaspersky Private Security Network (format fișier PKCS7 sau PEM).

   Exemplu:
   ```
   avp.com KSN /private C:\kpsn_config.pkcs7
   ```

Ca rezultat, Kaspersky Endpoint Security va utiliza componenta Kaspersky Private Security Network pentru a determina reputația fișierelor, aplicațiilor și site-urilor web. Secțiunea **Kaspersky Security Network** din setările politicii va afișa următoarea stare de funcționare: *Infrastructură: Kaspersky Private Security Network*.

Trebuie să activați modul KSN extins pentru ca Managed Detection and Response să funcționeze.

3 Activarea funcționalității Kaspersky Managed Detection and Response

Începând cu Kaspersky Endpoint Security for Windows 12.10, pentru a activa funcționalitatea Managed Detection and Response, ca alternativă la uno cod de activare, poți folosi și un fișier cheie.

Kaspersky Managed Detection and Response acceptă următoarele metode de licențiere:

- Funcționalitatea Managed Detection and Response este acoperită de licența Kaspersky Endpoint Security for Windows.

  Funcționalitatea este disponibilă imediat după activarea Kaspersky Endpoint Security for Windows.

- Se utilizează o licență separată pentru MDR (suplimentul Kaspersky Managed Detection and Response).

  Funcționalitatea devine disponibilă după adăugarea unei chei separate pentru suplimentul Kaspersky Managed Detection and Response. Ca rezultat, sunt adăugate două chei pe computer: o cheie pentru Kaspersky Endpoint Security și o cheie pentru Kaspersky Managed Detection and Response.

  Licențierea funcționalității autonome Managed Detection and Response se realizează la fel ca licențierea componentei Kaspersky Endpoint Security.

Asigurați-vă că funcționalitatea componentei MDR este inclusă în licență și că aceasta funcționează în interfața locală a aplicației.

4. **Activarea componentei Managed Detection and Response**

Încărcați fișierul de configurare BLOB în politica Kaspersky Endpoint Security (consultați instrucțiunile de mai jos). Fișierul BLOB conține Id-ul clientului și informații despre licența pentru componenta Kaspersky Managed Detection and Response. Fișierul BLOB se află în arhiva ZIP a fișierului de configurare MDR. Puteți obține arhiva ZIP în Consola Kaspersky Managed Detection and Response. Pentru informații detaliate despre un fișier BLOB, consultați Ajutorul Kaspersky Managed Detection and Response.

Începând cu Kaspersky Endpoint Security 12.6 for Windows, adăugarea unui fișier BLOB este opțională pentru Kaspersky Managed Detection and Response fără entități găzduite, dacă aveți o licență actuală.

Cum se activează componenta Managed Detection and Response în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Detection and Response → Managed Detection and Response (Industrial CyberSecurity)**.
4. Bifați caseta de selectare **Managed Detection and Response (Industrial CyberSecurity)**.
5. În blocul **Setări**, faceți clic pe **Încărcare** și selectați fișierul BLOB primit în Kaspersky Managed Detection and Response Console. Fișierul are extensia P7.

   În mod implicit, utilizatorului i se permite să gestioneze setările aplicației („lacătul" este deschis). Pentru a aplica politica pe computere, închide lacătele.

6. Salvați-vă modificările.

Cum se activează componenta Managed Detection and Response în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management → Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Built-in Agents Configuration → Managed Detection and Response**.
5. Duceți comutatorul **Managed Detection and Response ENABLED** la poziția activat.

6. Faceți clic pe **Upload** și selectați fișierul BLOB care a fost obținut în Kaspersky Managed Detection and Response Console. Fișierul are extensia P7.

   În mod implicit, utilizatorului i se permite să gestioneze setările politicii („lacătul" este deschis). Pentru a aplica politica pe computere, închide lacătele .

7. Salvați-vă modificările.

Cum se activează componenta Managed Detection and Response din linia de comandă

1. Executați interpretorul de linii de comandă (cmd.exe) ca administrator.
2. Deschideți directorul în care se află fișierul executabil Kaspersky Endpoint Security.
3. Execută următoare comandă:

   ```
   avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>
   ```

   Pentru a executa această comandă, funcția Protecție prin parolă trebuie activată. Utilizatorul trebuie să aibă permisiunea **Configurează setările aplicației**.

Ca rezultat, Kaspersky Endpoint Security va verifica fișierul BLOB. Verificarea fișierului BLOB include verificarea semnăturii digitale și a termenilor licenței. Dacă fișierul BLOB este verificat cu succes, Kaspersky Endpoint Security va descărca fișierul și îl va trimite către computer în timpul următoarei sincronizări cu Kaspersky Security Center. Verificați starea de funcționare a componentei, vizualizând *Report on status of application components*. De asemenea, puteți vizualiza starea de funcționare a unei componente în rapoarte, în interfața locală a Kaspersky Endpoint Security. Componenta **Managed Detection and Response** va fi adăugată la lista componentelor Kaspersky Endpoint Security.

5. **Configurarea altor componente ale aplicației pentru a primi telemetrie**

   Trebuie să activați următoarele componente pentru ca Managed Detection and Response să funcționeze:

   - Kaspersky Security Network (modul extins);
   - Behavior Detection.
   - Exploit Prevention.
   - Web Threat Protection.
   - Mail Threat Protection.
   - File Threat Protection.
   - Network Threat Protection.
   - Firewall.
   - Protecție AMSI.

- Scanare în fundal.

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Built-in Agents Configuration** → **Managed Detection and Response**.
5. Duceți comutatorul **Managed Detection and Response ENABLED** la poziția activat.
6. Salvați-vă modificările.

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)**.
4. Bifați caseta de selectare **Managed Detection and Response (Industrial CyberSecurity)**.
5. Salvați-vă modificările.

Ghid pentru migrarea KEA la KES pentru MDR

Kaspersky Endpoint Security for Windows include un agent încorporat pentru soluția Kaspersky Managed Detection and Response. Nu mai aveți nevoie de o aplicați Kaspersky Endpoint Agent separată pentru a utiliza soluția MDR. Toate funcțiile Kaspersky Endpoint Agent vor fi efectuate de Kaspersky Endpoint Security.

Când implementați Kaspersky Endpoint Security pe computere care au instalat Kaspersky Endpoint Agent, soluția Kaspersky Managed Detection and Response va continua să funcționeze cu Kaspersky Endpoint Security. În plus, Kaspersky Endpoint Agent va fi eliminat din computer. Același comportament în sistem va avea loc atunci când actualizați Kaspersky Endpoint Security la versiunea 11.6.0 sau o versiune ulterioară.

> Componenta Kaspersky Endpoint Security nu este compatibilă cu Kaspersky Endpoint Agent. Nu puteți instala ambele aplicații pe același computer.

Următoarele condiții trebuie îndeplinite pentru ca Kaspersky Endpoint Security să funcționeze ca parte a Kaspersky Managed Detection and Response:

- Kaspersky Security Center versiunea 13.2 sau o versiune ulterioară (inclusiv Agentul de rețea). În versiunile anterioare ale Kaspersky Security Center, este imposibil de activat caracteristica Managed Detection and Response.
- Este stabilită o conexiune în fundal între Kaspersky Security Center Web Console și Serverul de administrare. Pentru ca soluția MDR să funcționeze cu Serverul de administrare prin intermediul Kaspersky Security Center Web Console, trebuie să stabiliți o nouă conexiune securizată, o *conexiune în fundal*.

Pași pentru migrarea configurației [KES+KEA] la [KES+agent încorporat] pentru MDR

1. **Efectuarea upgrade-ului pentru plug-in-ul de gestionare Kaspersky Endpoint Security**

   Componenta MDR poate fi gestionată utilizând Plag-in-ul de gestionare Kaspersky Endpoint Security versiunea 11.6 sau o versiune ulterioară. În funcție de tipul de consolă Kaspersky Security Center pe care îl utilizați, actualizați plug-in-ul de gestionare în Consola de administrare (MMC) sau plug-in-ul web în Web Console.

2. **Migrarea politicilor și activităților**

   Transferați setările Kaspersky Endpoint Agent la Kaspersky Endpoint Security for Windows. Sunt disponibile următoarele opțiuni:

   - un expert pentru migrarea de la Kaspersky Endpoint Agent la Kaspersky Endpoint Security. Un expert pentru migrarea de la Kaspersky Endpoint Agent la Kaspersky Endpoint Security funcționează numai în Web Console

     Cum se migrează setările politicilor și ale activităților de la Kaspersky Endpoint Agent la Kaspersky Endpoint Security în Web Console

     În fereastra principală a Web Console, selectați **Operations** → **Migration from Kaspersky Endpoint Agent**.

     Aceasta execută Expertul de migrare a politicilor și activităților. Urmează instrucțiunile din expert.

     Pasul 1. Migrarea politicii

     Expertul de migrare creează o nouă politică ce combină setările politicilor Kaspersky Endpoint Security și Kaspersky Endpoint Agent. În lista de politici, selectați politicile Kaspersky Endpoint Agent ale căror setări doriți să le îmbinați cu politica Kaspersky Endpoint Security. Faceți clic pe politica Kaspersky Endpoint Agent pentru a selecta Kaspersky Endpoint Security cu care doriți să îmbinați setările. Asigurați-vă că ați selectat politicile corecte și treceți la pasul următor.

     Pasul 2. Migrarea activităților

     Expertul de migrare nu acceptă activități MDR. Sari peste acest pas.

     Pasul 3. Finalizarea expertului

     Ieșiți din Expert. În urma utilizării expertului, va fi creată o nouă politică Kaspersky Endpoint Security. Politica va combina setările de la Kaspersky Endpoint Security și Kaspersky Endpoint Agent. Politica se numește *<Kaspersky Endpoint Security policy name> & <Kaspersky Endpoint Agent policy name>*. Noua politică are starea *Inactive*. Pentru a continua, modificați stările politicilor Kaspersky Endpoint Agent și Kaspersky Endpoint Security în *Inactive* și activați noua politică îmbinată.

   - Un expert standard de conversie în bloc a politicilor și activităților. Expertul de conversie în bloc a politicilor și activităților este disponibil numai în Consola de administrare (MMC). Pentru mai multe detalii despre Expertul de conversie în bloc a politicilor și activităților, consultați Ajutor pentru Kaspersky Security Center.

3 Licențierea funcționalității MDR

Pentru a activa Kaspersky Endpoint Security ca parte a soluției Kaspersky Managed Detection and Response, aveți nevoie de o licență separată pentru suplimentul Kaspersky Managed Detection and Response. Puteți adăuga cheia utilizând activitatea *Add key*. Ca rezultat, două chei vor fi adăugate la aplicație: *Kaspersky Endpoint Security* și *Kaspersky Managed Detection and Response*.

4 Instalarea/efectuarea upgrade-ului aplicației Kaspersky Endpoint Security

Pentru a migra funcționalitatea MDR în timpul instalării sau efectuării upgrade-ului unei aplicații, se recomandă utilizarea activității de instalare la distanță. Când creați o activitate de instalare la distanță, trebuie să selectați componenta MDR în setările pachetului de instalare.

De asemenea, puteți face upgrade aplicației utilizând următoarele metode:

- Utilizând serviciul de actualizare Kaspersky.
- Local, folosind Expertul de configurare.

Kaspersky Endpoint Security acceptă selectarea automată a componentelor atunci când se face upgrade-ul unei aplicații pe un computer pe care este instalată aplicația Kaspersky Endpoint Agent. Selectarea automată a componentelor depinde de permisiunile contului de utilizator care face upgrade-ul aplicației.

Dacă faceți upgrade pentru Kaspersky Endpoint Security utilizând fișierul EXE sau MSI din contul de sistem (SYSTEM), Kaspersky Endpoint Security obține acces la licențele curente ale soluțiilor Kaspersky. Prin urmare, dacă pe computer este instalat Kaspersky Endpoint Agent și soluția MDR este activată, programul de instalare Kaspersky Endpoint Security configurează automat setul de componente și selectează componenta MDR. Acest lucru determină componenta Kaspersky Endpoint Security să treacă la utilizarea agentului încorporat și elimină Kaspersky Endpoint Agent. Executarea programului de instalare MSI din contul de sistem (SYSTEM) este efectuată, de obicei, atunci când se face upgrade prin intermediul serviciului de actualizare Kaspersky sau când se implementează un pachet de instalare prin Kaspersky Security Center.

Dacă faceți upgrade pentru Kaspersky Endpoint Security utilizând un fișier MSI dintr-un cont de utilizator fără privilegii, Kaspersky Endpoint Security nu obține acces la licențele curente ale soluțiilor Kaspersky. În acest caz, Kaspersky Endpoint Security selectează automat componente pe baza unui set de componente ale Kaspersky Endpoint Agent. Ulterior, componenta Kaspersky Endpoint Security comută la utilizarea agentului încorporat și elimină Kaspersky Endpoint Agent.

Kaspersky Endpoint Security acceptă efectuarea upgrade-ului fără repornirea computerului. Puteți selecta modul de efectuare a upgrade-ului aplicației în proprietățile politicii.

5 Verificarea funcționării aplicației

Dacă după instalarea sau efectuarea upgrade-ului aplicației, computerul are starea *Critical* în consola Kaspersky Security Center:

- asigurați-vă că Agentul de rețea versiunea 13.2 sau o versiune ulterioară este instalată pe computer.
- Verificați starea de funcționare a agentului încorporat, vizualizând *Report on status of application components*. Dacă o componentă are starea *Not installed*, instalați componenta, utilizând activitatea *Change application components*. Dacă o componentă are starea *Nu este acoperită de licență*, asigurați-vă că ați activat funcționalitatea agentului încorporat.
- Asigurați-vă că acceptați Declarația Kaspersky Security Network în noua politică a Kaspersky Endpoint Security for Windows.

Endpoint Detection and Response

Kaspersky Endpoint Security for Windows include un agent încorporat pentru soluția Kaspersky Endpoint Detection and Response Optimum (denumită în continuare „EDR Optimum"). Începând cu versiunea 11.8.0, Kaspersky Endpoint Security for Windows include un agent încorporat pentru soluția Kaspersky Endpoint Detection and Response Expert (denumită în continuare „EDR Expert"). *Kaspersky Endpoint Detection and Response* sunt o serie de soluții pentru protejarea infrastructurii IT corporative împotriva amenințărilor cibernetice avansate. Funcționalitatea soluțiilor combină detectarea automată a amenințărilor cu capacitatea de a reacționa la aceste amenințări pentru a contracara atacurile avansate, inclusiv exploatările, programele ransomware, atacurile fără fișiere noi, precum și metode care utilizează instrumente de sistem legitime. EDR Expert oferă o funcționalitate mai bună de monitorizare și răspuns decât EDR Optimum. Pentru detalii despre soluții, consultați Ajutor Kaspersky Endpoint Detection and Response Optimum și Ajutor Kaspersky Endpoint Detection and Response Expert.

Instrumente Threat Intelligence

Kaspersky Endpoint Detection and Response utilizează următoarele instrumente Threat Intelligence:

- Integrarea cu Portalul Kaspersky Threat Intelligence, care conține și afișează informații despre reputația fișierelor și a adreselor web.
- Baza de date Kaspersky Threats.
- Infrastructura serviciului clould al Kaspersky Security Network (denumit în continuare „KSN"), care oferă acces la informații în timp real despre reputația fișierelor, site-urilor web și a software-urilor din baza de cunoștințe Kaspersky. Utilizarea datelor de la Kaspersky Security Network asigură răspunsul mai rapid al aplicațiilor Kaspersky la amenințări, îmbunătățește performanța unor componente de protecție și reduce posibilitatea alarmelor false.
- Tehnologia Cloud Sandbox care vă permite să executați fișierele detectate într-un mediu izolat și să le verificați reputația.

Principiul de funcționare al soluției

Kaspersky Endpoint Detection and Response revizuiește și analizează dezvoltarea amenințărilor și oferă *personalului de securitate* sau *Administratorului* informații despre potențialul atac, care sunt necesare pentru un răspuns în timp util. Kaspersky Endpoint Detection and Response afișează detalii de detecție într-o fereastră separată. O *alertă* este un eveniment din infrastructura IT corporativă pe care aplicația l-a identificat ca neobișnuit sau suspect și care poate reprezenta o amenințare de securitate pentru infrastructura IT corporativă. *Detalii detecție* este un instrument pentru vizualizarea tuturor informațiilor colectate despre o amenințare detectată. Detaliile detecției includ, de exemplu, istoricul fișierelor care apar pe computer. Pentru detalii despre gestionarea detectării, consultați Ajutor Kaspersky Endpoint Detection and Response Optimum și Ajutor Kaspersky Endpoint Detection and Response Expert.

Suport pentru versiunile anterioare ale Kaspersky Endpoint Security

Dacă utilizați Kaspersky Endpoint Security 11.2.0–11.6.0 pentru interoperabilitatea cu Kaspersky Endpoint Detection and Response Optimum, aplicația include Kaspersky Endpoint Agent. Puteți instala Kaspersky Endpoint Agent împreună cu Kaspersky Endpoint Security. În Kaspersky Endpoint Security 11.9.0, pachetul de distribuție Kaspersky Endpoint Agent nu mai face parte din kitul de distribuție al Kaspersky Endpoint Security.

Soluția Kaspersky Endpoint Detection and Response Expert nu acceptă interoperabilitatea cu Kaspersky Endpoint Agent. Soluția Kaspersky Endpoint Detection and Response Expert folosește Kaspersky Endpoint Security cu agent încorporat (versiunea 11.8.0 și ulterioară).

Integrarea agentului încorporat cu EDR Optimum / EDR Expert

Pentru a configura integrarea cu Kaspersky Endpoint Detection and Response, trebuie să adaugi componenta Endpoint Detection and Response Optimum sau Endpoint Detection and Response Expert (cloud) și să configurezi Kaspersky Endpoint Security.

Componentele Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud) și Endpoint Detection and Response Expert (on-premises) nu sunt compatibile între ele.

Trebuie îndeplinite următoarele condiții pentru ca Endpoint Detection and Response să funcționeze:

- Kaspersky Security Center versiunea 13.2 sau o versiune ulterioară. În versiunile anterioare ale Kaspersky Security Center, este imposibil de activat caracteristica Endpoint Detection and Response.
- Pluginul de gestionare Kaspersky Endpoint Detection and Response.

  Începând cu Kaspersky Endpoint Security versiunea 12.6, afișarea detaliilor alertelor a fost mutată din plug-in-ul de gestionare Kaspersky Endpoint Security în plug-in-ul de gestionare EDR. Plug-in-ul de gestionare EDR este un plug-in unic pentru lucrul cu agenți pe sistemele de operare Windows, Mac și Linux. Acum, când lucrați cu EDR Optimum, veți avea nevoie de plug-in-ul de gestionare Kaspersky Endpoint Security pentru a crea activități de răspuns la amenințări și de plug-in-ul de management EDR pentru a vizualiza detaliile alertelor.
- Componenta Endpoint Detection and Response Optimum din cadrul Kaspersky Endpoint Security acceptă interacțiunea cu soluția Kaspersky Endpoint Detection and Response Optimum 2.0. Interacțiunea cu Kaspersky Endpoint Detection and Response Optimum versiunea 1.0 nu este acceptată.
- Componenta EDR Optimum poate fi gestionată în Kaspersky Security Center Web Console și Kaspersky Security Center Cloud Console.

  Componenta EDR Expert poate fi gestionată numai utilizând Kaspersky Security Center Cloud Console. Nu puteți gestiona această funcționalitate utilizând Consola de administrare (MMC).
- Aplicația este activată și funcționalitatea este acoperită de licență.
- Componenta Endpoint Detection and Response este activată.

- Componentele aplicației de care depinde Endpoint Detection and Response sunt activate și funcționale. Endpoint Detection and Response depinde de următoarele componente:
  - File Threat Protection.
  - Web Threat Protection.
  - Mail Threat Protection.
  - Exploit Prevention.
  - Behavior Detection.
  - Host Intrusion Prevention.
  - Remediation Engine.
  - Control adaptiv al anomaliilor.

Integrarea cu Kaspersky Endpoint Detection and Response presupune următorii pași:

1. **Instalarea componentelor Endpoint Detection and Response**

   Poți selecta componenta Endpoint Detection and Response Optimum sau componenta Endpoint Detection and Response Expert (cloud) în timpul instalării sau upgrade-ului, precum și utilizarea activității *Modificare componente ale aplicației*.

   > Trebuie să reporniți computerul pentru a finaliza efectuarea upgrade-ului aplicației cu noile componente.

2. **Activarea componentei Kaspersky Endpoint Detection and Response**

   Puteți obține o licență pentru utilizarea componentei Kaspersky Endpoint Detection and Response în următoarele moduri:

   - Funcționalitatea Endpoint Detection and Response este inclusă în licența Kaspersky Endpoint Security for Windows.

     Funcționalitatea este disponibilă imediat după activarea Kaspersky Endpoint Security for Windows.

   - Achiziționarea unei licențe separate pentru EDR Optimum sau EDR Expert (Kaspersky Endpoint Detection and Response Add-on).

     Funcționalitatea devine disponibilă după adăugarea unei chei separate pentru Kaspersky Endpoint Detection and Response. Ca rezultat, sunt adăugate două chei pe computer: o cheie pentru Kaspersky Endpoint Security și o cheie pentru Kaspersky Endpoint Detection and Response.

     Licențierea funcționalității individuale Endpoint Detection and Response se realizează la fel ca licențierea componentei Kaspersky Endpoint Security.

   Asigurați-vă că în licență este inclusă caracteristica EDR Optimum sau EDR Expert și că aceasta se execută în interfața locală a aplicației.

   Pentru mai multe informații despre Acordul de licență pentru utilizatorul final al doluției EDR Optimum, consultă secțiunea Ajutor pentru Kaspersky Endpoint Detection and Response Optimum.

3. **Activarea componentelor Endpoint Detection and Response**

   Puteți activa sau dezactiva componenta în setările politicii Kaspersky Endpoint Security for Windows.

Cum se activează sau dezactivează componenta Endpoint Detection and Response în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Built-in Agents Configuration** → **Endpoint Detection and Response**.
5. Duceți comutatorul **Endpoint Detection and Response ENABLED** la poziția activat.
6. Salvați-vă modificările.

Componenta Kaspersky Endpoint Detection and Response este activată. Verificați starea de funcționare a componentei, vizualizând *Report on status of application components*. De asemenea, puteți vizualiza starea de funcționare a unei componente în rapoarte, în interfața locală a Kaspersky Endpoint Security. Componenta **Endpoint Detection and Response Optimum** sau **Endpoint Detection and Response Expert (cloud)** este adăugată în lista de componente Kaspersky Endpoint Security.

4 **Activarea transferului de date pe serverul de administrare**

Pentru a activa toate caracteristicile Endpoint Detection and Response, transferul de date trebuie să fie activat pentru următoarele tipuri de date:

- date despre fișierul carantină.

  Datele sunt necesare pentru a obține informații despre fișierele carantinate pe un computer prin Web Console și Cloud Console. De exemplu, poți descărca un fișier din carantină pentru analiză în Web Console și Cloud Console.

- date despre lanțul de dezvoltare a amenințării.

  Datele sunt necesare pentru a obține informații despre amenințările detectate pe un computer în Web Console și Cloud Console. Puteți vedea detaliile detecției și să întreprindeți acțiuni de răspuns în Web Console și Cloud Console.

Cum se activează transferul de date pe Serverul de administrare în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **General Settings** → **KSC Integration**.
5. În blocul **Data transfer to Administration Server**, faceți clic pe linkul **Advanced settings**.

6. În fereastra care se deschide, bifează următoarele casete de selectare:

   - **About Quarantine files**.
   - **About a threat development chain**.

7. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Scanare pentru descoperirea indicatorilor de compromitere (activitate standard)

Un *Indicator de compromitere (IOC)* este un set de date despre un obiect sau o activitate care indică accesul neautorizat la computer (compromiterea datelor). De exemplu, multe încercări nereușite de conectare la sistem pot constitui un Indicator de compromitere. Activitatea *IOC Scan* permite găsirea Indicatorilor de compromitere pe computer și luarea măsurilor de răspuns la amenințări.

Kaspersky Endpoint Security caută indicatorii de compromitere folosind fișiere IOC. *Fișierele IOC* sunt fișiere care conțin seturile de indicatori pe care aplicația încearcă să le potrivească pentru a contoriza o detectare. Fișierele IOC trebuie să fie conforme cu standardul OpenIOC.

Modul de rulare al activității IOC Scan

Kaspersky Endpoint Detection and Response vă permite să creați activități standard de Scanare IOC pentru a detecta datele compromise. *Activitate de scanare IOC standard* este un grup sau o activitate locală care este creată și configurată manual în Web Console. Activitățile sunt executate folosind fișiere IOC pregătite de utilizator. Dacă vreți să adăugați manual un indicator de compromitere, citiți cerințele pentru fișiere IOC.

Fișierul pe care îl puteți descărca făcând clic pe linkul de mai jos, conține un tabel cu lista completă a termenilor IOC din standardul OpenIOC.

DESCARCĂ FIȘIERUL IOC_TERMS.XLSX

Kaspersky Endpoint Security acceptă, de asemenea activități de scanare IOC autonome atunci când aplicația este utilizată ca parte a soluției Kaspersky Sandbox.

Crearea fișierului IOC

Începând cu Kaspersky Endpoint Security 12.10 for Windows, poți crea fișiere IOC direct în setările activității. Pentru a crea un fișier IOC, trebuie să pregătești un fișier TXT cu o listă de indicatori de compromitere. Poți adăuga liste cu următoarele obiecte ca indicatori de compromitere:

- Hash-uri de fișiere (MD5/SHA256).

  Aplicația pregătește un fișier IOC cu un domeniu de scanare FileItem/Md5sum sau FileItem/Sha256sum.

- Adrese IP (IPv4, IPv6).

  Aplicația pregătește un fișier IOC cu un domeniu de scanare PortItem/RemoteIP.

- Nume DNS.

  Aplicația pregătește un fișier IOC cu un domeniu de scanare DnsEntryItem/RecordName.

Cum se creează un fișier IOC în Web Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Tasks**.

   Lista activităților se deschide.

2. Selectează activitatea **IOC Scan**.

   Se va deschide fereastra de proprietăți a activității. Dacă este necesar, creează activitatea **IOC Scan**.

3. Selectați fila **Application settings**.

4. Accesează secțiunea **Threat Scan**.

5. Fă clic pe **Redefine IOC files**.

6. Această acțiune deschide formularul pentru crearea unui fișier IOC:

   a. În **IOC files source**, selectează **Generate from file**.

   b. Introdu numele fișierului IOC.

   c. Selectează un fișier TXT cu o listă de indicatori de compromitere.

   d. Selectează tipul fișierului IOC: **DNS names**, **File hashes**, **IP addresses**.

   e. Fă clic pe **Generate**.

   Kaspersky Endpoint Security adaugă fișierele IOC la colecția IOC. Dacă este necesar, poți exclude temporar fișierele IOC din domeniul de aplicare al activității.

7. Salvați-vă modificările.

Crearea unei activități IOC Scan

Puteți crea manual activități de *IOC Scan*:

- În detaliile alertei (numai pentru EDR Optimum).

  Detalii detecție este un instrument pentru vizualizarea tuturor informațiilor colectate despre o amenințare detectată. Detaliile detecției includ, de exemplu, istoricul fișierelor care apar pe computer. Pentru detalii despre gestionarea detectării, consultați Ajutor Kaspersky Endpoint Detection and Response Optimum și Ajutor Kaspersky Endpoint Detection and Response Expert.

- Folosind Expertul de activitate.

Puteți configura activitatea pentru EDR Optimum în Web Console și Cloud Console. Setările activității pentru EDR Expert sunt disponibile numai în Cloud Console.

Pentru a crea o activitate IOC Scan:

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **Add**.

   Expertul de activitate pornește.

3. Configurați setările pentru activitate:

   a. În lista verticală **Application**, selectează **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. În lista verticală **Task type**, selectează **IOC Scan**.

   c. În câmpul **Task name**, introduceți o descriere succintă.

   d. În blocul **Devices to which the task will be assigned**, selectați domeniul activității.

4. Selectați dispozitive în funcție de opțiunea selectată pentru domeniul activității. Mergeți la pasul următor.

5. Introduceți acreditările contului utilizatorului ale cărui drepturi doriți să le utilizați pentru a executa activitatea. Mergeți la pasul următor.

   În mod implicit, Kaspersky Endpoint Security pornește activitatea drept cont de utilizator de sistem (SYSTEM).

   Contul de sistem (SYSTEM) nu are permisiunea să execute activitatea *IOC Scan* pe unitățile de rețea. Dacă doriți să executați activitatea pentru o unitate de rețea, selectați contul unui utilizator care are acces la acea unitate.

   Pentru activitățile de Scanare IOC autonome pe unitățile de rețea, trebuie să selectați manual contul de utilizator care are acces la acea unitate în proprietățile activității.

6. Finalizați expertul.

   Se va afișa o activitate nouă în lista de activități.

7. Faceți clic pe activitatea nouă.

   Se va deschide fereastra de proprietăți a activității.

8. Selectați fila **Application settings**.

9. Accesează secțiunea **Threat Scan**.

10. Încarcă fișierele IOC pentru a căuta indicatorii de compromitere.

    După ce încarci fișierele IOC, aplicația afișează informații rezumative despre fișier, inclusiv lista indicatorilor care nu au trecut verificarea. După încărcarea fișierelor IOC, poți edita manual fișierele în editorul încorporat, direct în proprietățile activității. Kaspersky Endpoint Security acceptă editarea fișierelor IOC care sunt conforme cu standardul OpenIOC 1.1. Nu este posibilă modificarea conținutului fișierelor IOC compatibile cu OpenIOC versiunea 1.0.

    Kaspersky Endpoint Security adaugă fișierele IOC la colecția IOC. Dacă este necesar, poți exclude temporar fișierele IOC din domeniul de aplicare al activității.

Adăugarea sau eliminarea fișierelor IOC după executarea activității nu este recomandată. Acest lucru poate face ca rezultatele scanării IOC să fie afișate incorect pentru executările anterioare ale activității. Pentru a căuta indicatorii de compromitere după noile fișiere IOC, se recomandă adăugarea de noi activități.

11. Dacă este necesar, bifați caseta de selectare **Retrospective IOC Scan**. *Scanare IOC retrospectivă* este un mod al activității *IOC Scan* în care Kaspersky Endpoint Security scanează pentru a descoperi indicatorii de compromitere utilizând datele pentru o anumită perioadă de timp. Acest mod este destinat căutării indicatorilor de compromitere pe baza datelor de telemetrie ale computerului protejat, cum ar fi activitatea de rețea, procesele, fișierele și alte date de telemetrie. Kaspersky Endpoint Security analizează datele din jurnalele sistemului de operare și jurnalele browserului de pe computer. Scanarea IOC retrospectivă analizează jurnalele următoarelor browsere: Google Chrome, Mozilla Firefox, Microsoft Edge (versiunea 79 sau o versiune ulterioară).

12. Configurați acțiunile la detectarea IOC:

    - **Isolate device from the network**. Dacă această opțiune este selectată, Kaspersky Endpoint Security izolează computerul de rețea pentru a preveni răspândirea amenințării. Puteți configura durata izolării în Endpoint Detection and Response component settings.

      Dacă această casetă de selectare este debifată, poți izola computerul de rețea după executarea manuală a activității. Dacă activitatea *IOC Scan* detectează un IOC, poți izola computerul de rețea direct din IOC (proprietățile activității *IOC Scan* → **Application settings** → **IOC Scan results**). Kaspersky Endpoint Security permite, de asemenea, gestionarea imediată a setărilor suplimentare: Perioada de dezactivare a izolării rețelei și Excluderi izolare rețea.

    - **Move copy to Quarantine, delete object**. Dacă această opțiune este selectată, Kaspersky Endpoint Security șterge obiectul rău intenționat găsit pe computer. Înainte de a șterge obiectul, Kaspersky Endpoint Security creează o copie de rezervă în caz că obiectul trebuie restaurat ulterior. Kaspersky Endpoint Security mută copia de rezervă în Carantină.

      Dacă această casetă de selectare este debifată, poți caractina fișierul manual după executarea manuală a activității. Dacă activitatea *IOC Scan* detectează un fișier care poate compromite datele, poți carantina acest fișier direct din rezultatele componentei Scanare IOC (**Application settings** → **IOC Scan results**). Prin urmare, Kaspersky Endpoint Security pornește expertul de creare a activităților cu datele presetate ale fișierului detectat. Trebuie doar să gestionezi setările suplimentare ale activităților, de exemplu, să configurezi programul activităților.

    - **Run Critical Areas Scan**. Dacă această opțiune este selectată, Kaspersky Endpoint Security execută activitatea *Critical Areas Scan*. În mod implicit, Kaspersky Endpoint Security scanează memoria kernel, procesele care se execută și sectoarele de boot ale discurilor.

13. Accesează secțiunea **Advanced**.

14. Selectați tipurile de date (documente IOC) care trebuie analizate ca parte a activității.

    Kaspersky Endpoint Security selectează automat tipurile de date (documente IOC) pentru activitatea *IOC Scan* în conformitate cu conținutul fișierelor IOC încărcate. Nu este recomandat să deselectați tipurile de date.

    În plus, puteți configura domeniile de scanare pentru următoarele tipuri de date:

    - **Files - FileItem**. Setați un Domeniu de scanare IOC pe computer utilizând domenii prestabilite.

      În mod implicit, Kaspersky Endpoint Security scanează pentru depistarea IOC numai zonele importante ale computerului, cum ar fi directorul Descărcări, desktop-ul, directorul cu fișierele temporare ale sistemului de operare etc. De asemenea, puteți adăuga manual și domeniul de scanare.

- **Windows Event Log - EventLogItem**. Introduceți perioada de timp în care au fost înregistrate evenimentele. De asemenea, puteți selecta care jurnal de evenimente Windows trebuie utilizat pentru scanarea IOC. În mod implicit, sunt selectate următoarele jurnale de evenimente: jurnal evenimente aplicație, jurnal evenimente de sistem și jurnal evenimente de securitate.

- **Windows Registry - RegistryItem**. Configurează domeniul de aplicare pentru Scanare IOC în registry.

  În mod implicit, Kaspersky Endpoint Security scanează un set de chei de registry.

15. În fereastra cu proprietățile activității, selectați fila **Schedule**.

16. Configurați planificarea activității.

> Opțiunea Wake-on-LAN nu este disponibilă pentru această activitate. Asigurați-vă că este pornit computerul pentru a executa această activitate.

17. Salvați-vă modificările.

18. Bifați caseta de selectare de lângă activitate.

19. Fă clic pe **Start**.

Ca urmare, Kaspersky Endpoint Security execută căutarea indicatorilor de compromitere pe computer. Puteți vizualiza rezultatele căutării în proprietățile activităților din secțiunea **Results**. Puteți vizualiza informațiile despre indicatorii de compromitere detectați în proprietățile activității: **Application settings** → **IOC Scan results**. În rezultatele Scanării IOC, poți, de asemenea, să carantinezi fișierul detectat manual sau să izolezi computerul de rețea.

Kaspersky Endpoint Security caută duplicate între înregistrările create pentru același fișier IOC și păstrează doar înregistrările unice în rezultatele activității. Duplicatele sunt înregistrări de același tip care au aceleași valori în toate câmpurile comparate. De asemenea, este posibil ca aplicația să nu creeze o înregistrare dacă îi lipsește o valoare într-unul sau mai multe câmpuri (consultă tabelul de mai jos).

Tip	Câmpuri comparate	Condiție pentru necrearea unei înregistrări
FileItem	• FullPath • Md5sum • Sha256sum • PID • UPID • ImagePath	• Valoare lipsă în câmpurile FullPath, Md5sum, Sha256sum. • Valori lipsă în câmpul FullPath și valori identice în câmpurile Md5sum, Sha256sum.
RegistryItem	• Hive • KeyPath • ValueName • Text • Type	Valoare lipsă în cel puțin unul dintre următoarele câmpuri: Hive, KeyPath, ValueName.
ProcessItem	• startTime • PID	Valori lipsă în câmpurile startTime sau PID.

> Fereastra **Alert Details** poate afișa înregistrări RegistryItem cu valori identice ale câmpurilor. Astfel de înregistrări nu sunt duplicate deoarece au valori diferite ale câmpului Text, care nu este afișat în interfață.

> Rezultatele scanării IOC sunt păstrate timp de 30 de zile. După această perioadă, Kaspersky Endpoint Security șterge automat intrările cele mai vechi.

Telemetrie extinsă pentru scanarea IOC

Recomandăm activarea telemetriei extinse pe computer pentru scanarea IOC retrospectivă. Telemetria extinsă îmbunătățește precizia detectării IOC, dar utilizează mai multe resurse ale computerului.

Telemetria extinsă include suport pentru următorii termeni suplimentari:

- FileItem/Md5sum
- FileItem/Sha256sum
- FileItem/SizeInBytes
- FileItem/Created
- FileItem/Modified
- FileItem/Changed
- FileItem/Accessed
- FileItem/FileAttributes

Dacă telemetria extinsă este dezactivată, Kaspersky Endpoint Security poate roti informațiile despre indicatorii de compromitere detectați.

Pentru a activa telemetria extinsă:

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.
   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Built-in Agents Configuration** → **Endpoint Detection and Response**.
5. Bifați caseta de selectare **Enable advanced system activity logging**.
6. Salvați-vă modificările.

Mută fișierul în Carantină

Atunci când reacționează la amenințări, Kaspersky Endpoint Detection and Response poate crea activitatea *Move file to Quarantine*. Acest lucru este necesar pentru a minimiza consecințele amenințării. *Carantină* este un spațiu de stocare locală special de pe computer. Utilizatorul poate pune în carantină fișierele pe care le consideră periculoase pentru computer. Fișierele introduse în carantină sunt stocate într-o stare criptată și nu amenință securitatea dispozitivului. Kaspersky Endpoint Security utilizează Carantina numai atunci când este integrată cu soluțiile Kaspersky Detection and Response. În alte cazuri, Kaspersky Endpoint Security plasează fișierul relevant în Copie de rezervă. Pentru detalii privind gestionarea funcției Carantină ca parte a soluțiilor, consultă Kaspersky Sandbox Help, Kaspersky Endpoint Detection and Response Optimum Help, Kaspersky Endpoint Detection and Response Expert Help, Kaspersky Anti Targeted Attack Platform Help, and Kaspersky Endpoint Detection and Response Expert (on-premises) Help.

Puteți crea activitățile *Move file to Quarantine* în următoarele moduri:

- În detaliile alertei (numai pentru EDR Optimum).

  Detalii detecție este un instrument pentru vizualizarea tuturor informațiilor colectate despre o amenințare detectată. Detaliile detecției includ, de exemplu, istoricul fișierelor care apar pe computer. Pentru detalii despre gestionarea detectării, consultați Ajutor Kaspersky Endpoint Detection and Response Optimum și Ajutor Kaspersky Endpoint Detection and Response Expert.

- Folosind Expertul de activitate.

  Trebuie să introduceți calea fișierului sau codul hash (SHA256 sau MD5) al acestuia, sau atât calea fișierului, cât și hash-ul fișierului.

- În setările activității *IOC Scan*.

  Dacă activitatea *IOC Scan* detectează un fișier care poate compromite datele, poți carantina acest fișier direct din rezultatele componentei Scanare IOC (**Application settings** → **IOC Scan results**). Prin urmare, Kaspersky Endpoint Security pornește expertul de creare a activităților cu datele presetate ale fișierului detectat. Trebuie doar să gestionezi setările suplimentare ale activităților, de exemplu, să configurezi programul activităților.

Activitatea *Move file to Quarantine* are următoarele limitări:

1. Dimensiunea fișierului nu trebuie să depășească 100 MO.
2. Obiectele de sistem critice (SCO) nu pot fi carantinate. SCO-urile sunt fișiere pe care sistemul de operare și aplicația Kaspersky Endpoint Security for Windows trebuie să le poată executa.
3. Puteți configura activitatea pentru EDR Optimum în Web Console și Cloud Console. Setările activității pentru EDR Expert sunt disponibile numai în Cloud Console.
4. Nu puteți scana un obiect în carantină ca urmare a activității *Move file to Quarantine*.

Pentru a crea o activitate Move file to Quarantine:

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **Add**.

   Expertul de activitate pornește.

3. Configurați setările pentru activitate:

   a. În lista verticală **Application**, selectează **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. În lista verticală **Task type**, selectează **Move file to Quarantine**.

   c. În câmpul **Task name**, introduceți o descriere succintă.

   d. În blocul **Devices to which the task will be assigned**, selectați domeniul activității.

4. Selectați dispozitive în funcție de opțiunea selectată pentru domeniul activității. Fă clic pe **Next**.

5. Introduceți acreditările contului utilizatorului ale cărui drepturi doriți să le utilizați pentru a executa activitatea. Fă clic pe **Next**.

   În mod implicit, Kaspersky Endpoint Security pornește activitatea drept cont de utilizator de sistem (SYSTEM).

6. Termină expertul făcând clic pe butonul **Finish**.

   Se va afișa o activitate nouă în lista de activități.

7. Faceți clic pe activitatea nouă.

   Se va deschide fereastra de proprietăți a activității.

8. Selectați fila **Application settings**.

9. În lista de fișiere, faceți clic pe **Add**.

   Expertul de adăugare a fișierului pornește.

10. Pentru a adăuga fișierul, trebuie să introduceți calea completă a fișierului sau atât codul hash al fișierului, cât și calea.

    Dacă fișierul se află pe o unitate de rețea, introduceți calea fișierului începând cu `\\`, și nu litera corespunzătoare unității. De exemplu, `\\server\shared_folder\file.exe`. În cazul în care calea fișierului conține litera unei unități de rețea, puteți primi o eroare *Fișier negăsit*.

11. În fereastra cu proprietățile activității, selectați fila **Schedule**.

12. Configurați planificarea activității.

    Opțiunea Wake-on-LAN nu este disponibilă pentru această activitate. Asigurați-vă că este pornit computerul pentru a executa această activitate.

13. Salvați-vă modificările.

14. Bifați caseta de selectare de lângă activitate.

15. Fă clic pe **Start**.

Drept urmare, Kaspersky Endpoint Security mută fișierul în Carantină.

Dacă fișierul este blocat de un alt proces, activitatea este afișată ca *Completed*, dar fișierul în sine este carantinat doar după repornirea computerului. După repornirea computerului, confirmați faptul că fișierul este șters.

Activitatea *Move file to Quarantine* se poate termina cu eroarea *Acces refuzat* dacă încercați să carantinați un fișier executabil care se execută în prezent. Creați o activitate Terminate process pentru fișier și încercați din nou.

Activitatea *Move file to Quarantine* poate termina cu eroarea *Spațiu insuficient în spațiul de stocare Carantină* dacă încercați să puneți în carantină un fișier care este prea mare. Goliți carantina sau măriți carantina. Apoi încercați din nou.

Puteți restaura un fișier din Carantină sau puteți goli Carantina folosind Web Console. Puteți restaura obiectele local pe computer folosind linia de comandă.

Obținere fișier

Puteți obține fișiere de pe computerele utilizatorului. De exemplu, puteți configura obținerea unui fișier jurnal de evenimente creat de o aplicație terță. Ca urmare a executării activității, fișierul este salvat în Carantină. *Carantină* este un spațiu de stocare locală special de pe computer. Poți descărca acest fișier din Carantină pe computerul tău utilizând Web Console (**Operații → Spații de stocare → Carantină**). Pe computerul utilizatorului, fișierul rămâne în directorul original.

Dimensiunea fișierului nu trebuie să depășească 100 MO.

Puteți configura activitatea pentru EDR Optimum în Web Console și Cloud Console. Setările activității pentru EDR Expert sunt disponibile numai în Cloud Console.

Pentru a crea o activitate Obținere fișier:

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **Add**.

   Expertul de activitate pornește.

3. Configurați setările pentru activitate:

   a. În lista verticală **Application**, selectează **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. În lista verticală **Task type**, selectează **Get file**.

   c. În câmpul **Task name**, introduceți o descriere succintă.

   d. În blocul **Devices to which the task will be assigned**, selectați domeniul activității.

4. Selectați dispozitive în funcție de opțiunea selectată pentru domeniul activității. Fă clic pe **Next**.

5. Introduceți acreditările contului utilizatorului ale cărui drepturi doriți să le utilizați pentru a executa activitatea. Fă clic pe **Next**.

   În mod implicit, Kaspersky Endpoint Security pornește activitatea drept cont de utilizator de sistem (SYSTEM).

6. Termină expertul făcând clic pe butonul **Finish**.

   Se va afișa o activitate nouă în lista de activități.

7. Faceți clic pe activitatea nouă.

   Se va deschide fereastra de proprietăți a activității.

8. Selectați fila **Application settings**.

9. În lista de fișiere, faceți clic pe **Add**.

   Expertul de adăugare a fișierului pornește.

10. Pentru a adăuga fișierul, trebuie să introduceți calea completă a fișierului sau atât codul hash al fișierului, cât și calea.

    Dacă fișierul se află pe o unitate de rețea, introduceți calea fișierului începând cu `\\`, și nu litera corespunzătoare unității. De exemplu, `\\server\shared_folder\file.exe`. În cazul în care calea fișierului conține litera unei unități de rețea, puteți primi o eroare *Fișier negăsit*.

11. În fereastra cu proprietățile activității, selectați fila **Schedule**.

12. Configurați planificarea activității.

    Opțiunea Wake-on-LAN nu este disponibilă pentru această activitate. Asigurați-vă că este pornit computerul pentru a executa această activitate.

13. Salvați-vă modificările.

14. Bifați caseta de selectare de lângă activitate.

15. Fă clic pe **Start**.

    Drept urmare, Kaspersky Endpoint Security creează o copie a fișierului și mută copia în carantină. Descărcați fișierul din Carantină în Web Console.

Ștergere fișiere

Puteți șterge de la distanță fișiere folosind activitatea *Delete file*. De exemplu, puteți șterge de la distanță un fișier atunci când răspundeți la amenințări.

Activitatea *Delete file* are următoarele limitări:

- System Critical Object (SCO) nu poate fi șters. SCO-urile sunt fișiere pe care sistemul de operare și aplicația Kaspersky Endpoint Security trebuie să le poată executa.
- Puteți configura activitatea pentru EDR Optimum în Web Console și Cloud Console. Setările activității pentru EDR Expert sunt disponibile numai în Cloud Console.

Pentru a crea o activitate Delete file:

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **Add**.

   Expertul de activitate pornește.

3. Configurați setările pentru activitate:

   a. În lista verticală **Application**, selectează **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. În lista verticală **Task type**, selectează **Delete file**.

   c. În câmpul **Task name**, introduceți o descriere succintă.

   d. În blocul **Devices to which the task will be assigned**, selectați domeniul activității.

4. Selectați dispozitive în funcție de opțiunea selectată pentru domeniul activității. Fă clic pe **Next**.

5. Introduceți acreditările contului utilizatorului ale cărui drepturi doriți să le utilizați pentru a executa activitatea. Fă clic pe **Next**.

   În mod implicit, Kaspersky Endpoint Security pornește activitatea drept cont de utilizator de sistem (SYSTEM).

6. Termină expertul făcând clic pe butonul **Finish**.

   Se va afișa o activitate nouă în lista de activități.

7. Faceți clic pe activitatea nouă.

   Se va deschide fereastra de proprietăți a activității.

8. Selectați fila **Application settings**.

9. În lista de fișiere, faceți clic pe **Add**.

   Expertul de adăugare a fișierului pornește.

10. Pentru a adăuga fișierul, trebuie să introduceți calea completă a fișierului sau atât codul hash al fișierului, cât și calea.

    Dacă fișierul se află pe o unitate de rețea, introduceți calea fișierului începând cu `\\`, și nu litera corespunzătoare unității. De exemplu, `\\server\shared_folder\file.exe`. În cazul în care calea fișierului conține litera unei unități de rețea, puteți primi o eroare *Fișier negăsit*.

11. În fereastra cu proprietățile activității, selectați fila **Schedule**.

12. Configurați planificarea activității.

    Opțiunea Wake-on-LAN nu este disponibilă pentru această activitate. Asigurați-vă că este pornit computerul pentru a executa această activitate.

13. Salvați-vă modificările.

14. Bifați caseta de selectare de lângă activitate.

15. Fă clic pe **Start**.

    Drept urmare, Kaspersky Endpoint Security șterge fișierul din computer. Dacă fișierul este blocat de un alt proces, activitatea este afișată ca *Done*, dar fișierul în sine este șters doar după repornirea computerului. După repornirea computerului, confirmați faptul că fișierul este șters.

Activitatea *Delete file* se poate termina cu eroarea *Access denied or file not found* dacă încercați să ștergeți un fișier executabil care se execută în prezent. Creați o activitate Terminate process pentru fișier și încercați din nou.

Pornire proces

Puteți executa fișiere de la distanță, folosind activitatea *Process start*. De exemplu, puteți executa de la distanță un utilitar care creează fișierul de configurare a computerului. Apoi puteți utiliza activitatea *Receive file from device* pentru a primi fișierul creat în Kaspersky Security Center Web Console.

Puteți configura activitatea pentru EDR Optimum în Web Console și Cloud Console. Setările activității pentru EDR Expert sunt disponibile numai în Cloud Console.

Pentru a crea o activitate Process start:

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **Add**.

   Expertul de activitate pornește.

3. Configurați setările pentru activitate:

   a. În lista verticală **Application**, selectează **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. În lista verticală **Task type**, selectează **Process start**.

   c. În câmpul **Task name**, introduceți o descriere succintă.

   d. În blocul **Devices to which the task will be assigned**, selectați domeniul activității.

4. Selectați dispozitive în funcție de opțiunea selectată pentru domeniul activității. Fă clic pe **Next**.

5. Introduceți acreditările contului utilizatorului ale cărui drepturi doriți să le utilizați pentru a executa activitatea. Fă clic pe **Next**.

   În mod implicit, Kaspersky Endpoint Security pornește activitatea drept cont de utilizator de sistem (SYSTEM).

6. Termină expertul făcând clic pe butonul **Finish**.

   Se va afișa o activitate nouă în lista de activități.

7. Faceți clic pe activitatea nouă.

8. Se va deschide fereastra de proprietăți a activității.

9. Selectați fila **Application settings**.

10. Introduceți comanda de pornire a procesului.

    Să presupunem că doriți să rulați un utilitar (`utility.exe`) care salvează informațiile despre configurația computerului într-un fișier numit `conf.txt` în folderul curent (în mod implicit). Utilitarul se află în folderul `C:\Users\admin\Diagnostic\`. Trebuie să salvați fișierul de configurare în folderul `C:\Users\admin\Documents\Configuration`. Introduceți următoarele valori:

    - **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. În fereastra cu proprietățile activității, selectați fila **Schedule**.

12. Configurați planificarea activității.

    Opțiunea Wake-on-LAN nu este disponibilă pentru această activitate. Asigurați-vă că este pornit computerul pentru a executa această activitate.

13. Salvați-vă modificările.

14. Bifați caseta de selectare de lângă activitate.

15. Fă clic pe **Start**.

    Ca urmare, Kaspersky Endpoint Security execută comanda în modul silențios și pornește procesul. Puteți vizualiza rezultatele căutării în proprietățile activităților din secțiunea **Execution results**.

Terminare proces

Puteți termina de la distanță procesele folosind activitatea *Terminate process*. De exemplu, puteți închide de la distanță un utilitar de testare a vitezei de Internet care a fost pornit folosind activitatea *Execută procesul*.

Dacă doriți să interziceți rularea unui fișier, puteți configura fișierul Componenta de prevenire a executării. Puteți interzice executarea fișierelor executabile, scripturilor, fișierelor în format Office.

Activitatea *Terminate process* are următoarele limitări:

- Procesele pentru Obiectele de sistem critice (SCO) nu pot fi terminate. SCO-urile sunt fișiere pe care sistemul de operare și aplicația Kaspersky Endpoint Security trebuie să le poată executa.
- Puteți configura activitatea pentru EDR Optimum în Web Console și Cloud Console. Setările activității pentru EDR Expert sunt disponibile numai în Cloud Console.

Pentru a crea o activitate Terminate process:

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Fă clic pe **Add**.

   Expertul de activitate pornește.

3. Configurați setările pentru activitate:

   a. În lista verticală **Application**, selectează **Kaspersky Endpoint Security for Windows 14.1.0**.

   b. În lista verticală **Task type**, selectează **Terminate process**.

   c. În câmpul **Task name**, introduceți o descriere succintă.

   d. În blocul **Devices to which the task will be assigned**, selectați domeniul activității.

4. Selectați dispozitive în funcție de opțiunea selectată pentru domeniul activității. Fă clic pe **Next**.

5. Introduceți acreditările contului utilizatorului ale cărui drepturi doriți să le utilizați pentru a executa activitatea. Fă clic pe **Next**.

   În mod implicit, Kaspersky Endpoint Security pornește activitatea drept cont de utilizator de sistem (SYSTEM).

6. Termină expertul făcând clic pe butonul **Finish**.

   Se va afișa o activitate nouă în lista de activități.

7. Faceți clic pe activitatea nouă.

   Se va deschide fereastra de proprietăți a activității.

8. Selectați fila **Application settings**.

9. Pentru a finaliza procesul, trebuie să selectați fișierul pe care doriți să îl închideți. Poți selecta un fișier într-unul din următoarele moduri:

   - Introduceți numele complet în fișier.
   - Introduceți codul hash al fișierului și calea către fișier.
   - Introduceți PID-ul procesului (numai pentru activitățile locale).

Dacă fișierul se află pe o unitate de rețea, introduceți calea fișierului începând cu `\\`, și nu litera corespunzătoare unității. De exemplu, `\\server\shared_folder\file.exe`. În cazul în care calea fișierului conține litera unei unități de rețea, puteți primi o eroare *Fișier negăsit*.

10. În fereastra cu proprietățile activității, selectați fila **Schedule**.
11. Configurați planificarea activității.

    Opțiunea Wake-on-LAN nu este disponibilă pentru această activitate. Asigurați-vă că este pornit computerul pentru a executa această activitate.

12. Fă clic pe **Save**.
13. Bifați caseta de selectare de lângă activitate.
14. Fă clic pe **Start**.

    Drept urmare, Kaspersky Endpoint Security oprește procesul pe computer. De exemplu, dacă rulează o aplicație GAME și terminați procesul game.exe, aplicația este închisă fără a salva date. Puteți vizualiza rezultatele căutării în proprietățile activităților din secțiunea **Results**.

Prevenirea executării

Prevenirea executării permite gestionarea fișierelor care rulează și a scripturilor executabile, precum și deschiderea fișierelor în format Office. În acest fel, puteți, de exemplu, împiedica executarea aplicațiilor pe care le considerați nesigure. Ca urmare, răspândirea amenințării poate fi oprită. Suporturi pentru prevenirea executării un set de extensii de fișiere Office și un set de interpreți de scenariu.

Regulă pentru prevenirea executării

Prevenirea executării gestionează accesul utilizatorilor la fișiere cu reguli de prevenire a executării. *Regula de prevenire a executării* este un set de criterii pe care aplicația le ia în considerare atunci când reacționează la executarea unui obiect, de exemplu când blochează executarea unui obiect. Aplicația identifică fișierele după căile sau sumele lor de verificare calculate folosind algoritmii de combinare MD5 și SHA256.

Puteți crea reguli prevenire executare:

- În detaliile alertei (numai pentru EDR Optimum).

  Detalii detecție este un instrument pentru vizualizarea tuturor informațiilor colectate despre o amenințare detectată. Detaliile detecției includ, de exemplu, istoricul fișierelor care apar pe computer. Pentru detalii despre gestionarea detectării, consultați Ajutor Kaspersky Endpoint Detection and Response Optimum și Ajutor Kaspersky Endpoint Detection and Response Expert.

- Folosirea unei politici de grup sau a setărilor aplicației locale.

  Trebuie să introduceți calea fișierului sau codul hash (SHA256 sau MD5) al acestuia, sau atât calea fișierului, cât și hash-ul fișierului.

De asemenea, puteți gestiona local prevenirea executării folosind Linie de comanda.

Componenta Prevenirea executării are următoarele limitări:

1. Regulile de prevenire nu acoperă fișierele de pe CD-uri sau din imaginile ISO. Aplicația nu blochează executarea sau deschiderea acestor fișiere.

2. Este imposibil să blocați pornirea obiectelor critice de sistem (SCO). SCO-urile sunt fișiere pe care sistemul de operare și aplicația Kaspersky Endpoint Security trebuie să le poată executa.

3. Nu este recomandat să creați mai mult de 5000 de reguli de prevenire a executării, deoarace acest lucru poate cauza instabilitatea sistemului.

Moduri ale regulilor de prevenire a executării

Componenta de prevenire a executării poate funcționa în două moduri:

- **Numai statistici**

  În acest mod, Kaspersky Endpoint Security publică un eveniment despre încercările de a executa obiecte executabile sau de a deschide documente care corespund criteriilor regulii de prevenire în jurnalul de evenimente Windows și în Kaspersky Security Center, dar nu blochează încercarea de a executa sau deschide obiectul sau documentul. Acest mod este selectat în mod implicit.

- **Activ**

  În acest mod, aplicația blochează executarea obiectelor sau deschiderea documentelor care corespund criteriilor regulii de prevenire. Aplicația publică, de asemenea, un eveniment despre încercările de a executa obiecte sau de a deschide documente în jurnalul de evenimente Windows și în jurnalul de evenimente Kaspersky Security Center.

Gestionarea prevenirii executării

Puteți configura setările componentei în Web Console.

Pentru a preveni executarea:

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **Built-in Agents Configuration** → **Endpoint Detection and Response**.

5. Selectați fila **Execution Prevention**.

6. Duceți comutatorul **Execution Prevention ENABLED** la poziția activat.

7. În blocul **Action on execution or opening of forbidden object**, selectați modul de funcționare a componentei:

- **Block and add to event log**. În acest mod, aplicația blochează executarea obiectelor sau deschiderea documentelor care corespund criteriilor regulii de prevenire. Aplicația publică, de asemenea, un eveniment despre încercările de a executa obiecte sau de a deschide documente în jurnalul de evenimente Windows și în jurnalul de evenimente Kaspersky Security Center.

- **Add to event log**. În acest mod, Kaspersky Endpoint Security publică un eveniment despre încercările de a executa obiecte executabile sau de a deschide documente care corespund criteriilor regulii de prevenire în jurnalul de evenimente Windows și în Kaspersky Security Center, dar nu blochează încercarea de a executa sau deschide obiectul sau documentul. Acest mod este selectat în mod implicit.

8. Creați o listă de reguli de prevenire a executării:

a. Fă clic pe **Add**.

b. Aceasta deschide o fereastră; în această fereastră, introduceți numele regulii de prevenire a executării (de exemplu, *Cererea A*).

c. În lista verticală **Type**, selectați obiectul pe care dorești să îl adaugi: **Executable file**, **Script**, **Microsoft Office document**.

Dacă selectați un tip de obiect greșit, Kaspersky Endpoint Security nu blochează fișierul sau scriptul.

d. Pentru a adăuga fișierul, trebuie să introduceți codul hash al fișierului (SHA256 sau MD5), calea completă către fișier sau atât codul hash, cât și calea.

> Dacă fișierul se află pe o unitate de rețea, introduceți calea fișierului începând cu `\\`, și nu litera corespunzătoare unității. De exemplu, `\\server\shared_folder\file.exe`. În cazul în care calea fișierului conține o literă de unitate de rețea, Kaspersky Endpoint Security nu blochează fișierul sau scriptul.

Suporturi pentru prevenirea executării un set de extensii de fișiere Office și un set de interpreți de scenariu.

9. Salvați-vă modificările.

Drept urmare, Kaspersky Endpoint Security blochează executarea obiectelor: rularea fișierelor și scripturilor executabile, deschiderea fișierelor în format office. Cu toate acestea puteți, de exemplu, să deschideți un fișier script într-un editor de text, chiar dacă rularea scriptului este împiedicată. Când blocați executarea unui obiect, Kaspersky Endpoint Security afișează o notificare standard (a se vedea figura de mai jos) dacă notificările sunt activate în setările aplicației.



Reguli pentru prevenirea executării

Izolarea rețelei de calculatoare

Izolarea rețelei computerului permite izolarea automată a unui computer față de rețea ca răspuns la detectarea unui indicator de compromitere (IOC) – acesta este *modul automat*. Poți activa manual opțiunea Izolare rețea în timp ce analizezi amenințarea detectată – acesta este *modul manual*.

Când Izolare rețea este activată, aplicația separă toate conexiunile active și blochează toate conexiunile TCP/IP noi de pe computer, cu excepția următoarelor conexiuni:

- conexiunile listate în Excluderi izolare rețea,
- conexiunile inițiate de serviciile Kaspersky Endpoint Security,
- conexiunile inițiate de Agentul de rețea Kaspersky Security Center,
- conexiunile la SVM și la Serverul de integrare dacă aplicația este utilizată în modul Light Agent.
- Conectările la KSN la integrarea aplicației cu Kaspersky Managed Detection and Response.

Puteți configura setările componentei în Web Console.

Modul automat Izolare rețea

Puteți configura izolarea rețelei pentru a fi activată automat ca răspuns la o detectare IOC. Poți configura modul automat Izolare rețea cu o politică de grup.

Cum se configurează izolarea rețelei pentru a fi pornită automat ca răspuns la o detectare IOC

1. În fereastra principală a Web Console, selectați **Asset management** → **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe activitatea **IOC Scan** a Kaspersky Endpoint Security.

   Se va deschide fereastra de proprietăți a activității.

   Dacă este necesar, creați activitatea *IOC Scan*.

3. Selectați fila **Application settings**.

4. În blocul **Action on IOC detection**, bifați casetele de selectare **Take response actions after an IOC is found** și **Isolate computer from the network**.

5. Salvați-vă modificările.

Ca urmare, atunci când este detectat un IOC, aplicația izolează computerul de rețea pentru a preveni răspândirea amenințării.

Poți configura ca Izolarea automată a rețelei să fie dezactivată după o anumită perioadă de timp. În mod implicit, aplicația dezactivează izolarea rețelei după ce au trecut 8 ore de la momentul în care a fost pornită. De asemenea, poți dezactiva manual modul Izolare rețea (consultă instrucțiunile de mai jos). După oprirea izolării rețelei, computerul poate folosi Rețeaua fără restricții.

Cum se configurează întârzierea pentru dezactivarea modului Izolare rețea a unui computer

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Built-in Agents Configuration** → **Endpoint Detection and Response**.
5. Selectați fila **Network Isolation**.
6. Selectează întârzierea pentru dezactivarea opțiunii Izolare rețea.
7. Salvați-vă modificările.

Modul manual Izolare rețea

Poți activa sau dezactiva manual modul Izolare rețea. Poți configura modul manual Izolare rețea utilizând proprietățile computerului din consola Kaspersky Security Center.

Puteți activa izolarea rețelei:

- În detaliile alertei (numai pentru EDR Optimum).

  Detalii detecție este un instrument pentru vizualizarea tuturor informațiilor colectate despre o amenințare detectată. Detaliile detecției includ, de exemplu, istoricul fișierelor care apar pe computer. Pentru detalii despre gestionarea detectării, consultați Ajutor Kaspersky Endpoint Detection and Response Optimum și Ajutor Kaspersky Endpoint Detection and Response Expert.
- Folosind setările locale ale aplicației.
- În setările activității *IOC Scan*.

  Dacă activitatea *IOC Scan* detectează un IOC, poți izola computerul de rețea direct din IOC (proprietățile activității *IOC Scan* → **Application settings** → **IOC Scan results**). Kaspersky Endpoint Security permite, de asemenea, gestionarea imediată a setărilor suplimentare: Perioada de dezactivare a izolării rețelei și Excluderi izolare rețea.

Cum se activează manual izolarea în rețea a unui computer

1. În fereastra principală a Web Console, selectați **Asset management** → **Assets (Devices)**.
2. Selectează computerul pentru care dorești să configurezi setări locale pentru aplicație.

   Se vor deschide proprietățile computerului.
3. Selectați fila **Applications**.

4. Fă clic pe **Kaspersky Endpoint Security for Windows**.

   Se vor deschide setările locale pentru aplicație.

5. Selectați fila **Application settings**.

6. Accesați **Detection and Response → Endpoint Detection and Response**.

7. În blocul **Network isolation**, fă clic pe **Isolate computer from the network**.

Poți configura ca Izolarea automată a rețelei să fie dezactivată după o anumită perioadă de timp. În mod implicit, aplicația dezactivează izolarea rețelei după ce au trecut 8 ore de la momentul în care a fost pornită. După oprirea izolării rețelei, computerul poate folosi Rețeaua fără restricții.

Cum se configurează întârzierea pentru dezactivarea modului Izolare rețea a unui computer în modul manual

1. În fereastra principală a Web Console, selectați **Asset management → Assets (Devices)**.

2. Selectează computerul pentru care dorești să configurezi setări locale pentru aplicație.

   Se vor deschide proprietățile computerului.

3. Selectați fila **Tasks**.

   Aceasta afișează lista activităților disponibile pe computer.

4. Selectează activitatea **Network isolation**.

5. Selectați fila **Application settings**.

6. Aceasta deschide o fereastră; în această fereastră, selectează întârzierea pentru dezactivarea modului Izolare rețea.

7. Salvați-vă modificările.

Cum se dezactivează manual izolarea rețelei a unui computer

1. În fereastra principală a Web Console, selectați **Asset management → Assets (Devices)**.

2. Selectează computerul pentru care dorești să configurezi setări locale pentru aplicație.

   Se vor deschide proprietățile computerului.

3. Selectați fila **Applications**.

4. Fă clic pe **Kaspersky Endpoint Security for Windows**.

   Se vor deschide setările locale pentru aplicație.

5. Selectați fila **Application settings**.

6. Accesați **Detection and Response → Endpoint Detection and Response**.

7. În blocul **Network isolation**, fă clic pe **Unblock computer isolated from the network**.

De asemenea, puteți activa sau dezactiva Izolarea rețelei local, folosind linia de comandă.

Începând cu Kaspersky Endpoint Security 12.10 for Windows, poți gestiona funcția Izolare rețea în detaliile alertei. În plus, în detaliile alertei poți specifica perioada de timp pentru Izolare rețea a computerului. Pentru detalii despre gestionarea detectării, consultați Ajutor Kaspersky Endpoint Detection and Response Optimum și Ajutor Kaspersky Endpoint Detection and Response Expert.

Excluderi izolare rețea

Puteți configura Network isolation exclusions. Conexiunile de rețea care corespund regulilor nu sunt blocate pe computere atunci când opțiunea Izolare rețea este activată.

Pentru a configura Network isolation exclusions, puteți utiliza o listă de *profiluri de rețea standard*. În mod implicit, excluderile includ profiluri de rețea care conțin reguli care asigură funcționarea neîntreruptă a computerelor cu serverul DNS/DHCP și rolurile clientului DNS/DHCP. De asemenea, puteți modifica setările standard ale profilurilor de rețea sau puteți defini excluderile manual (consultați instrucțiunile de mai jos).

Excluderile specificate în proprietățile politicii se aplică numai dacă opțiunea Izolare rețea este activată automat ca răspuns la o amenințare detectată. Excluderile specificate în proprietățile computerului se aplică numai dacă opțiunea Izolare rețea este activată manual în proprietățile computerului în consola Kaspersky Security Center sau în detaliile alertei.

O politică activă nu împiedică aplicarea excluderilor din izolarea rețelei configurată în proprietățile computerului, deoarece acești parametri au scenarii de utilizare diferite.

Cum se adaugă o excludere de la Izolare rețea în modul automat

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Built-in Agents Configuration** → **Endpoint Detection and Response**.
5. Selectați fila **Network Isolation**.
6. În blocul **Network isolation exclusions**, fă clic pe **Exclusions**.
7. Această acțiune deschide o fereastră; în această fereastră, fă clic pe **Add** → **Add from profile** și selectează profiluri de rețea standard pentru configurarea excluderilor.

   Network isolation exclusions din profil sunt adăugate la lista Network isolation exclusions. Puteți vizualiza proprietățile conexiunilor la rețea. Dacă este necesar, puteți modifica setările conexiunii la rețea.
8. Dacă este necesar, adăugați manual o excludere de izolare a rețelei. Pentru aceasta, în fereastra cu lista de excluderi, fă clic pe **Add** → **Add** și editează manual setările conexiunii la rețea.
9. Salvați-vă modificările.

Cum se adaugă o excludere de la Izolare rețea în modul manual

1. În fereastra principală a Web Console, selectați **Asset management** → **Assets (Devices)**.
2. Selectează computerul pentru care dorești să configurezi setări locale pentru aplicație.

   Se vor deschide proprietățile computerului.
3. Selectați fila **Tasks**.

   Aceasta afișează lista activităților disponibile pe computer.
4. Selectează activitatea **Network isolation**.
5. Selectați fila **Application settings**.
6. Aceasta deschide o fereastră; în această fereastră, fă clic pe **Exclusions**.
7. Aceasta deschide o fereastră; în această fereastră, faceți clic pe **Add from profile** și selectați profiluri de rețea standard pentru configurarea excluderilor.

   Network isolation exclusions din profil sunt adăugate la lista Network isolation exclusions. Puteți vizualiza proprietățile conexiunilor la rețea. Dacă este necesar, puteți modifica setările conexiunii la rețea.
8. Dacă este necesar, adăugați manual o excludere de izolare a rețelei. Pentru a face acest lucru, în fereastra cu lista de excluderi, faceți clic pe **Add** și editați manual setările conexiunii la rețea.
9. Salvați-vă modificările.

De asemenea, puteți vizualiza lista de excludere a izolării rețelei local utilizând Linia de comanda. În acest caz, computerul trebuie izolat.

Începând cu Kaspersky Endpoint Security 12.10 for Windows, poți adăuga excluderile pentru Izolare rețea în detaliile alertei. Pentru detalii despre gestionarea detectării, consultați Ajutor Kaspersky Endpoint Detection and Response Optimum și Ajutor Kaspersky Endpoint Detection and Response Expert.

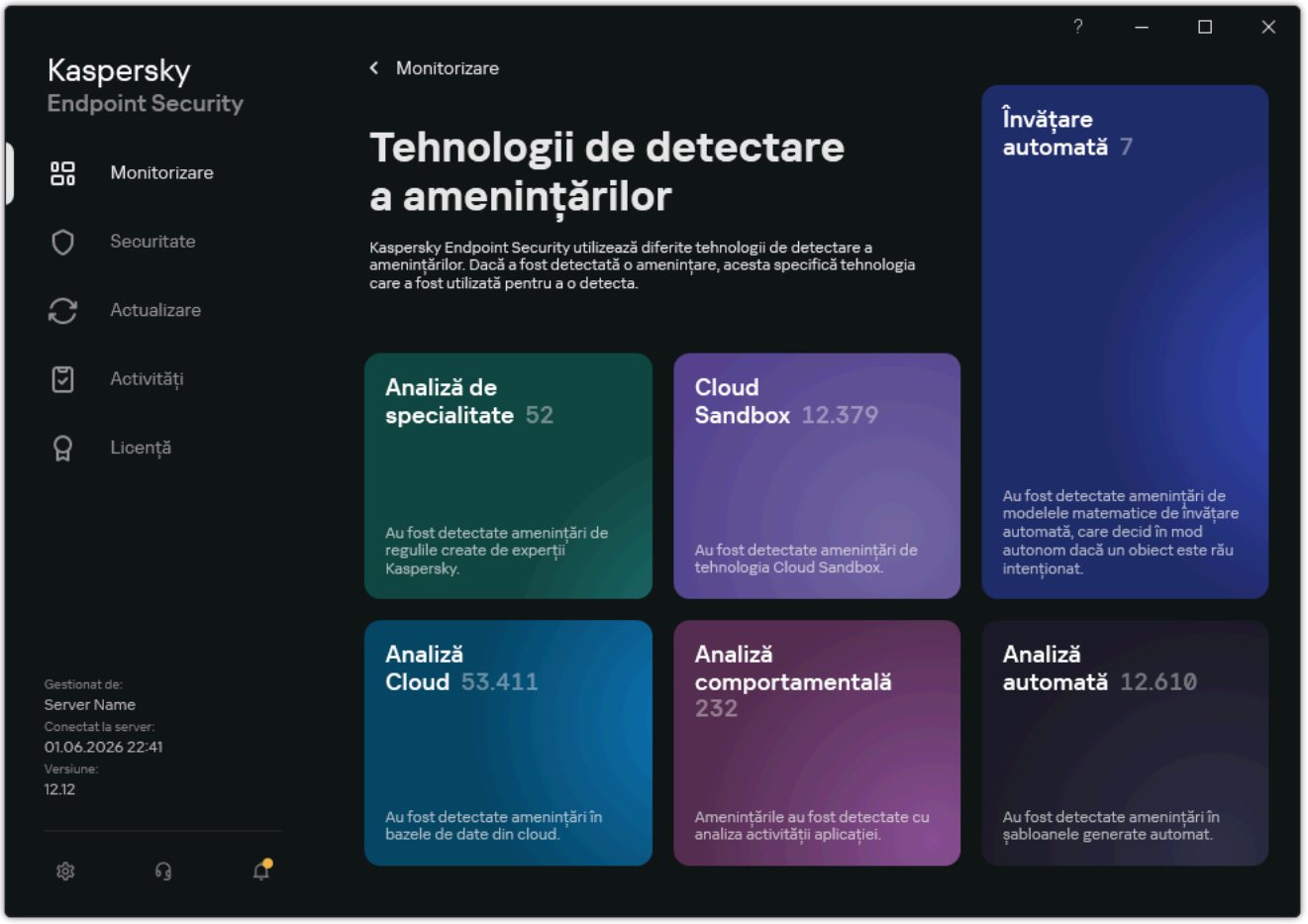
Cloud Sandbox

Cloud Sandbox este o tehnologie care vă permite să detectați amenințările avansate pe un computer. Kaspersky Endpoint Security redirecționează automat fișierele detectate către Cloud Sandbox pentru analiză. Cloud Sandbox execută aceste fișiere într-un mediu izolat pentru a identifica activitățile rău intenționate și a decide asupra reputației lor. Datele din aceste fișiere sunt apoi trimise către Kaspersky Security Network. Prin urmare, dacă Cloud Sandbox a detectat un fișier rău intenționat, Kaspersky Endpoint Security va efectua acțiunea corespunzătoare pentru a elimina această amenințare de pe toate computerele pe care este detectat acest fișier.

Pentru ca tehnologia Cloud Sandbox să funcționeze, trebuie să activezi utilizarea Kaspersky Security Network.

Dacă utilizezi Kaspersky Private Security Network, tehnologia Cloud Sandbox nu este disponibilă.

Tehnologia Cloud Sandbox este activată permanent și este disponibilă pentru toți utilizatorii Kaspersky Security Network, indiferent de tipul de licență pe care îl folosesc. Dacă ai instalat deja soluția Endpoint Detection and Response Optimum, poți activa un contor separat pentru amenințările detectate de Cloud Sandbox. Poți utiliza acest contor pentru a întocmi statistici în timpul analizei amenințărilor detectate. Kaspersky Endpoint Security indică tehnologia de detectare a amenințărilor Cloud Sandbox în *Report on threats* din consola Kaspersky Security Center.



Contoarele de amenințări

Pentru a activa contorul Cloud Sandbox:

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Built-in Agents Configuration** → **Endpoint Detection and Response**.
5. Selectați fila **Cloud Sandbox**.
6. Duceți comutatorul **Cloud Sandbox ENABLED** la poziția activat.
7. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Ori de câte ori există o amenințare, Kaspersky Endpoint Security activează contorul pentru amenințările detectate folosind Cloud Sandbox în fereastra principală a aplicației din **Tehnologii de detectare a amenințărilor**. Kaspersky Endpoint Security va indica, de asemenea, tehnologia de detectare a amenințărilor Cloud Sandbox în *Report on threats* din consola Kaspersky Security Center.

Ghid pentru migrarea KEA la KES pentru EDR Optimum

Kaspersky Endpoint Security for Windows include un agent încorporat pentru soluția Kaspersky Endpoint Detection and Response Optimum. Nu mai aveți nevoie de o aplicați Kaspersky Endpoint Agent separată pentru a utiliza soluția EDR Optimum. Toate funcțiile Kaspersky Endpoint Agent vor fi efectuate de Kaspersky Endpoint Security.

Când implementați Kaspersky Endpoint Security pe computere care au instalat Kaspersky Endpoint Agent, soluția Kaspersky Endpoint Detection and Response Optimum va continua să funcționeze cu Kaspersky Endpoint Security. În plus, Kaspersky Endpoint Agent va fi eliminat din computer. Același comportament în sistem va avea loc atunci când actualizați Kaspersky Endpoint Security la versiunea 11.7.0 sau o versiune ulterioară.

Componenta Kaspersky Endpoint Security nu este compatibilă cu Kaspersky Endpoint Agent. Nu puteți instala ambele aplicații pe același computer.

Următoarele condiții trebuie îndeplinite pentru ca Kaspersky Endpoint Security să funcționeze ca parte a Kaspersky Endpoint Detection and Response Optimum:

- Kaspersky Endpoint Detection and Response Optimum versiunea 2.0 sau o versiune ulterioară.
- Kaspersky Security Center versiunea 13.2 sau o versiune ulterioară (inclusiv Agentul de rețea). În versiunile anterioare ale Kaspersky Security Center, este imposibil de activat caracteristica EDR Optimum.
- Caracteristica EDR Optimum pot fi gestionată numai utilizând Kaspersky Security Center Web Console.
- Transferul de date pe Serverul de administrare este activat. Datele sunt necesare pentru a obține informații despre fișierele carantinate pe un computer prin Web Console.
- Este stabilită o conexiune în fundal între Kaspersky Security Center Web Console și Serverul de administrare. Pentru ca soluția EDR Optimum să funcționeze cu Serverul de administrare prin intermediul Kaspersky Security Center Web Console, trebuie să stabiliți o nouă conexiune securizată, o *conexiune în fundal*.

Pași pentru migrarea configurației [KES+KEA] la [KES+agent încorporat] pentru EDR Optimum

1. **Se face upgrade pentru plug-in-ul web Kaspersky Endpoint Security**

   Componenta EDR Optimum poate fi gestionată utilizând Plag-in-ul web Kaspersky Endpoint Security versiunea 11.7.0 sau o versiune ulterioară.

2. **Migrarea politicilor și activităților**

   Transferați setările Kaspersky Endpoint Agent la Kaspersky Endpoint Security for Windows. Pentru a face acest lucru, utilizați expertul pentru migrarea de la Kaspersky Endpoint Agent în Web Console.

   Cum se migrează setările politicilor și ale activităților de la Kaspersky Endpoint Agent la Kaspersky Endpoint Security în Web Console

   În fereastra principală a Web Console, selectați **Operations → Migration from Kaspersky Endpoint Agent**.

   Aceasta execută Expertul de migrare a politicilor și activităților. Urmează instrucțiunile din expert.

Pasul 1. Migrarea politicii

Expertul de migrare creează o nouă politică ce combină setările politicilor Kaspersky Endpoint Security și Kaspersky Endpoint Agent. În lista de politici, selectați politicile Kaspersky Endpoint Agent ale căror setări doriți să le îmbinați cu politica Kaspersky Endpoint Security. Faceți clic pe politica Kaspersky Endpoint Agent pentru a selecta Kaspersky Endpoint Security cu care doriți să îmbinați setările. Asigurați-vă că ați selectat politicile corecte și treceți la pasul următor.

Pasul 2. Migrarea activităților

Expertul pentru migrare creează noi activități pentru Kaspersky Endpoint Security. În lista de activități, selectați activitățile Kaspersky Endpoint Agent pe care doriți să le creați pentru politica Kaspersky Endpoint Security. Mergeți la pasul următor.

Pasul 3. Finalizarea expertului

Ieșiți din Expert. Ca rezultat, expertul efectuează următoarele acțiuni:

- Creează o nouă politică Kaspersky Endpoint Security.

  Politica va combina setările de la Kaspersky Endpoint Security și Kaspersky Endpoint Agent. Politica se numește *<Kaspersky Endpoint Security policy name> & <Kaspersky Endpoint Agent policy name>*. Noua politică are starea *Inactive*. Pentru a continua, modificați stările politicilor Kaspersky Endpoint Agent și Kaspersky Endpoint Security în *Inactive* și activați noua politică îmbinată.

  > După migrarea de la Kaspersky Endpoint Agent la Kaspersky Endpoint Security for Windows, asigurați-vă că noua politică are setarea funcționalitatea pentru transferul datelor către Serverul de administrare (date despre fișierul carantină și date despre lanțul de dezvoltare a amenințării). Valorile parametrului pentru transferul de date nu sunt migrate dintr-o politică Kaspersky Endpoint Agent.

- Creează noi activități de Kaspersky Endpoint Security.

  Noile activități sunt copii ale activităților Kaspersky Endpoint Agent. În același timp, Expertul lasă activitățile componentei Kaspersky Endpoint Agent neschimbate.

3 Licențierea funcționalității EDR Optimum

Dacă folosiți o licență obișnuită Kaspersky Endpoint Detection and Response Optimum sau Kaspersky Optimum Security pentru a activa Kaspersky Endpoint Security for Windows și Kaspersky Endpoint Agent, funcționalitatea EDR Optimum va fi activată automat după efectuarea upgrade-ului aplicației la versiunea 11.7.0 sau la o versiune ulterioară. Nu trebuie să faceți nimic.

Dacă folosiți o licență independentă Kaspersky Endpoint Detection and Response Optimum Add-on pentru a activa funcționalitatea EDR Optimum, trebuie să vă asigurați că cheia EDR Optimum este adăugată la depozitul Kaspersky Security Center și că funcționalitatea de distribuire automată a cheii licenței este activată. După efectuarea upgrade-ului aplicației la versiunea 11.7.0 sau la o versiune ulterioară, funcționalitatea EDR Optimum este activată automat.

Dacă folosiți o licență Kaspersky Endpoint Detection and Response Optimum sau Kaspersky Optimum Security pentru a activa Kaspersky Endpoint Agent și o licență diferită pentru a activa Kaspersky Endpoint Security for Windows, trebuie să înlocuiți cheia pentru Kaspersky Endpoint Security for Windows cu o cheie Kaspersky Endpoint Detection and Response Optimum sau Kaspersky Optimum Security. Puteți înlocui cheia utilizând activitatea *Add key*.

4. **Instalarea/efectuarea upgrade-ului aplicației Kaspersky Endpoint Security**

Pentru a migra funcționalitatea EDR Optimum în timpul instalării sau efectuării upgrade-ului unei aplicații, se recomandă utilizarea activității de instalare la distanță. Când creați o activitate de instalare la distanță, trebuie să selectați componenta EDR Optimum în setările pachetului de instalare.

De asemenea, puteți face upgrade aplicației utilizând următoarele metode:

- Utilizând serviciul de actualizare Kaspersky.
- Local, folosind Expertul de configurare.

Kaspersky Endpoint Security acceptă selectarea automată a componentelor atunci când se face upgrade-ul unei aplicații pe un computer pe care este instalată aplicația Kaspersky Endpoint Agent. Selectarea automată a componentelor depinde de permisiunile contului de utilizator care face upgrade-ul aplicației.

Dacă faceți upgrade pentru Kaspersky Endpoint Security utilizând fișierul EXE sau MSI din contul de sistem (SYSTEM), Kaspersky Endpoint Security obține acces la licențele curente ale soluțiilor Kaspersky. Prin urmare, dacă pe computer este instalat, de exemplu, Kaspersky Endpoint Agent și soluția EDR Optimum este activată, programul de instalare Kaspersky Endpoint Security configurează automat setul de componente și selectează componenta EDR Optimum. Acest lucru determină componenta Kaspersky Endpoint Security să treacă la utilizarea agentului încorporat și elimină Kaspersky Endpoint Agent. Executarea programului de instalare MSI din contul de sistem (SYSTEM) este efectuată, de obicei, atunci când se face upgrade prin intermediul serviciului de actualizare Kaspersky sau când se implementează un pachet de instalare prin Kaspersky Security Center.

Dacă faceți upgrade pentru Kaspersky Endpoint Security utilizând un fișier MSI dintr-un cont de utilizator fără privilegii, Kaspersky Endpoint Security nu obține acces la licențele curente ale soluțiilor Kaspersky. În acest caz, Kaspersky Endpoint Security selectează automat componentele pe baza configurației Kaspersky Endpoint Agent. Ulterior, componenta Kaspersky Endpoint Security comută la utilizarea agentului încorporat și elimină Kaspersky Endpoint Agent.

Kaspersky Endpoint Security acceptă efectuarea upgrade-ului fără repornirea computerului. Puteți selecta modul de efectuare a upgrade-ului aplicației în proprietățile politicii.

5. **Verificarea funcționării aplicației**

Dacă după instalarea sau efectuarea upgrade-ului aplicației, computerul are starea *Critical* în consola Kaspersky Security Center:

- asigurați-vă că Agentul de rețea versiunea 13.2 sau o versiune ulterioară este instalată pe computer.
- Verificați starea de funcționare a agentului încorporat, vizualizând *Report on status of application components*. Dacă o componentă are starea *Not installed*, instalați componenta, utilizând activitatea *Change application components*. Dacă o componentă are starea *Nu este acoperită de licență*, asigurați-vă că ați activat funcționalitatea agentului încorporat.
- Asigurați-vă că acceptați Declarația Kaspersky Security Network în noua politică a Kaspersky Endpoint Security for Windows.

Kaspersky Sandbox

Kaspersky Endpoint Security for Windows include un agent încorporat pentru integrarea cu soluția Kaspersky Sandbox. Componenta *Sandbox* detectează și blochează automat amenințările avansate de pe computere. Sandbox analizează comportamentul obiectelor pentru a detecta activitatea rău intenționată și activitatea caracteristică atacurilor țintite asupra infrastructurii IT a organizației. Sandbox analizează și scanează obiecte de pe servere speciale cu imagini virtuale implementate ale sistemelor de operare Microsoft Windows (servere Sandbox). Pentru informații detaliate despre soluție, consultați Ajutor pentru Kaspersky Sandbox și Ajutor pentru Kaspersky Anti Targeted Attack Platform.

Integrarea agentului încorporat cu Kaspersky Sandbox

Adăugarea componentei Kaspersky Sandbox este necesară pentru integrarea cu Kaspersky Sandbox. Puteți selecta componenta Sandbox în timpul instalării sau efectuării upgrade-ului, precum și utilizând activitatea *Modificare componente ale aplicației*.

Pentru a utiliza componenta, trebuie îndeplinite următoarele condiții:

- Kaspersky Security Center 13.2. Versiunile nterioare ale Kaspersky Security Center nu permit crearea activităților de Scanare IOC autonome ca răspuns la amenințări.
- Componenta poate fi gestionată numai utilizând Web Console. Nu puteți gestiona această componentă utilizând Consola de administrare (MMC).
- Aplicația este activată și funcționalitatea este acoperită de licență.
- Transferul de date pe Serverul de administrare este activat.

  Pentru a utiliza toate caracteristicile componentei Kaspersky Sandbox, asigurați-vă că transferul datelor fișierului carantină este dezactivat. Datele sunt necesare pentru a obține informații despre fișierele carantinate pe un computer prin Web Console. De exemplu, poți descărca un fișier din carantină pentru analiză în Web Console.

  Cum se activează transferul de date pe Serverul de administrare în Web Console

  1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
  2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

     Se deschide fereastra de proprietăți a politicii.
  3. Selectați fila **Application settings**.
  4. Accesați **General Settings** → **KSC Integration**.
  5. În blocul **Data transfer to Administration Server**, bifați caseta de selectare **About Quarantine files**.
  6. Salvați-vă modificările.
- Este stabilită o conexiune în fundal între Kaspersky Security Center Web Console și Serverul de administrare

  Pentru funcționarea Kaspersky Sandbox cu Serverul de administrare prin intermediul Kaspersky Security Center Web Console, trebuie să stabiliți o nouă conexiune securizată, o *conexiune în fundal*. Pentru detalii despre integrarea Kaspersky Security Center cu alte soluții Kaspersky, consultați Ajutor Kaspersky Security Center.

Stabilirea unei conexiuni de fundal în Consola Web

1. În fereastra principală a Web Console, selectați **Settings** → **Integration**.
2. Accesează secțiunea **Integration**.
3. Duceți comutatorul **Background connection for integration Enabled** la poziția activat.
4. Salvați-vă modificările.

Dacă nu este stabilită o conexiune de fundal între Kaspersky Security Center Web Console și Administration Server, activitățile de Scanare IOC autonome nu pot fi create ca parte a răspunsului la amenințare.

- Pentru a configura o conexiune de încredere cu serverul Sandbox, trebuie să pregătești un certificat TLS. Apoi, trebuie să adaugi certificatul pe computer, folosind o politică. De asemenea, trebuie să adaugi certificatul la serverul Sandbox.

  > Autentificarea mutuală folosind un crypto-container nu este disponibilă pentru Kaspersky Sandbox.

  Puteți adăuga un certificat TLS în Web Console sau local, folosind linia de comandă.

- Componenta Kaspersky Sandbox este activată.
- Componentele aplicației care asigură funcționarea componentei Sandbox sunt activate și operaționale. Următoarele componente asigură funcționarea componentei Sandbox:
  - File Threat Protection.
  - Host Intrusion Prevention.
  - Firewall.
  - Protecție AMSI.
  - Scanare în fundal.

Pentru a activa sau dezactiva integrarea cu Kaspersky Sandbox:

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.
   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Built-in Agents Configuration** → **Sandbox**.
5. Utilizați comutatorul **Integration with Sandbox ENABLED** pentru a activa sau a dezactiva componenta.
6. În blocul **Integration mode**, selectați modul de funcționare a componentei: **Kaspersky Sandbox**.
7. Faceți clic pe linkul **Connection settings**.
   Se deschide fereastra de setări a conexiunii serverului Sandbox.

8. În blocul **Server TLS certificate**, faceți clic pe **Upload** și selectați fișierul certificatului TLS.

   Kaspersky Endpoint Security poate avea un singur certificat TLS pentru un server Sandbox. Dacă ați adăugat anterior un certificat TLS, certificatul respectiv este revocat. Este utilizat doar ultimul certificat adăugat.

9. Configurează setările avansate ale conexiunii pentru serverele Sandbox:

   - **Timeout (msec)**. Conexiunea a expirat pentru serverul Sandbox. După expirarea perioadei de expirare configurată, Kaspersky Endpoint Security trimite o solicitare către următorul server. Poți crește perioada de expirare a conexiunii pentru server dacă viteza conexiunii este mică sau dacă conexiunea este instabilă. Perioada de expirare a solicitării recomandată este de 0.5 secunde sau mai puțin.

   - **Request queue**. Dimensiunea directorului cozii de solicitare. Când trimiți mai multe obiecte pentru scanare în Sandbox, Kaspersky Endpoint Security creează o coadă de solicitări. În mod implicit, dimensiunea directorului cozii de solicitare este limitată la 100 MO. După atingerea dimensiunii maxime, Sandbox încetează să mai adauge noi solicitări la coadă și trimite evenimentul corespunzător către Kaspersky Security Center. Puteți configura dimensiunea directorului cozii de solicitare în funcție de configurația serverului.

10. În blocul **Connection to Sandbox servers**, fă clic pe butonul **Add**.

11. Se deschide o fereastră; în fereastră, introduceți adresa serverului Kaspersky Sandbox (IPv4, IPv6, DNS) și portul.

    Pentru detalii despre implementarea imaginilor virtuale și configurarea serverelor Sandbox, consultați Ajutor Kaspersky Sandbox.

12. Salvați-vă modificările.

Ca rezultat, Kaspersky Endpoint Security verifică certificatul TLS. Dacă certificatul este verificat cu succes, Kaspersky Endpoint Security încarcă fișierul certificatului pe computer în timpul următoarei sincronizări cu Kaspersky Security Center. Dacă ați adăugat două certificate TLS, Kaspersky Sandbox va utiliza cel mai recent certificat pentru a stabili o conexiune de încredere. Verificați starea de funcționare a componentei, vizualizând *Report on status of application components*. De asemenea, puteți vizualiza starea de funcționare a unei componente în rapoarte, în interfața locală a Kaspersky Endpoint Security. Componenta **Sandbox** va fi adăugată la lista componentelor Kaspersky Endpoint Security.

Puteți activa sau dezactiva integrarea cu Kaspersky Sandbox în Web Console sau local folosind linia de comandă.

Kaspersky Endpoint Security salvează într-un raport informații despre funcționarea componentei Kaspersky Sandbox. Raportul conține și informații despre erori. Dacă primești o eroare cu o descriere care se potrivește cu formatul `Error code: XXX` (de exemplu, `0xa67b01f4`), contactează Suportul tehnic.

Scanare pentru descoperirea indicatorilor de compromitere (activitate independentă)

Un *Indicator de compromitere (IOC)* este un set de date despre un obiect sau o activitate care indică accesul neautorizat la computer (compromiterea datelor). De exemplu, multe încercări nereușite de conectare la sistem pot constitui un Indicator de compromitere. Activitatea *IOC Scan* permite găsirea Indicatorilor de compromitere pe computer și luarea măsurilor de răspuns la amenințări.

Kaspersky Endpoint Security caută indicatorii de compromitere folosind fișiere IOC. *Fișierele IOC* sunt fișiere care conțin seturile de indicatori pe care aplicația încearcă să le potrivească pentru a contoriza o detectare. Fișierele IOC trebuie să fie conforme cu standardul OpenIOC. Kaspersky Endpoint Security generează automat fișiere IOC pentru Kaspersky Sandbox.

Modul de rulare al activității IOC Scan

Aplicația creează activități individuale de scanare IOC pentru Kaspersky Sandbox. *Activitatea individuală de scanare IOC* este o activitate de grup care este creată automat atunci când se reacționează la o amenințare detectată de Kaspersky Sandbox. Kaspersky Endpoint Security generează automat fișierul IOC. Fișierele IOC personalizate nu sunt acceptate. Sarcinile sunt șterse automat după 30 de zile de la momentul creării. Pentru mai multe detalii despre activitățile de scanare IOC autonome, consultați Ajutorul Kaspersky Sandbox.

Setări activitate IOC Scan

Kaspersky Sandbox poate crea și rula automat activități de *IOC Scan* atunci când reacționează la amenințări.

Puteți configura setările numai în Web Console.

Aveți nevoie de Kaspersky Security Center 13.2 pentru ca activitățile individuale de scanare IOC ale Kaspersky Sandbox să funcționeze.

Pentru a modifica setările activității IOC Scan:

1. În fereastra principală a Web Console, selectează **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe activitatea **IOC Scan** a Kaspersky Endpoint Security.

   Se va deschide fereastra de proprietăți a activității.

3. Selectați fila **Application settings**.

4. Accesează secțiunea **IOC Scan settings**.

5. Configurați acțiunile la detectarea IOC:

- **Move copy to Quarantine, delete object**. Dacă această opțiune este selectată, Kaspersky Endpoint Security șterge obiectul rău intenționat găsit pe computer. Înainte de a șterge obiectul, Kaspersky Endpoint Security creează o copie de rezervă în caz că obiectul trebuie restaurat ulterior. Kaspersky Endpoint Security mută copia de rezervă în Carantină.

- **Run Critical Areas Scan**. Dacă această opțiune este selectată, Kaspersky Endpoint Security execută activitatea *Critical Areas Scan*. În mod implicit, Kaspersky Endpoint Security scanează memoria kernel, procesele care se execută și sectoarele de boot ale discurilor.

- **Run only when the computer is idle**. Amânarea începerii activității atunci când resursele computerului sunt ocupate. Kaspersky Endpoint Security pornește activitatea de scanare dacă computerul este blocat sau dacă economizorul de ecran este pornit. Dacă ați întrerupt executarea activității, de exemplu prin deblocarea computerului, Kaspersky Endpoint Security execută automat activitatea, continuând din punctul în care a fost întreruptă. Această opțiune de planificare vă permite să conservați resursele computerului atunci când acesta este utilizat.

6. Salvați-vă modificările.

Puteți vizualiza rezultatele căutării în proprietățile activităților din secțiunea **Results**. Puteți vizualiza informațiile despre indicatorii de compromitere detectați în proprietățile activității: **Application settings** → **IOC Scan results**.

Rezultatele scanării IOC sunt păstrate timp de 30 de zile. După această perioadă, Kaspersky Endpoint Security șterge automat intrările cele mai vechi.

Ghid pentru migrarea KEA la KES pentru Kaspersky Sandbox

Kaspersky Endpoint Security for Windows include un agent încorporat pentru soluția Kaspersky Sandbox. Nu mai aveți nevoie de o aplicați Kaspersky Endpoint Agent separată pentru a utiliza Kaspersky Sandbox. Toate funcțiile Kaspersky Endpoint Agent vor fi efectuate de Kaspersky Endpoint Security.

Când implementați Kaspersky Endpoint Security pe computere care au instalat Kaspersky Endpoint Agent, soluția Kaspersky Sandbox va continua să funcționeze cu Kaspersky Endpoint Security. În plus, Kaspersky Endpoint Agent va fi eliminat din computer. Același comportament în sistem va avea loc atunci când actualizați Kaspersky Endpoint Security la versiunea 11.7.0 sau o versiune ulterioară.

Componenta Kaspersky Endpoint Security nu este compatibilă cu Kaspersky Endpoint Agent. Nu puteți instala ambele aplicații pe același computer.

Următoarele condiții trebuie îndeplinite pentru ca Kaspersky Endpoint Security să funcționeze ca parte a Kaspersky Sandbox:

- Kaspersky Sandbox versiunea 2.0 sau o versiune ulterioară.

- Kaspersky Security Center versiunea 13.2 sau o versiune ulterioară (inclusiv Agentul de rețea). În versiunile anterioare ale Kaspersky Security Center, este imposibil de activat caracteristica Kaspersky Sandbox.

- Kaspersky Sandbox poate fi gestionată numai utilizând Kaspersky Security Center Web Console.

- Transferul de date pe Serverul de administrare este activat. Datele sunt necesare pentru a obține informații despre fișierele carantinate pe un computer prin Web Console.

- Este stabilită o conexiune în fundal între Kaspersky Security Center Web Console și Serverul de administrare. Pentru funcționarea Kaspersky Sandbox cu Serverul de administrare prin intermediul Kaspersky Security Center Web Console, trebuie să stabiliți o nouă conexiune securizată, o *conexiune în fundal*.

Pași pentru migrarea configurației [KES+KEA] la [KES+agent încorporat] pentru Kaspersky Sandbox

1. **Se face upgrade pentru plug-in-ul web Kaspersky Endpoint Security**

   Componenta Kaspersky Sandbox poate fi gestionată utilizând Plag-in-ul web Kaspersky Endpoint Security versiunea 11.7.0 sau o versiune ulterioară.

2. **Migrarea politicilor și activităților**

   Transferați setările Kaspersky Endpoint Agent la Kaspersky Endpoint Security for Windows. Pentru a face acest lucru, utilizați expertul pentru migrarea de la Kaspersky Endpoint Agent în Web Console.

   Cum se migrează setările politicilor și ale activităților de la Kaspersky Endpoint Agent la Kaspersky Endpoint Security în Web Console

   În fereastra principală a Web Console, selectați **Operations → Migration from Kaspersky Endpoint Agent**.

   Aceasta execută Expertul de migrare a politicilor și activităților. Urmează instrucțiunile din expert.

   Pasul 1. Migrarea politicii

   Expertul de migrare creează o nouă politică ce combină setările politicilor Kaspersky Endpoint Security și Kaspersky Endpoint Agent. În lista de politici, selectați politicile Kaspersky Endpoint Agent ale căror setări doriți să le îmbinați cu politica Kaspersky Endpoint Security. Faceți clic pe politica Kaspersky Endpoint Agent pentru a selecta Kaspersky Endpoint Security cu care doriți să îmbinați setările. Asigurați-vă că ați selectat politicile corecte și treceți la pasul următor.

   Pasul 2. Migrarea activităților

   Expertul pentru migrare creează noi activități pentru Kaspersky Endpoint Security. În lista de activități, selectați activitățile Kaspersky Endpoint Agent pe care doriți să le creați pentru politica Kaspersky Endpoint Security. Mergeți la pasul următor.

   Pasul 3. Finalizarea expertului

   Ieșiți din Expert. Ca rezultat, expertul efectuează următoarele acțiuni:

   - Creează o nouă politică Kaspersky Endpoint Security.

Politica va combina setările de la Kaspersky Endpoint Security și Kaspersky Endpoint Agent. Politica se numește *<Kaspersky Endpoint Security policy name> & <Kaspersky Endpoint Agent policy name>*. Noua politică are starea *Inactive*. Pentru a continua, modificați stările politicilor Kaspersky Endpoint Agent și Kaspersky Endpoint Security în *Inactive* și activați noua politică îmbinată.

După migrarea de la Kaspersky Endpoint Agent la Kaspersky Endpoint Security for Windows, asigurați-vă că noua politică are setarea funcționalitatea pentru transferul datelor către Serverul de administrare (date despre fișierul carantină și date despre lanțul de dezvoltare a amenințării). Valorile parametrului pentru transferul de date nu sunt migrate dintr-o politică Kaspersky Endpoint Agent.

- Creează noi activități de Kaspersky Endpoint Security.

  Noile activități sunt copii ale activităților Kaspersky Endpoint Agent. În același timp, Expertul lasă activitățile componentei Kaspersky Endpoint Agent neschimbate.

3 Licențierea funcționalității Kaspersky Sandbox

Pentru a activa Kaspersky Endpoint Security ca parte a soluției Kaspersky Sandbox, aveți nevoie de o licență separată pentru suplimentul Kaspersky Sandbox. Puteți adăuga cheia utilizând activitatea *Add key*. Ca rezultat, două chei vor fi adăugate la aplicație: *Kaspersky Endpoint Security* și *Kaspersky Sandbox*.

4 Instalarea/efectuarea upgrade-ului aplicației Kaspersky Endpoint Security

Pentru a migra funcționalitatea Kaspersky Sandbox în timpul instalării sau efectuării upgrade-ului unei aplicații, se recomandă utilizarea activității de instalare la distanță. Când creați o activitate de instalare la distanță, trebuie să selectați componenta Kaspersky Sandbox în setările pachetului de instalare.

De asemenea, puteți face upgrade aplicației utilizând următoarele metode:

- Utilizând serviciul de actualizare Kaspersky.
- Local, folosind Expertul de configurare.

Kaspersky Endpoint Security acceptă selectarea automată a componentelor atunci când se face upgrade-ul unei aplicații pe un computer pe care este instalată aplicația Kaspersky Endpoint Agent. Selectarea automată a componentelor depinde de permisiunile contului de utilizator care face upgrade-ul aplicației.

Dacă faceți upgrade pentru Kaspersky Endpoint Security utilizând fișierul EXE sau MSI din contul de sistem (SYSTEM), Kaspersky Endpoint Security obține acces la licențele curente ale soluțiilor Kaspersky. Prin urmare, dacă pe computer este instalat, de exemplu, Kaspersky Endpoint Agent și soluția Kaspersky Sandbox este activată, programul de instalare Kaspersky Endpoint Security configurează automat setul de componente și selectează componenta Kaspersky Sandbox. Acest lucru determină componenta Kaspersky Endpoint Security să treacă la utilizarea agentului încorporat și elimină Kaspersky Endpoint Agent. Executarea programului de instalare MSI din contul de sistem (SYSTEM) este efectuată, de obicei, atunci când se face upgrade prin intermediul serviciului de actualizare Kaspersky sau când se implementează un pachet de instalare prin Kaspersky Security Center.

Dacă faceți upgrade pentru Kaspersky Endpoint Security utilizând un fișier MSI dintr-un cont de utilizator fără privilegii, Kaspersky Endpoint Security nu obține acces la licențele curente ale soluțiilor Kaspersky. În acest caz, Kaspersky Endpoint Security selectează automat componentele pe baza configurației Kaspersky Endpoint Agent. Ulterior, componenta Kaspersky Endpoint Security comută la utilizarea agentului încorporat și elimină Kaspersky Endpoint Agent.

Kaspersky Endpoint Security acceptă efectuarea upgrade-ului fără repornirea computerului. Puteți selecta modul de efectuare a upgrade-ului aplicației în proprietățile politicii.

5 Verificarea funcționării aplicației

Dacă după instalarea sau efectuarea upgrade-ului aplicației, computerul are starea *Critical* în consola Kaspersky Security Center:

- asigurați-vă că Agentul de rețea versiunea 13.2 sau o versiune ulterioară este instalată pe computer.
- Verificați starea de funcționare a agentului încorporat, vizualizând *Report on status of application components*. Dacă o componentă are starea *Not installed*, instalați componenta, utilizând activitatea *Change application components*. Dacă o componentă are starea *Nu este acoperită de licență*, asigurați-vă că ați activat funcționalitatea agentului încorporat.
- Asigurați-vă că acceptați Declarația Kaspersky Security Network în noua politică a Kaspersky Endpoint Security for Windows.

Kaspersky Anti Targeted Attack Platform



Kaspersky Endpoint Security for Windows acceptă lucrul cu soluția Kaspersky Anti Targeted Attack Platform (EDR (KATA)). *Kaspersky Anti Targeted Attack Platform* este o soluție concepută pentru detectarea în timp util a amenințărilor sofisticate, cum ar fi atacuri direcționate, amenințări persistente avansate (APT), atacuri zero-day și altele. Kaspersky Anti Targeted Attack Platform include trei unități funcționale:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Poți achiziționa separat toate unitățile funcționale sau unitățile funcționale individuale. Pentru informații detaliate despre soluție, consultați Ajutor pentru Kaspersky Anti Targeted Attack Platform. Aplicația include agenți încorporați pentru componente EDR, NDR. Aplicația acceptă și lucrul cu componenta Sandbox care face parte din KATA.

Instrumente Threat Intelligence

Kaspersky Endpoint Detection and Response utilizează următoarele instrumente Threat Intelligence:

- Integrarea cu Portalul Kaspersky Threat Intelligence, care conține și afișează informații despre reputația fișierelor și a adreselor web.
- Baza de date Kaspersky Threats.
- Infrastructura serviciului clould al Kaspersky Security Network (denumit în continuare „KSN”), care oferă acces la informații în timp real despre reputația fișierelor, site-urilor web și a software-urilor din baza de cunoștințe Kaspersky. Utilizarea datelor de la Kaspersky Security Network asigură răspunsul mai rapid al aplicațiilor Kaspersky la amenințări, îmbunătățește performanța unor componente de protecție și reduce posibilitatea alarmelor false.

Principiul de funcționare al soluției

Kaspersky Endpoint Security este instalat pe computere individuale din infrastructura IT corporativă și monitorizează continuu procesele, conexiunile la rețea deschise și fișierele care sunt modificate. Informațiile despre evenimentele de pe computer (date de telemetrie) sunt trimise către serverul Kaspersky Anti Targeted Attack Platform. În acest caz, aplicația Kaspersky Endpoint Security trimite, de asemenea, informații către serverul Kaspersky Anti Targeted Attack Platform despre amenințările descoperite de aplicație, precum și informații despre rezultatele procesării pentru aceste amenințări.

Integrarea EDR (KATA) și NDR (KATA) este configurată pe consola Kaspersky Security Center. Agentul încorporat este apoi gestionat utilizând consola Kaspersky Anti Targeted Attack Platform, inclusiv executarea activităților, gestionarea obiectelor aflate în carantină, vizualizarea rapoartelor și alte acțiuni.

Configurații Kaspersky Endpoint Security pentru lucrul cu EDR / NDR (KATA)

Următoarele configurații pot fi utilizate pentru a lucra cu EDR / NDR (KATA):

- **[KES+agent încorporat]**. În această configurație, Kaspersky Endpoint Security acționează atât ca aplicație care asigură securitatea computerului, cât și ca aplicație pentru lucrul cu EDR / NDR (KATA). Agentul încorporat pentru EDR (KATA) este disponibil în Kaspersky Endpoint Security 12.1 for Windows sau o versiune ulterioară. Agentul încorporat pentru NDR (KATA) este disponibil în Kaspersky Endpoint Security 12.7 for Windows sau o versiune ulterioară.

- **[EPP terță+agent EPP+EDR]**. În această configurație, securitatea infrastructurii IT este asigurată de platforma de Endpoint Protection Platform (EPP) terță. Interacțiunea cu EDR/NDR (KATA) este asigurată de Kaspersky Endpoint Security în configurația Endpoint Detection and Response Agent (Agent EDR). În această configurație, EDR Agent este compatibil cu aplicațiile EPP terțe. EDR Agent pentru EDR (KATA) este disponibil în Kaspersky Endpoint Security 12.3 for Windows sau o versiune ulterioară. EDR Agent pentru NDR (KATA) este disponibil în Kaspersky Endpoint Security 12.7 for Windows sau o versiune ulterioară.

Suport pentru versiunile anterioare ale Kaspersky Endpoint Security

Dacă utilizați Kaspersky Endpoint Security 11.2.0–11.8.0 pentru interoperabilitatea cu Kaspersky Anti Targeted Attack Platform (EDR), aplicația include Kaspersky Endpoint Agent. Puteți instala Kaspersky Endpoint Agent împreună cu Kaspersky Endpoint Security.

Dacă utilizați Kaspersky Endpoint Security 11.9.0 – 12.0, trebuie să instalați Kaspersky Endpoint Agent separat, deoarece, începând cu Kaspersky Endpoint Security 11.9.0, pachetul de distribuție Kaspersky Endpoint Agent nu mai face parte din kitul de distribuție Kaspersky Endpoint Security.

Integrarea agentului încorporat cu EDR / NDR (KATA)

Pentru integrarea cu EDR / NDR (KATA), trebuie să adaugi componenta relevantă: Endpoint Detection and Response (KATA) sau Network Detection and Response (KATA). Poți selecta componente pentru integrarea cu EDR / NDR (KATA) în timpul instalării sau efectuării upgrade-ului aplicației, precum și utilizând activitatea *Modificare componente ale aplicației*.

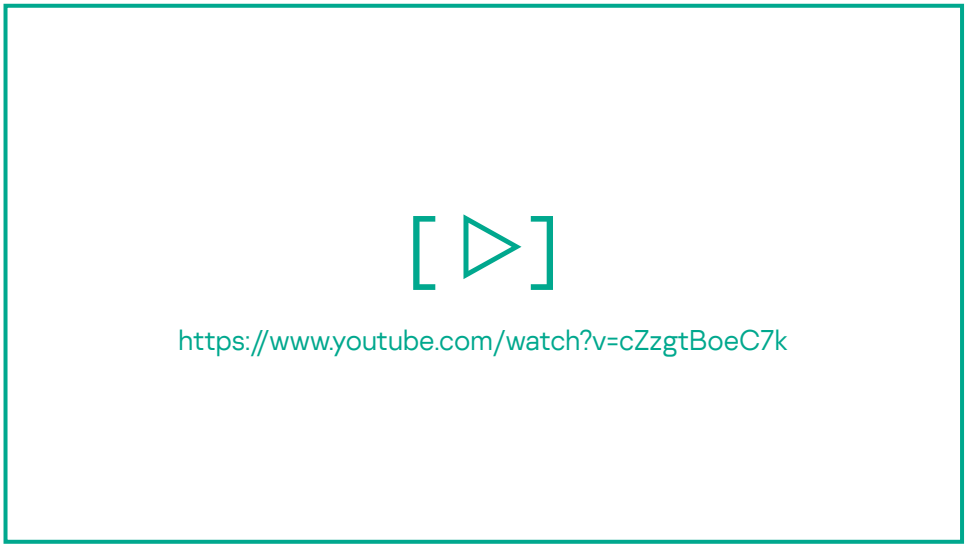
Începând cu versiunea 12.11 a Kaspersky Endpoint Security for Windows, componenta EDR (KATA) a fost redenumită ca **Endpoint Detection and Response Expert (version 8.0 or later)**. În această versiune a aplicației, componenta este compatibilă cu Kaspersky Anti Targeted Attack Platform 7.1 și versiunile anterioare, precum și cu Kaspersky Endpoint Detection and Response Expert (on-premises).

Componentele Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud) și Endpoint Detection and Response Expert (on-premises) nu sunt compatibile între ele.

Pentru a utiliza EDR / NDR (KATA), trebuie îndeplinite următoarele condiții:

- EDR (KATA): Kaspersky Anti Targeted Attack Platform versiunile 5.0–7.1.
- NDR (KATA): Kaspersky Anti Targeted Attack Platform versiunea 7.0 sau o versiune ulterioară.
- EDR (KATA): Kaspersky Endpoint Security for Windows 12.1 sau versiunile ulterioare. Pentru mai multe detalii despre compatibilitatea KATA cu diferite versiuni de Kaspersky Endpoint Security, vezi secțiunea de Ajutor pentru Kaspersky Anti Targeted Attack Platform.
- NDR (KATA): Kaspersky Endpoint Security for Windows 12.7 sau versiunile ulterioare.
- Kaspersky Security Center versiunea 14.2 sau o versiune ulterioară. În versiunile anterioare ale Kaspersky Security Center, este imposibil de activat funcționalitatea EDR / NDR (KATA).
- Aplicația este activată și funcționalitatea este acoperită de licență.
- Componentele Endpoint Detection and Response (KATA) și Network Detection and Response (KATA) sunt activate.
- Componentele aplicației care asigură funcționarea EDR / NDR (KATA) sunt activate și operaționale. Următoarele componente asigură funcționarea EDR / NDR (KATA):
  - File Threat Protection.
  - Web Threat Protection.
  - Mail Threat Protection.
  - Exploit Prevention.
  - Behavior Detection.
  - Host Intrusion Prevention.

- Protecție AMSI.
- Scanare în fundal.
- Kaspersky Security Network.





Integrarea cu Kaspersky Endpoint Detection and Response (KATA) presupune următorii pași:

1. **Instalarea componentelor Endpoint Detection and Response (KATA) și Network Detection and Response (KATA)**

   Poți selecta componentele EDR (KATA) și NDR (KATA) în timpul instalării sau efectuării upgrade-ului, precum și utilizând activitatea *Modificare componente ale aplicației*.

   > Trebuie să reporniți computerul pentru a finaliza efectuarea upgrade-ului aplicației cu noile componente.

2. **Activarea componentelelor Endpoint Detection and Response (KATA) și Network Detection and Response (KATA)**

   Trebuie să achiziționezi o licență separată pentru EDR (KATA) și NDR (KATA) (de exemplu, suplimentul Kaspersky Endpoint Detection and Response (KATA)).

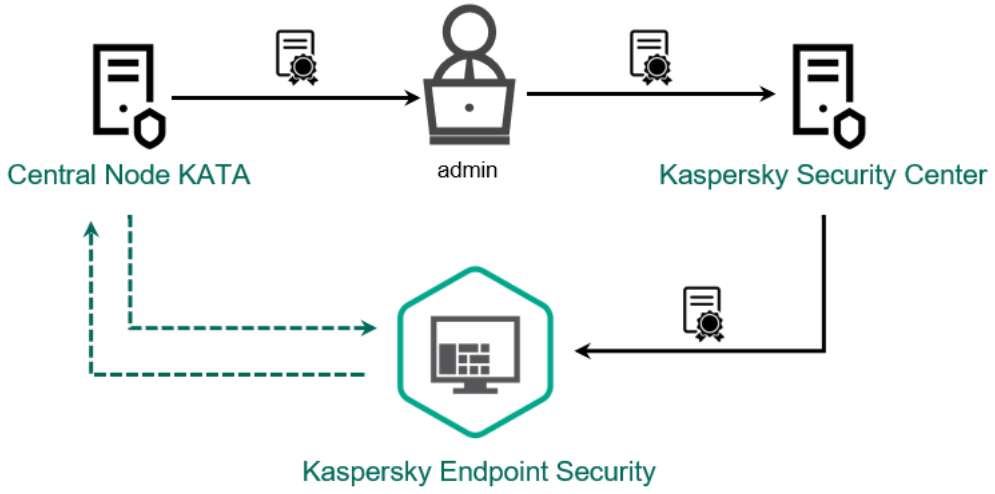
   Funcționalitatea devine disponibilă după adăugarea unei chei separate care acoperă funcționalitățile EDR (KATA) și NDR (KATA). Ca rezultat, sunt adăugate mai multe chei pe computer: o cheie pentru Kaspersky Endpoint Security și chei pentru Kaspersky Endpoint Detection and Response (KATA) și Network Detection and Response (KATA).

Licențierea funcționalităților autonome EDR (KATA) și NDR (KATA) se realizează la fel ca licențierea componentei Kaspersky Endpoint Security.

Asigurați-vă că ambele funcționalități EDR (KATA) și NDR (KATA) sunt incluse în licență și că aceasta se execută în interfața locală a aplicației.

3 Conectarea la Central Node

Kaspersky Anti Targeted Attack Platform necesită stabilirea unei conexiuni de încredere între Kaspersky Endpoint Security și componenta Central Node. Pentru a configura o conexiune de încredere, trebuie să utilizați un certificat TLS. Puteți obține un certificat TLS în consola Kaspersky Anti Targeted Attack Platform (consultați instrucțiunile din Ajutor Kaspersky Anti Targeted Attack Platform). Apoi, trebuie să adăugați certificatul TLS la Kaspersky Endpoint Security (consultați instrucțiunile de mai jos).



Adăugarea unui certificat TLS la Kaspersky Endpoint Security

În mod implicit, Kaspersky Endpoint Security verifică doar certificatul TLS al componentei Central Node. Pentru a face conexiunea mai sigură, puteți activa suplimentar verificarea computerului în Central Node (autentificare mutuală). Pentru a activa această verificare, trebuie să activați autentificarea mutuală în setările Central Node și Kaspersky Endpoint Security. Pentru a utiliza autentificarea mutuală, veți avea nevoie și de un cripto-container. Un *cripto-container* este o arhivă PFX cu un certificat și o cheie privată. Puteți obține un cripto-container în consola Kaspersky Anti Targeted Attack Platform (consultați instrucțiunile din Ajutor Kaspersky Anti Targeted Attack Platform).

Cum conectați un computer Kaspersky Endpoint Security la Central Node utilizând Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați **Policies**.
3. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
4. În fereastra politicii, selectează **Detection and Response** și selectează componenta pe care dorești să o configurezi: **Endpoint Detection and Response Expert (on-premises)** sau **Network Detection and Response (KATA)**.
5. Bifează caseta de selectare corespunzătoare: **Endpoint Detection and Response Expert (versiunea 7.1 sau o versiune anterioară)** sau **Network Detection and Response (KATA)**.
6. Fă clic pe **Setări conectare server**.

7. Configurați conexiunea la server:

   - **Expirare (sec)**. Expirarea timpului maxim de răspuns al serverului Central Node. Când timpul de expirare se termină, Kaspersky Endpoint Security încearcă să se conecteze la un alt server Central Node.

   - **Certificat TLS server**. Certificat TLS pentru stabilirea unei conexiuni de încredere cu serverul Central Node. Puteți obține un certificat TLS în consola Kaspersky Anti Targeted Attack Platform (consultați instrucțiunile din Ajutor Kaspersky Anti Targeted Attack Platform).

   - **Utilizează autentificarea mutuală**. Autentificare mutuală la stabilirea unei conexiuni securizate între Kaspersky Endpoint Security și serverul Central Node. Pentru a utiliza autentificarea mutuală, trebuie să activezi autentificarea mutuală în setările serverului Central Node, apoi să obții un container crypto și să setezi o parolă pentru a proteja containerul crypto. Un *cripto-container* este o arhivă PFX cu un certificat și o cheie privată. Puteți obține un cripto-container în consola Kaspersky Anti Targeted Attack Platform (consultați instrucțiunile din Ajutor Kaspersky Anti Targeted Attack Platform). După configurarea setărilor Central Node, trebuie să activați și autentificarea mutuală în setările Kaspersky Endpoint Security și să încărcați un container crypto protejat prin parolă.

     Criptocontainerul trebuie să fie protejat prin parolă. Nu este posibil să adăugați un criptocontainer cu o parolă necompletată.

8. Fă clic pe **OK**.

9. Adăugați servere Central Node. Pentru a face acest lucru, specificați adresa serverului (IPv4, IPv6) și portul de conectare la server.

   Poți adăuga mai multe adrese de server Central Node. Kaspersky Endpoint Security încearcă să se conecteze la server la prima adresă IP. Dacă nu se poate stabili o conexiune, Kaspersky Endpoint Security încearcă să se conecteze la a doua adresă IP din listă și așa mai departe.

10. Dacă este necesar, configurează telemetria.

11. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum conectați un computer Kaspersky Endpoint Security la Central Node utilizând Web Console

1. În fereastra principală a Web Console, selectați fila **Asset management → Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesează secțiunea **Built-in Agents Configuration** și selectează componenta pe care dorești să o configurezi: **Endpoint Detection and Response Expert (on-premises)** sau **Network Detection and Response (KATA)**.

5. Activează comutatorul corespunzător: **Endpoint Detection and Response Expert (on-premises) ENABLED** sau **Network Detection and Response (KATA) ENABLED**.

6. Pentru a configura EDR (KATA), selectează **Endpoint Detection and Response Expert (version 7.1 or earlier)** din lista de soluții.

7. Fă clic pe **Connection settings**.

8. Configurați conexiunea la server:

   - **Timeout (sec)**. Expirarea timpului maxim de răspuns al serverului Central Node. Când timpul de expirare se termină, Kaspersky Endpoint Security încearcă să se conecteze la un alt server Central Node.

   - **Server certificate**. Certificat TLS pentru stabilirea unei conexiuni de încredere cu serverul Central Node. Puteți obține un certificat TLS în consola Kaspersky Anti Targeted Attack Platform (consultați instrucțiunile din Ajutor Kaspersky Anti Targeted Attack Platform).

   - **Use two-way authentication**. Autentificare mutuală la stabilirea unei conexiuni securizate între Kaspersky Endpoint Security și serverul Central Node. Pentru a utiliza autentificarea mutuală, trebuie să activezi autentificarea mutuală în setările serverului Central Node, apoi să obții un container crypto și să setezi o parolă pentru a proteja containerul crypto. Un *cripto-container* este o arhivă PFX cu un certificat și o cheie privată. Puteți obține un cripto-container în consola Kaspersky Anti Targeted Attack Platform (consultați instrucțiunile din Ajutor Kaspersky Anti Targeted Attack Platform). După configurarea setărilor Central Node, trebuie să activați și autentificarea mutuală în setările Kaspersky Endpoint Security și să încărcați un container crypto protejat prin parolă.

     Criptocontainerul trebuie să fie protejat prin parolă. Nu este posibil să adăugați un criptocontainer cu o parolă necompletată.

9. Fă clic pe **OK**.

10. Adăugați servere Central Node. Pentru a face acest lucru, specificați adresa serverului (IPv4, IPv6) și portul de conectare la server.

    Poți adăuga mai multe adrese de server Central Node. Kaspersky Endpoint Security încearcă să se conecteze la server la prima adresă IP. Dacă nu se poate stabili o conexiune, Kaspersky Endpoint Security încearcă să se conecteze la a doua adresă IP din listă și așa mai departe.

11. Dacă este necesar, configurează telemetria.

12. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

De asemenea, puteți adăuga un certificat TLS local folosind linia de comandă.

Ca rezultat, computerul este adăugat în consola Kaspersky Anti Targeted Attack Platform. Verificați starea de funcționare a componentelor, vizualizând *Report on status of application components*. De asemenea, poți vizualiza starea de funcționare a componentelor în rapoarte, în interfața locală a Kaspersky Endpoint Security. Componentele **Endpoint Detection and Response Expert (version 8.0 or later)** și Network Detection and Response (KATA) vor fi adăugate la lista componentelor Kaspersky Endpoint Security.

Poți verifica starea componentelor din consola Kaspersky Security Center în proprietățile computerului din secțiunea **Components**. Ține cont de următoarele aspecte când verifici starea componentei în consolă. În cazul în care componenta nu este instalată și funcționalitatea nu este acoperită de licența ta, consola afișează starea **Not supported by license** în loc de **Not installed**.

Începând cu Kaspersky Endpoint Security 12.6 for Windows, poți monitoriza starea componentei EDR (KATA) în Consola de administrare Kaspersky Security Center (MMC). Starea curentă a componentei este afișată în proprietățile computerului din coloana **Endpoint Sensor status** (*Running*, *Starting*, *Stopped*, *Paused*, *Failed*, *Unknown*). Web Console nu afișează starea pentru Endpoint Sensor.

Configurarea telemetriei EDR (KATA)

Telemetrie este o listă de evenimente care au avut loc pe computerul protejat. Kaspersky Endpoint Security analizează datele de telemetrie și le trimite către Kaspersky Anti Targeted Attack Platform în timpul sincronizării. Evenimentele de telemetrie ajung pe server aproape continuu. Kaspersky Endpoint Security inițiază sincronizarea cu serverul atunci când este îndeplinită oricare dintre următoarele condiții:

- intervalul de sincronizare a expirat;
- numărul de evenimente din memoria tampon depășește limita superioară.

Prin urmare, în mod implicit, aplicația se sincronizează la fiecare 30 de secunde sau ori de câte ori memoria tampon conține 1024 de evenimente. Puteți configura comportamentul de sincronizare în politica Kaspersky Endpoint Security și puteți selecta valorile optime care să corespundă încărcării rețelei dvs. (consultați instrucțiunile de mai jos).

Dacă nu există nicio conexiune între Kaspersky Endpoint Security și server, aplicația pune în coadă evenimentele noi. Când conexiunea este restabilită, Kaspersky Endpoint Security trimite evenimentele din coadă către server în ordinea corespunzătoare. Pentru a evita supraîncărcarea serverului, Kaspersky Endpoint Security poate sări peste unele evenimente. Pentru a activa acest lucru, puteți optimiza setările de transmitere a evenimentelor, de exemplu, puteți seta o valoare maximă pentru numărul evenimentelor pe oră (consultați instrucțiunile de mai jos).

Dacă utilizați Kaspersky Anti Targeted Attack Platform împreună cu o altă soluție care utilizează, de asemenea, telemetria, puteți dezactiva telemetria pentru KATA (EDR) (consultați instrucțiunile de mai jos). Acest lucru vă permite să optimizați încărcarea serverului pentru aceste soluții. De exemplu, dacă aveți soluțiile Managed Detection and Response și KATA (EDR) implementate, puteți utiliza telemetria MDR și puteți crea activități Răspuns la amenințare în KATA (EDR).

Cum se configurează telemetria în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați **Policies**.
3. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
4. În fereastra politicii, selectează **Detection and Response** și selectează componenta pe care dorești să o configurezi: **Endpoint Detection and Response Expert (on-premises)** sau **Network Detection and Response (KATA)**.
5. Configurați setarea **Trimite solicitarea de sincronizare la serverul KATA la fiecare (min)**. Frecvența solicitărilor de sincronizare trimise către serverul. În timpul sincronizării, Kaspersky Endpoint Security trimite informații despre setările și activitățile modificate ale aplicației.
6. Asigurați-vă că este selectată caseta de validare **Trimite telemetrie către KATA**.
7. Dacă este necesar, configurează sincronizarea cu setările serverului în blocul **Setări transmitere date**:
   - **Întârziere maximă între transmiterea evenimentelor (sec)**. Aplicația se sincronizează cu serverul pentru a trimite evenimente după expirarea intervalului de sincronizare. Valoarea implicită este 30 de secunde.
   - **Numărul maxim de evenimente de pachete**. Aplicația se sincronizează cu serverul atunci când memoria tampon este umplută cu evenimente. Valoarea implicită este de 1024 de evenimente.

8. Dacă este necesar, bifați caseta de selectare **Activează limitarea solicitărilor** din blocul **Limitarea solicitărilor**.

   Această caracteristică ajută la optimizarea încărcării serverului. Dacă această funcționalitate este activată, aplicația restricționează transmiterea evenimentului. Dacă numărul de evenimente depășește limitele configurate, Kaspersky Endpoint Security oprește trimiterea evenimentelor.

9. Configurați setările de optimizare pentru trimiterea evenimentelor către server:

   - **Numărul maxim de evenimente pe oră**. Aplicația analizează fluxul de date de telemetrie și restricționează trimiterea evenimentelor dacă fluxul de evenimente depășește limita de evenimente pe oră configurată. Kaspersky Endpoint Security reia trimiterea evenimentelor după o oră. Valoarea implicită este de 3000 de evenimente pe oră. Dacă aplicația este instalată pe un server, fluxul de date de telemetrie este mai mare. Pentru servere, se recomandă creșterea valorii la 60.000 de evenimente pe oră.

   - **Procentajul depășirii limitei de evenimente**. Aplicația sortează evenimentele după tip (de exemplu, evenimente „modificări în registry") și restricționează transmiterea evenimentelor dacă raportul dintre evenimente de același tip și numărul total de evenimente depășește limita configurată în procente. Kaspersky Endpoint Security reia trimiterea evenimentelor atunci când raportul dintre alte evenimente și numărul total de evenimente devine din nou suficient de mare. Valoarea implicită este 15%.

10. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se configurează telemetria în Web Console

1. În fereastra principală a Web Console, selectați fila **Asset management → Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **Built-in Agents Configuration → Endpoint Detection and Response Expert (on-premises)**.

5. Pentru a configura EDR (KATA), selectează **Endpoint Detection and Response Expert (version 7.1 or earlier)** din lista de soluții.

6. Asigură-te că ai bifat caseta de selectare **Send telemetry to KATA servers** din blocul **Data transmission settings**.

7. Configurați setarea **Send sync request to server every (min)**. Frecvența solicitărilor de sincronizare trimise către serverul. În timpul sincronizării, Kaspersky Endpoint Security trimite informații despre setările și activitățile modificate ale aplicației.

8. Asigurați-vă că este selectată caseta de validare **Send telemetry to KATA servers**.

9. Dacă este necesar, configurează sincronizarea cu setările serverului în blocul **Data transmission settings**:

   - **Maximum event transmission delay (sec)**. Aplicația se sincronizează cu serverul pentru a trimite evenimente după expirarea intervalului de sincronizare. Valoarea implicită este 30 de secunde.

   - **Maximum number of event packages**. Aplicația se sincronizează cu serverul atunci când memoria tampon este umplută cu evenimente. Valoarea implicită este de 1024 de evenimente.

10. Dacă este necesar, bifați caseta de selectare **Enable request throttling** din blocul **Request throttling**.

    Această caracteristică ajută la optimizarea încărcării serverului. Dacă această funcționalitate este activată, aplicația restricționează transmiterea evenimentului. Dacă numărul de evenimente depășește limitele configurate, Kaspersky Endpoint Security oprește trimiterea evenimentelor.

11. Configurați setările de optimizare pentru trimiterea evenimentelor către server:

    - **Maximum number of events per hour**. Aplicația analizează fluxul de date de telemetrie și restricționează trimiterea evenimentelor dacă fluxul de evenimente depășește limita de evenimente pe oră configurată. Kaspersky Endpoint Security reia trimiterea evenimentelor după o oră. Valoarea implicită este de 3000 de evenimente pe oră. Dacă aplicația este instalată pe un server, fluxul de date de telemetrie este mai mare. Pentru servere, se recomandă creșterea valorii la 60.000 de evenimente pe oră.

    - **Percentage of event limit excess**. Aplicația sortează evenimentele după tip (de exemplu, evenimente „modificări în registry") și restricționează transmiterea evenimentelor dacă raportul dintre evenimente de același tip și numărul total de evenimente depășește limita configurată în procente. Kaspersky Endpoint Security reia trimiterea evenimentelor atunci când raportul dintre alte evenimente și numărul total de evenimente devine din nou suficient de mare. Valoarea implicită este 15%.

12. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesează secțiunea **Integrare KATA** → **Excluderi telemetrie**.

5. În **Setări transmitere date**, bifează caseta de selectare **Utilizează excluderi**.

6. Faceți clic pe **Adăugare** și configurați excluderile:

   Criteriile sunt combinate cu *ȘI* logic.

   - **Cale**. Calea completă către fișier, inclusiv numele și extensia acestuia. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști. Pentru ca excluderea să funcționeze, trebuie specificată calea către fișier.

   - **Linie de comandă**. Comanda folosită pentru a executa obiectul.

   - **Descriere**. Valoarea parametrului FileDescription dintr-o resursă RT_VERSION (VersionInfo).

     Pentru mai multe detalii despre resursa VersionInfo, vizitează site-ul web Microsoft.

   - **Nume original fișier**. Valoarea parametrului OriginalFilename dintr-o resursă RT_VERSION (VersionInfo).

   - **Versiunea**. Valoarea parametrului FileVersion dintr-o resursă RT_VERSION (VersionInfo).

   - **MD5**. Codul hash MD5 al fișierului.

- **SHA256**. Codul hash SHA256 al fișierului.
- **Tipuri evenimente**. Pentru ca excluderea să funcționeze, trebuie să selectați cel puțin un tip de eveniment.

7. Salvați-vă modificările.

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Tasks**.
   Lista activităților se deschide.
2. Fă clic pe **New task**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Selectarea tipului activității

1. Selectați **Kaspersky Endpoint Security for Windows (14.1)** → **Derulare înapoi actualizare**.

Pasul 2. Selectarea dispozitivelor cărora le va fi atribuită activitatea

Selectați computerele pe care se va efectua activitatea. Sunt disponibile următoarele opțiuni:

- Atribuirea activității unui grup de administrare. În acest caz, activitatea este atribuită computerelor incluse într-un grup de administrare creat anterior.
- Selectare computere detectate în rețea de Serverul de administrare: *dispozitive neatribuite*. Dispozitivele specifice pot include dispozitive din grupuri de administrare, precum și dispozitive neatribuite.
- Specificarea manuală a adreselor computerelor sau importarea adreselor dintr-o listă. Poți specifica nume NetBIOS, adrese IP și subrețele IP ale dispozitivelor cărora dorești să le atribui activitatea.

Pasul 3. Configurarea unei planificări de pornire a activității

Configurează planificarea activității, de exemplu, manual.

Pasul 4. Definirea numelui activității

Introdu un nume pentru activitate.

Pasul 7. Finalizarea creării activității

Ieșiți din Expert. Dacă este necesar, bifați caseta de selectare **Run the task after the wizard finishes**. Puteți monitoriza progresul activității în proprietățile activității.

Excluderi telemetrie EDR (KATA)

Pentru a îmbunătăți performanța și a optimiza transmiterea datelor către serverul de telemetrie, poți configura excluderile de telemetrie. De exemplu, poți alege să nu trimiți date de comunicare în rețea pentru aplicații individuale.

Cum se creează o excludere de telemetrie în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Setări generale** → **Excluderi și tipuri de obiecte**.
4. În blocul **Setări telemetrie** → **Telemetrie EDR (KATA) / NDR (KATA)**, fă clic pe butonul **Setări**.
5. În fereastra care se deschide, configurează excluderile de telemetrie (vezi tabelul de mai jos).

   Aplicația combină condițiile de excludere cu AND-ul logic. Pentru a crea o regulă, trebuie să specifici o valoare în câmpul **Cale completă** și să selectezi cel puțin un tip de eveniment în lista **Utilizează pentru următoarele tipuri de evenimente**.
6. Salvați-vă modificările.

Cum se creează o excludere de telemetrie în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **General Settings** → **Telemetry Settings**.
5. Selectați fila **EDR (KATA) / NDR (KATA) telemetry**.
6. În fereastra care se deschide, configurează excluderile de telemetrie (vezi tabelul de mai jos).

   Aplicația combină condițiile de excludere cu AND-ul logic. Pentru a crea o regulă, trebuie să specifici o valoare în câmpul **Full path** și să selectezi cel puțin un tip de eveniment.
7. Salvați-vă modificările.

Parametru	Descriere
Procese excluse	**Optimizează dimensiunea telemetriei de trimis**. Kaspersky Endpoint Security permite optimizarea cantității de date trimise și excluderea evenimentelor cu anumite coduri din telemetrie: codul 102 (comunicații de bază) și 8 (activitatea de rețea a procesului) pentru protocolul Microsoft SMB, serviciul WinRM și procesul klnagent.exe a Agentului de rețea, precum și informații extinse despre tipurile de pachete de rețea pentru toate tipurile de protocoale de rețea. Kaspersky Endpoint Security combină criteriile de declanșare a regulilor cu un AND logic. **Process** și **Parent process**: • **Full path**. Calea completă către fișier, inclusiv numele și extensia acestuia. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști. • **Command line text**. Comandă folosită pentru a executa fișierul. • **Description**. Valoarea parametrului FileDescription dintr-o resursă RT_VERSION (VersionInfo). • **Original file name**. Valoarea parametrului OriginalFilename dintr-o resursă RT_VERSION (VersionInfo). • **Version**. Valoarea parametrului FileVersion dintr-o resursă RT_VERSION (VersionInfo). • **File checksums**. MD5 și SHA256. De asemenea, puteți selecta manual un fișier, iar aplicația va completa automat câmpurile din fișierul selectat. În sistemele de operare pe 64 de biți, trebuie să introduci manual parametrii versiunii pe 64 de biți a fișierului executabil al unui proces din directorul `C:\windows\system32` deoarece aplicația populează câmpurile parametrilor fișierului executabil cu date din proprietățile versiunii pe 32 de biți a aceluiași fișier executabil în directorul `C:\windows\syswow64`. De exemplu, dacă selectezi `C:\windows\system32\cmd.exe`, pluginul afișează parametrii pentru `C:\windows\syswow64\cmd.exe`. Un astfel de comportament este dictat de particularitățile sistemului de operare. **Utilizează pentru următoarele tipuri de evenimente**: • **Modifică fișier**. • **Evenimente de rețea**. • **Proces: introducere interactivă în consolă**. • **Modul încărcat**. • **Registry modificat**. • **Jurnalele DNS**. • **Acces proces**. • **Intruziune cod**. • **Interogarea WMI**. • **Canal**. • **LDAP**. • **AMSI**.
Comunicații în rețea excluse	**Nume regulă**. **Direcție**. **Protocol**. **Soclu brut**. **Număr protocol**. **Certificat TLS**. **Interval sau port local**. **Interval sau port la distanță**. **Adresă locală**. Adresa de rețea a computerului pentru care Kaspersky Endpoint Security exclude telemetria din traficul de rețea. **Adresă la distanță**. Adresa de rețea a computerului pentru care Kaspersky Endpoint Security exclude telemetria din traficul de rețea. Numai formatul IPv4 este acceptat pentru adresele IP. **Aplicații**. Lista fișierelor executabile ale aplicațiilor pentru care Kaspersky Endpoint Security exclude telemetria EDR din traficul de rețea.

Parametru	Descriere
Operații excluse pentru fișiere	**Nume regulă**. **Nume fișier sau mască**. Numele sau masca unui fișier sau director; Kaspersky Endpoint Security aplică regula de excludere atunci când este accesat acest fișier sau director. Kaspersky Endpoint Security acceptă caracterele `*` și `?` la introducerea unei măști. **Tipul operațiunii**. **Calea anterioară**. Kaspersky Endpoint Security combină criteriile de declanșare a regulilor cu un AND logic. **Process** și **Parent process**: • **Full path**. Calea completă către fișier, inclusiv numele și extensia acestuia. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști. • **Command line text**. Comandă folosită pentru a executa fișierul. • **Description**. Valoarea parametrului FileDescription dintr-o resursă RT_VERSION (VersionInfo). • **Original file name**. Valoarea parametrului OriginalFilename dintr-o resursă RT_VERSION (VersionInfo). • **Version**. Valoarea parametrului FileVersion dintr-o resursă RT_VERSION (VersionInfo). • **File checksums**. MD5 și SHA256. De asemenea, puteți selecta manual un fișier, iar aplicația va completa automat câmpurile din fișierul selectat. În sistemele de operare pe 64 de biți, trebuie să introduci manual parametrii versiunii pe 64 de biți a fișierului executabil al unui proces din directorul `C:\windows\system32` deoarece aplicația populează câmpurile parametrilor fișierului executabil cu date din proprietățile versiunii pe 32 de biți a aceluiași fișier executabil în directorul `C:\windows\syswow64`. De exemplu, dacă selectezi `C:\windows\system32\cmd.exe`, pluginul afișează parametrii pentru `C:\windows\syswow64\cmd.exe`. Un astfel de comportament este dictat de particularitățile sistemului de operare.
Operațiuni DNS excluse	**Nume regulă**. Kaspersky Endpoint Security combină criteriile de declanșare a regulilor cu un AND logic. **Process** și **Parent process**: • **Full path**. Calea completă către fișier, inclusiv numele și extensia acestuia. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști. • **Command line text**. Comandă folosită pentru a executa fișierul. • **Description**. Valoarea parametrului FileDescription dintr-o resursă RT_VERSION (VersionInfo). • **Original file name**. Valoarea parametrului OriginalFilename dintr-o resursă RT_VERSION (VersionInfo). • **Version**. Valoarea parametrului FileVersion dintr-o resursă RT_VERSION (VersionInfo). • **File checksums**. MD5 și SHA256. De asemenea, puteți selecta manual un fișier, iar aplicația va completa automat câmpurile din fișierul selectat. În sistemele de operare pe 64 de biți, trebuie să introduci manual parametrii versiunii pe 64 de biți a fișierului executabil al unui proces din directorul `C:\windows\system32` deoarece aplicația populează câmpurile parametrilor fișierului executabil cu date din proprietățile versiunii pe 32 de biți a aceluiași fișier executabil în directorul `C:\windows\syswow64`. De exemplu, dacă selectezi `C:\windows\system32\cmd.exe`, pluginul afișează parametrii pentru `C:\windows\syswow64\cmd.exe`. Un astfel de comportament este dictat de particularitățile sistemului de operare. **DNS**: • **Adresa IP a serverului DNS**. • **Opțiuni de interogare**. • **Stare**. • **Nume domeniu**. • **ID-ul tipului de setări**. • **Date răspuns**.

Parametru	Descriere
Operațiuni LDAP excluse	**Nume regulă**. **Domeniu de căutare LDAP**. **Filtru**. **Nume distinctiv pentru căutarea obiectelor LDAP**. **Atributele obiectului**. Kaspersky Endpoint Security combină criteriile de declanșare a regulilor cu un AND logic. **Process** și **Parent process**: • **Full path**. Calea completă către fișier, inclusiv numele și extensia acestuia. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști. • **Command line text**. Comandă folosită pentru a executa fișierul. • **Description**. Valoarea parametrului FileDescription dintr-o resursă RT_VERSION (VersionInfo). • **Original file name**. Valoarea parametrului OriginalFilename dintr-o resursă RT_VERSION (VersionInfo). • **Version**. Valoarea parametrului FileVersion dintr-o resursă RT_VERSION (VersionInfo). • **File checksums**. MD5 și SHA256. De asemenea, puteți selecta manual un fișier, iar aplicația va completa automat câmpurile din fișierul selectat. În sistemele de operare pe 64 de biți, trebuie să introduci manual parametrii versiunii pe 64 de biți a fișierului executabil al unui proces din directorul `C:\windows\system32` deoarece aplicația populează câmpurile parametrilor fișierului executabil cu date din proprietățile versiunii pe 32 de biți a aceluiași fișier executabil în directorul `C:\windows\syswow64`. De exemplu, dacă selectezi `C:\windows\system32\cmd.exe`, pluginul afișează parametrii pentru `C:\windows\syswow64\cmd.exe`. Un astfel de comportament este dictat de particularitățile sistemului de operare.
Interogări de acces la procese excluse	**Nume regulă**. **Tipul operațiunii**. **Accesul solicitat la proces**. **Urma stivei de apelare**. Kaspersky Endpoint Security combină criteriile de declanșare a regulilor cu un AND logic. **Process**, **Parent process**, **File of the target process**, **Handle to the source process** și **Handle to the target process**. • **Cale completă**. Calea completă către fișier, inclusiv numele și extensia acestuia. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști. • **Text linie de comandă**. Comandă folosită pentru a executa fișierul. • **Specifică criteriile de declanșare a regulii și tipurile de evenimente pentru care se utilizează această regulă**. Valoarea parametrului FileDescription dintr-o resursă RT_VERSION (VersionInfo). • **Nume original fișier**. Valoarea parametrului OriginalFilename dintr-o resursă RT_VERSION (VersionInfo). • **Versiune**. Valoarea parametrului FileVersion dintr-o resursă RT_VERSION (VersionInfo). • **Sume de control**. MD5 și SHA256. De asemenea, puteți selecta manual un fișier, iar aplicația va completa automat câmpurile din fișierul selectat. În sistemele de operare pe 64 de biți, trebuie să introduci manual parametrii versiunii pe 64 de biți a fișierului executabil al unui proces din directorul `C:\windows\system32` deoarece aplicația populează câmpurile parametrilor fișierului executabil cu date din proprietățile versiunii pe 32 de biți a aceluiași fișier executabil în directorul `C:\windows\syswow64`. De exemplu, dacă selectezi `C:\windows\system32\cmd.exe`, pluginul afișează parametrii pentru `C:\windows\syswow64\cmd.exe`. Un astfel de comportament este dictat de particularitățile sistemului de operare.

Parametru	Descriere
Injectări de cod excluse	**Nume regulă**. **Metoda de acces**. **Stiva de apeluri**. **Linia de comandă modificată**. **Adresa de injectare**. **Numele DLL-ului injectat**. Kaspersky Endpoint Security combină criteriile de declanșare a regulilor cu un AND logic. **Process** și **Parent process**: • **Full path**. Calea completă către fișier, inclusiv numele și extensia acestuia. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști. • **Command line text**. Comandă folosită pentru a executa fișierul. • **Description**. Valoarea parametrului FileDescription dintr-o resursă RT_VERSION (VersionInfo). • **Original file name**. Valoarea parametrului OriginalFilename dintr-o resursă RT_VERSION (VersionInfo). • **Version**. Valoarea parametrului FileVersion dintr-o resursă RT_VERSION (VersionInfo). • **File checksums**. MD5 și SHA256. De asemenea, puteți selecta manual un fișier, iar aplicația va completa automat câmpurile din fișierul selectat. În sistemele de operare pe 64 de biți, trebuie să introduci manual parametrii versiunii pe 64 de biți a fișierului executabil al unui proces din directorul `C:\windows\system32` deoarece aplicația populează câmpurile parametrilor fișierului executabil cu date din proprietățile versiunii pe 32 de biți a aceluiași fișier executabil în directorul `C:\windows\syswow64`. De exemplu, dacă selectezi `C:\windows\system32\cmd.exe`, pluginul afișează parametrii pentru `C:\windows\syswow64\cmd.exe`. Un astfel de comportament este dictat de particularitățile sistemului de operare.
Interogări WMI excluse	**Nume regulă**. **Tipul operațiunii WMI**. **Interogarea la distanță**. **Numele unui computer care a executat o comandă WMI**. **Cont utilizator WMI**. **Comanda WMI executată**. **Nume spațiu WMI**. **Filtrul consumatorului evenimentului WMI**. **Numele consumatorului de evenimente WMI creat**. **Codul sursă al unui consumator de evenimente WMI**. Kaspersky Endpoint Security combină criteriile de declanșare a regulilor cu un AND logic. **Process** și **Parent process**: • **Full path**. Calea completă către fișier, inclusiv numele și extensia acestuia. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști. • **Command line text**. Comandă folosită pentru a executa fișierul. • **Description**. Valoarea parametrului FileDescription dintr-o resursă RT_VERSION (VersionInfo). • **Original file name**. Valoarea parametrului OriginalFilename dintr-o resursă RT_VERSION (VersionInfo). • **Version**. Valoarea parametrului FileVersion dintr-o resursă RT_VERSION (VersionInfo). • **File checksums**. MD5 și SHA256. De asemenea, puteți selecta manual un fișier, iar aplicația va completa automat câmpurile din fișierul selectat. În sistemele de operare pe 64 de biți, trebuie să introduci manual parametrii versiunii pe 64 de biți a fișierului executabil al unui proces din directorul `C:\windows\system32` deoarece aplicația populează câmpurile parametrilor fișierului executabil cu date din proprietățile versiunii pe 32 de biți a aceluiași fișier executabil în directorul `C:\windows\syswow64`. De exemplu, dacă selectezi `C:\windows\system32\cmd.exe`, pluginul afișează parametrii pentru `C:\windows\syswow64\cmd.exe`. Un astfel de comportament este dictat de particularitățile sistemului de operare.

Parametru	Descriere
Operațiuni canale excluse	**Nume regulă**. **Nume canal**. **Tipul operațiunii**. Kaspersky Endpoint Security combină criteriile de declanșare a regulilor cu un AND logic. **Process** și **Parent process**: • **Full path**. Calea completă către fișier, inclusiv numele și extensia acestuia. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști. • **Command line text**. Comandă folosită pentru a executa fișierul. • **Description**. Valoarea parametrului FileDescription dintr-o resursă RT_VERSION (VersionInfo). • **Original file name**. Valoarea parametrului OriginalFilename dintr-o resursă RT_VERSION (VersionInfo). • **Version**. Valoarea parametrului FileVersion dintr-o resursă RT_VERSION (VersionInfo). • **File checksums**. MD5 și SHA256. De asemenea, puteți selecta manual un fișier, iar aplicația va completa automat câmpurile din fișierul selectat. În sistemele de operare pe 64 de biți, trebuie să introduci manual parametrii versiunii pe 64 de biți a fișierului executabil al unui proces din directorul `C:\windows\system32` deoarece aplicația populează câmpurile parametrilor fișierului executabil cu date din proprietățile versiunii pe 32 de biți a aceluiași fișier executabil în directorul `C:\windows\syswow64`. De exemplu, dacă selectezi `C:\windows\system32\cmd.exe`, pluginul afișează parametrii pentru `C:\windows\syswow64\cmd.exe`. Un astfel de comportament este dictat de particularitățile sistemului de operare.
Modificări de registry excluse	**Nume regulă**. **Tipul operațiunii**. **Cale**. **Nume valoare**. **Valoare**. **Numele complet al unui fișier de registry**. Kaspersky Endpoint Security combină criteriile de declanșare a regulilor cu un AND logic. **Process** și **Parent process**: • **Full path**. Calea completă către fișier, inclusiv numele și extensia acestuia. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști. • **Command line text**. Comandă folosită pentru a executa fișierul. • **Description**. Valoarea parametrului FileDescription dintr-o resursă RT_VERSION (VersionInfo). • **Original file name**. Valoarea parametrului OriginalFilename dintr-o resursă RT_VERSION (VersionInfo). • **Version**. Valoarea parametrului FileVersion dintr-o resursă RT_VERSION (VersionInfo). • **File checksums**. MD5 și SHA256. De asemenea, puteți selecta manual un fișier, iar aplicația va completa automat câmpurile din fișierul selectat. În sistemele de operare pe 64 de biți, trebuie să introduci manual parametrii versiunii pe 64 de biți a fișierului executabil al unui proces din directorul `C:\windows\system32` deoarece aplicația populează câmpurile parametrilor fișierului executabil cu date din proprietățile versiunii pe 32 de biți a aceluiași fișier executabil în directorul `C:\windows\syswow64`. De exemplu, dacă selectezi `C:\windows\system32\cmd.exe`, pluginul afișează parametrii pentru `C:\windows\syswow64\cmd.exe`. Un astfel de comportament este dictat de particularitățile sistemului de operare.
Operațiuni excluse cu dispozitive	**Nume regulă**. **Tip dispozitiv**. **ID dispozitiv**. **Nume dispozitiv**.

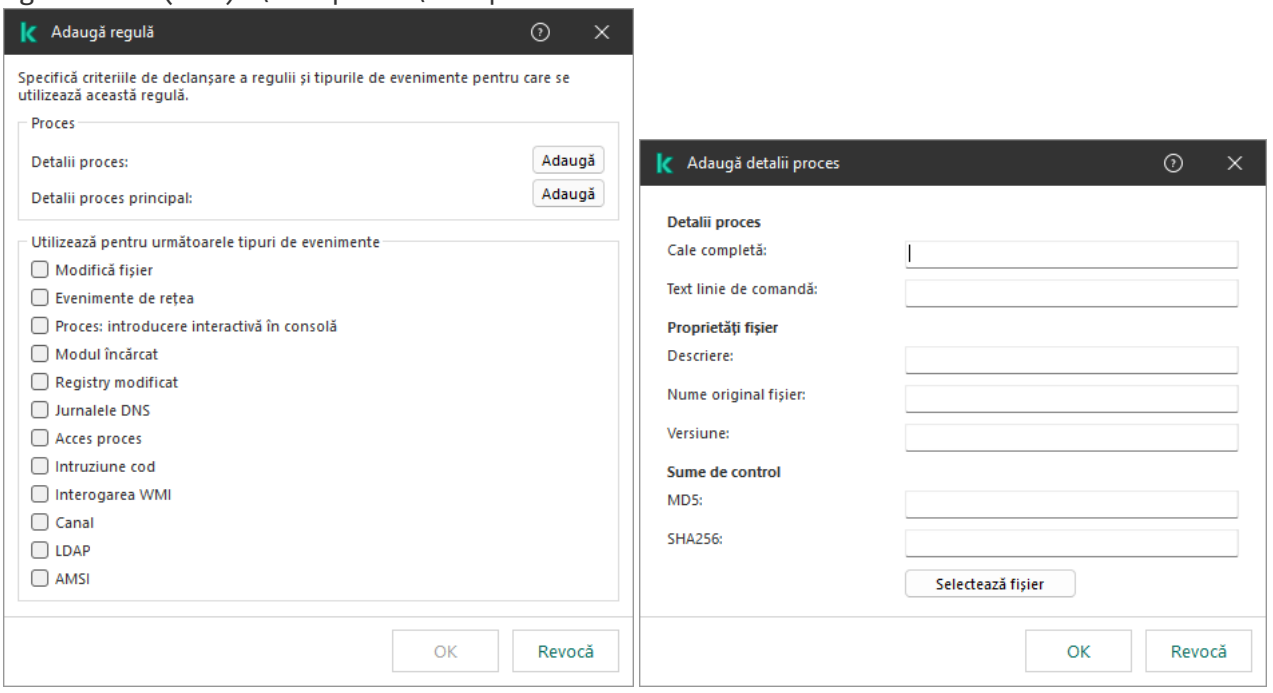
Exemplul 1. Procese excluse

Pentru a exclude din telemetrie evenimentele aplicațiilor (proceselor) terțe, deschide fereastra de excluderi din telemetria EDR în fila **Procese excluse** și adaugă fișierul executabil al aplicației.

Kaspersky Endpoint Security combină criteriile de declanșare a regulilor cu un AND logic.

Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști. De exemplu:

- `C:\Program Files\*\notepad++.exe`
- `%ProgramFiles(x86)%\Notepad++\notepad++.exe`



Excluderea unui proces

Exemplul 1. Modificarea fișierului

Dacă editezi adesea scripturi în aplicația Notepad++ și dorești să excluzi evenimentele de modificare pentru scripturile corespunzătoare, adaugă fișierul executabil Notepad++ la excluderile de telemetrie.

Specifică setările după cum urmează:

- **Cale completă**: `C:\Program Files\Notepad++\notepad++.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.
- **Utilizează pentru următoarele tipuri de evenimente**: Modifică fișier.

Exemplul 2. Evenimente în rețea

Dacă utilizezi aplicația WinSCP pentru a gestiona fișierele de pe un server la distanță și dorești să excluzi evenimentele de rețea, adaugă fișierul executabil WinSCP la excluderile de telemetrie.

Specifică setările după cum urmează:

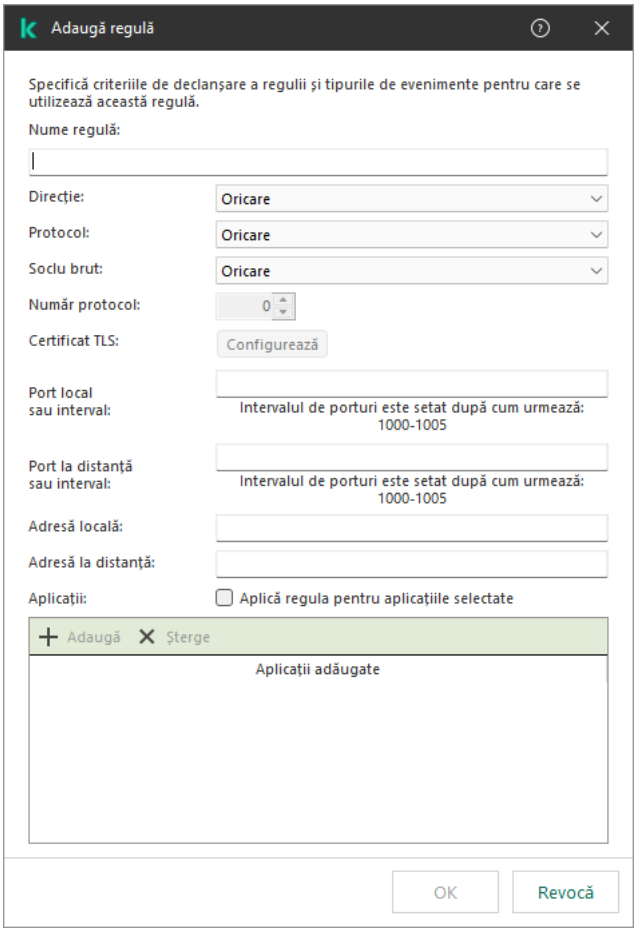
- **Cale completă**: `C:\Program Files (x86)\WinSCP\WinSCP.exe`.
- **SHA256**: 47204338f0e092057024c9186f228c02417e917777f3e841d52b58251a956a74 (optional).
- **Utilizează pentru următoarele tipuri de evenimente**: Evenimente de rețea.

Exemplul 2. Comunicații în rețea excluse

Pentru a exclude evenimentele de conexiune la serviciu la distanță din telemetrie, deschide fereastra de excluderi de la telemetrie EDR în fila **Comunicații în rețea excluse** și adaugă setările conexiunii: protocol, port, direcție, adresă IP, certificat TLS și altele.

Kaspersky Endpoint Security combină criteriile de declanșare a regulilor cu un AND logic.

Nu poți specifica o adresă de subrețea (de exemplu, 10.28.0.0/24). Aplicația permite doar specificarea unei adrese IP (de exemplu, 10.28.0.105).



Excluderea comunicațiilor în rețea

Dacă utilizezi un server web corporativ și dorești să excluzi evenimentele din browser atunci când te conectezi la acel server web, adaugă adresa IP a serverului și fișierul executabil al browserului la excluderile de telemetrie.

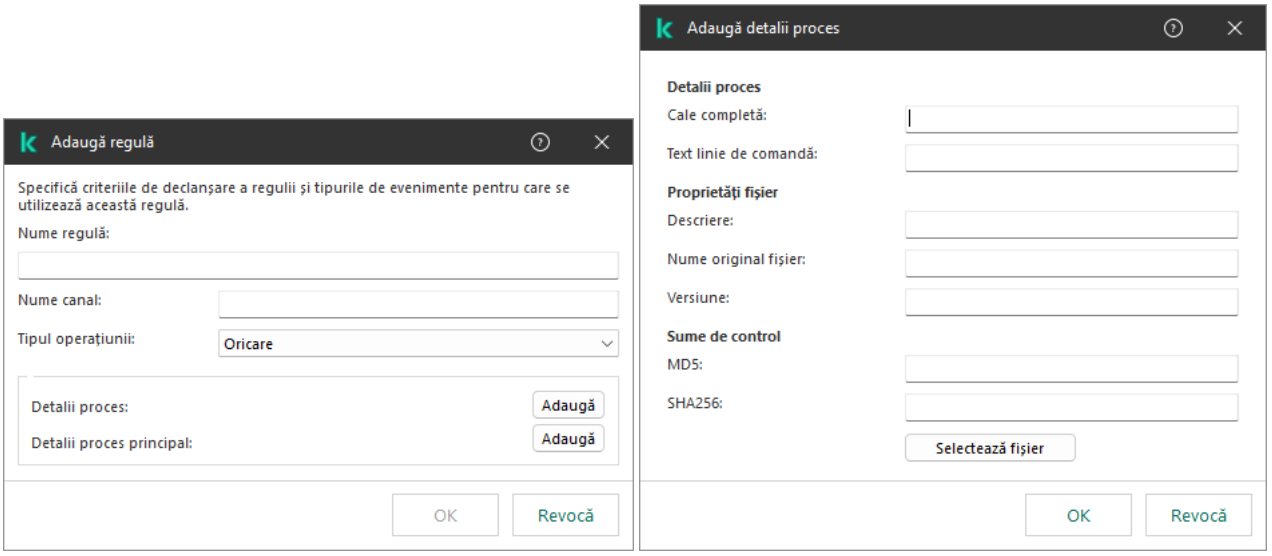
Specifică setările după cum urmează:

- **Protocol**: TCP.
- **Interval sau port la distanță**: 443.
- **Adresă la distanță**: 10.28.0.105.
- **Aplicații**: `C:\Program Files (x86)\Google\Chrome\Application\chrome.exe`; `C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe`.

Exemplul 3. Operațiunile cu fișiere excluse

Pentru a exclude din telemetrie evenimentele care implică operațiuni cu fișiere de încredere, deschide fereastra de excluderi de telemetrie EDR în fila **Operații excluse pentru fișiere** și adaugă fișierul de încredere.

Kaspersky Endpoint Security combină criteriile de declanșare a regulilor cu un AND logic.



Excluderea operațiunilor cu fișiere

Dacă o aplicație scrie într-un jurnal și dorești să excluzi evenimentele de modificare a fișierului din jurnal, adaugă fișierul jurnal și fișierul executabil al aplicației din telemetrie.

Specifică setările după cum urmează:

- **Nume fișier sau mască**: `C:\Apache24\logs\error.log`.
- **Tipul operațiunii**: Modificare fișier.
- **Cale completă**: `C:\Apache24\bin\httpd.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.

Exemplul 4. Modificările de registry excluse

Pentru a exclude evenimentele de modificare a registry-ului din telemetrie, deschide fereastra de excluderi de telemetrie EDR în fila **Modificări de registry excluse** și adaugă o cheie de registry.

Kaspersky Endpoint Security combină criteriile de declanșare a regulilor cu un AND logic.

Dacă o aplicație își modifică frecvent valorile de registry și dorești să excluzi aceste evenimente de modificare a registry-ului din telemetrie, adaugă cheia de registry și fișierul executabil al aplicației la excluderile de telemetrie.

Specifică setările după cum urmează:

- **Tipul operațiunii**: Modifică.
- **Cale**: HKEY_LOCAL_MACHINE\SOFTWARE\SimonTatham\PuTTY64.
- **Cale completă**: `C:\Program Files\PuTTY\putty.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.

KATA Sandbox

Kaspersky Anti Targeted Attack Platform include componenta Sandbox (KATA Sandbox). *Sandbox* este o tehnologie care vă permite să detectați amenințările avansate pe un computer. Sandbox analizează comportamentul obiectelor pentru a detecta activitatea rău intenționată și activitatea caracteristică atacurilor țintite asupra infrastructurii IT a organizației. Sandbox analizează și scanează obiecte de pe servere speciale cu imagini virtuale implementate ale sistemelor de operare Microsoft Windows (servere Sandbox). Pentru informații detaliate despre soluție, consultați Ajutor pentru Kaspersky Anti Targeted Attack Platform.

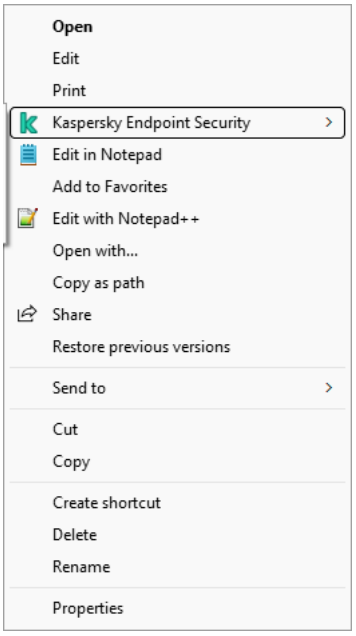
Pentru a activa KATA Sandbox, ai nevoie de o cheie de licență care include funcționalitatea KATA sau KEDR. Pentru detalii despre funcționalitățile disponibile, consultă Ajutor pentru Kaspersky Anti Targeted Attack Platform.

KATA Sandbox permite scanarea fișierelor în următoarele moduri:

- *Manual*. Utilizatorul trimite manual fișierul pentru scanare din meniul contextual (**Trimite către Sandbox**). Când trimiți un fișier către Sandbox, aplicația scanează fișierul folosind bazele de date antivirus.
- *Automat*. Aplicația detectează automat obiectele și le trimite către Sandbox pentru scanare.

După ce fișierul este trimis către Sandbox, fișierul rămâne accesibil utilizatorului. Kaspersky Endpoint Security înregistrează în jurnal evenimentul corespunzător și trimite evenimentul către Kaspersky Security Center și consola Kaspersky Anti Targeted Attack Platform. Dacă Sandbox detectează activitate rău intenționată, Kaspersky Endpoint Security efectuează o acțiune automată Răspuns la amenințare (de exemplu, șterge obiectul și inițiază o Scanare zone critice).

Pentru ca KATA Sandbox să funcționeze în modul manual, trebuie să fie implementat Kaspersky Anti Targeted Attack Platform 7.0 sau o versiune ulterioară. Pentru ca KATA Sandbox să funcționeze în modul automat, trebuie implementat Kaspersky Anti Targeted Attack Platform 8.0 sau o versiune ulterioară.



Scanarea în KATA Sandbox din meniul contextual

Integrarea agentului încorporat cu KATA Sandbox

Adăugarea componentei KATA Sandbox este necesară pentru integrarea cu Kaspersky Sandbox. Puteți selecta componenta Sandbox în timpul instalării sau efectuării upgrade-ului, precum și utilizând activitatea *Modificare componente ale aplicației*.

Pentru a trimite fișiere pentru scanare, trebuie să activezi integrarea cu KATA Sandbox și să adaugi un server Central Node care este implementat în soluție. Componenta poate fi gestionată numai utilizând Kaspersky Security Center Web Console. Nu puteți gestiona această componentă utilizând Consola de administrare (MMC).

Pentru a activa sau dezactiva integrarea cu KATA Sandbox:

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Built-in Agents Configuration** → **Sandbox**.
5. Utilizați comutatorul **Integration with Sandbox ENABLED** pentru a activa sau a dezactiva componenta.

6. Selectează modul de funcționare KATA Sandbox:

   - **Manually**. Utilizatorul trimite manual fișierul pentru scanare din meniul contextual (**Trimite către Sandbox**).
   - **Automatically**. Aplicația detectează automat obiectele și le trimite către Sandbox pentru scanare.
   - **Combined**.

7. Faceți clic pe linkul **Connection settings**.

8. Configurează setările de conectare la serverul Central Node:

   - **Timeout (msec)**. Conexiunea a expirat pentru serverul Central Node. După expirarea perioadei de expirare configurată, Kaspersky Endpoint Security trimite o solicitare către următorul server. Poți crește perioada de expirare a conexiunii pentru server dacă viteza conexiunii este mică sau dacă conexiunea este instabilă. Perioada de expirare a solicitării recomandată este de 0.5 secunde sau mai puțin.
   - **Request queue**. Dimensiunea directorului cozii de solicitare. Când trimiți mai multe obiecte pentru scanare în Sandbox, Kaspersky Endpoint Security creează o coadă de solicitări. În mod implicit, dimensiunea directorului cozii de solicitare este limitată la 100 MO. După atingerea dimensiunii maxime, Sandbox încetează să mai adauge noi solicitări la coadă și trimite evenimentul corespunzător către Kaspersky Security Center. Puteți configura dimensiunea directorului cozii de solicitare în funcție de configurația serverului.
   - **Server TLS certificate**. Pentru a configura o conexiune de încredere cu serverul Central Node, trebuie să pregătești un certificat TLS. Apoi, trebuie să adaugi certificatul pe computer, folosind o politică. De asemenea, trebuie să adaugi certificatul la serverul Central Node.
   - **Use two-way authentication**. Autentificare mutuală la stabilirea unei conexiuni securizate între Kaspersky Endpoint Security și serverul Central Node. Pentru a utiliza autentificarea mutuală, trebuie să activezi autentificarea mutuală în setările serverului Central Node, apoi să obții un container crypto și să setezi o parolă pentru a proteja containerul crypto. Un *cripto-container* este o arhivă PFX cu un certificat și o cheie privată. Puteți obține un cripto-container în consola Kaspersky Anti Targeted Attack Platform (consultați instrucțiunile din Ajutor Kaspersky Anti Targeted Attack Platform). După configurarea setărilor Central Node, trebuie să activați și autentificarea mutuală în setările Kaspersky Endpoint Security și să încărcați un container crypto protejat prin parolă.

9. În blocul **Connection to Sandbox servers**, fă clic pe butonul **Add**.

10. Se deschide o fereastră; în fereastră, introduceți adresa serverului Central Node (IPv4, IPv6, DNS) și portul.

    Pentru detalii despre implementarea imaginilor virtuale și configurarea serverelor Central Node, consultă Ajutor Kaspersky Anti Targeted Attack Platform.

11. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Ca rezultat, componenta Sandbox este activată. Verificați starea de funcționare a componentei, vizualizând *Report on status of application components*. De asemenea, puteți vizualiza starea de funcționare a unei componente în rapoarte, în interfața locală a Kaspersky Endpoint Security. Componenta **Sandbox** va fi adăugată la lista componentelor Kaspersky Endpoint Security.

Configurarea acțiunilor Răspuns la amenințare

Dacă Sandbox detectează activitate rău intenționată, Kaspersky Endpoint Security efectuează o acțiune automată Răspuns la amenințare (de exemplu, șterge obiectul și inițiază o Scanare zone critice).

Pentru a configura acțiunile Răspuns la amenințare:

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Built-in Agents Configuration** → **Sandbox**.
5. Selectați acțiunea relevantă în blocul **Action on threat detection**:

   - **Move copy to Quarantine, delete object**. Dacă această opțiune este selectată, Kaspersky Endpoint Security șterge obiectul rău intenționat găsit pe computer. Înainte de a șterge obiectul, Kaspersky Endpoint Security creează o copie de rezervă în caz că obiectul trebuie restaurat ulterior. Kaspersky Endpoint Security mută copia de rezervă în Carantină.
   - **Run Critical Areas Scan**. Dacă această opțiune este selectată, Kaspersky Endpoint Security execută activitatea *Critical Areas Scan*. În mod implicit, Kaspersky Endpoint Security scanează memoria kernel, procesele care se execută și sectoarele de boot ale discurilor.
   - **Create IOC Scan task**. Dacă această opțiune este selectată, Kaspersky Endpoint Security creează automat o activitate de *IOC Scan (activitate de scanare IOC autonomă)*. Pentru această activitate, puteți configura modul de executare, domeniul de scanare și acțiunea la detectarea IOC (*Move copy to Quarantine, delete object* sau *Run Critical Areas Scan*). Pentru a modifica alte setări ale activității *IOC Scan*, accesați setările activității.
6. Dacă este necesar, configurează setările activității *Scanare IOC* în blocul **IOC Scan scope**.

   - **Critical file areas**. Dacă această opțiune este selectată, Kaspersky Endpoint Security efectuează o scanare IOC numai în zonele cu fișiere critice ale computerului: memoria kernel și sectoarele de boot.
   - **File areas on system drive of the computer**. DACĂ este selectată această opțiune, Kaspersky Endpoint Security efectuează o scanare IOC pe unitatea de sistem a computerului.
7. Dacă este necesar, configurează setările activității *Scanare IOC* în blocul **Run IOC Scan task**.

   - **Manually**. Mod de executare în care poți porni manual activitatea *IOC Scan* la un moment care îți este convenabil.
   - **Automatically**. Modul de executare în care Kaspersky Endpoint Security execută automat activitatea *IOC Scan* după ce este detectată o amenințare.
   - **Run only when the computer is idle**. Modul de executare în care Kaspersky Endpoint Security execută activitatea *Scanare IOC* dacă economizorul de ecran este activ sau ecranul este blocat. Dacă utilizatorul deblochează computerul, Kaspersky Endpoint Security pune în pauză activitatea. Aceasta înseamnă că activitatea poate dura câteva zile până la finalizare.
8. Configurează setările avansate ale activității pentru *Scanare IOC*.
9. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Ghid de migrare KEA la KES pentru EDR (KATA)

Începând cu versiunea 12.1, Kaspersky Endpoint Security for Windows include un agent încorporat pentru gestionarea componentei Kaspersky Endpoint Detection and Response ca parte a soluției Kaspersky Anti Targeted Attack Platform. Nu mai aveți nevoie de o aplicați Kaspersky Endpoint Agent separată pentru a utiliza soluția EDR (KATA). Toate funcțiile Kaspersky Endpoint Agent vor fi efectuate de Kaspersky Endpoint Security. Sarcina pe serverele Kaspersky Anti Targeted Attack Platform va rămâne aceeași.

Când implementați Kaspersky Endpoint Security pe computere care au instalat Kaspersky Endpoint Agent, soluția Kaspersky Anti Targeted Attack Platform (EDR) vor continua să funcționeze cu Kaspersky Endpoint Security. În plus, Kaspersky Endpoint Agent va fi eliminat din computer. Același comportament în sistem va avea loc atunci când actualizați Kaspersky Endpoint Security la versiunea 12.1 sau o versiune ulterioară.

Componenta Kaspersky Endpoint Security nu este compatibilă cu Kaspersky Endpoint Agent. Nu puteți instala ambele aplicații pe același computer.

Următoarele condiții trebuie îndeplinite pentru ca Kaspersky Endpoint Security să funcționeze ca parte a soluției Endpoint Detection and Response (KATA):

- Kaspersky Anti Targeted Attack Platform versiunea 5.0 sau o versiune ulterioară.
- Kaspersky Security Center versiunea 14.2 sau o versiune ulterioară (inclusiv Agentul de rețea). În versiunile anterioare ale Kaspersky Security Center, este imposibil de activat caracteristica Endpoint Detection and Response (KATA).

Pași pentru migrarea configurației [KES+KEA] la [KES+agent încorporat] pentru EDR (KATA)

1. **Efectuarea upgrade-ului pentru plug-in-ul de gestionare Kaspersky Endpoint Security**

   Componenta EDR (KATA) poate fi gestionată utilizând Plag-in-ul de gestionare Kaspersky Endpoint Security versiunea 12.1 sau o versiune ulterioară. În funcție de tipul de consolă Kaspersky Security Center pe care îl utilizați, actualizați plug-in-ul de gestionare în Consola de administrare (MMC) sau plug-in-ul web în Web Console.

2. **Migrarea politicilor și activităților**

   Transferați setările Kaspersky Endpoint Agent la Kaspersky Endpoint Security for Windows. Sunt disponibile următoarele opțiuni:

   - un expert pentru migrarea de la Kaspersky Endpoint Agent la Kaspersky Endpoint Security. Un expert pentru migrarea de la Kaspersky Endpoint Agent la Kaspersky Endpoint Security funcționează numai în Web Console

     Cum se migrează setările politicilor și ale activităților de la Kaspersky Endpoint Agent la Kaspersky Endpoint Security în Web Console

     În fereastra principală a Web Console, selectați **Operations** → **Migration from Kaspersky Endpoint Agent**.

     Aceasta execută Expertul de migrare a politicilor și activităților. Urmează instrucțiunile din expert.

Pasul 1. Migrarea politicii

Expertul de migrare creează o nouă politică ce combină setările politicilor Kaspersky Endpoint Security și Kaspersky Endpoint Agent. În lista de politici, selectați politicile Kaspersky Endpoint Agent ale căror setări doriți să le îmbinați cu politica Kaspersky Endpoint Security. Faceți clic pe politica Kaspersky Endpoint Agent pentru a selecta Kaspersky Endpoint Security cu care doriți să îmbinați setările. Asigurați-vă că ați selectat politicile corecte și treceți la pasul următor.

Pasul 2. Migrarea activităților

Expertul de migrare nu acceptă activități EDR (KATA). Sari peste acest pas.

Pasul 3. Finalizarea expertului

Ieșiți din Expert. În urma utilizării expertului, va fi creată o nouă politică Kaspersky Endpoint Security. Politica va combina setările de la Kaspersky Endpoint Security și Kaspersky Endpoint Agent. Politica se numește *<Kaspersky Endpoint Security policy name> & <Kaspersky Endpoint Agent policy name>*. Noua politică are starea *Inactive*. Pentru a continua, modificați stările politicilor Kaspersky Endpoint Agent și Kaspersky Endpoint Security în *Inactive* și activați noua politică îmbinată.

Expertul de migrare în Web Console omite următoarele setări ale politicii și nu le migrează:

- Interzicerea modificării setărilor **Connection settings** („lacăt").

  În mod implicit, setările pot fi modificate („lacătul" este deschis). Prin urmare, setările nu sunt aplicate pe computer. Trebuie să interziceți modificarea setărilor și să închideți „lacătul".

- Crypto-container.

  Dacă utilizați autentificarea mutuală pentru conectarea la serverele Central Node, trebuie să adăugați din nou cripto-containerul.

Deoarece Expertul de migrare nu migrează aceste setări, este posibil să întâmpinați erori atunci când conectați computerul la serverele Central Node. Pentru a remedia erorile, trebuie să accesați proprietățile politicii și să configurați setările de conectare.

- Un expert standard de conversie în bloc a politicilor și activităților. Expertul de conversie în bloc a politicilor și activităților este disponibil numai în Consola de administrare (MMC). Pentru mai multe detalii despre Expertul de conversie în bloc a politicilor și activităților, consultați Ajutor pentru Kaspersky Security Center.

Pentru a vă asigura că Kaspersky Endpoint Security funcționează corect pe servere, se recomandă să adăugați fișierele importante pentru funcționarea serverului în zona de încredere. Pentru serverele SQL, trebuie să adăugați fișiere de baze de date MDF și LDF. Pentru serverele Microsoft Exchange, trebuie să adăugați fișiere CHK, EDB, JRS, LOG și JSL. Puteți utiliza măști, de exemplu, `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

Începând cu Kaspersky Endpoint Security 12.6 for Windows, excluderile de scanare și aplicații de încredere sunt adăugate la zona de încredere. Excluderile de la scanare și aplicațiile de încredere predefinite ajută la configurarea rapidă a Kaspersky Endpoint Security pe serverele SQL, serverele Microsoft Exchange și System Center Configuration Manager. Aceasta înseamnă că nu trebuie să configurați manual o zonă de încredere pentru aplicație pe servere.

Excluderile telemetriei EDR nu migrează de la politica Kaspersky Endpoint Agent la politica Kaspersky Endpoint Security. Kaspersky Endpoint Security are propriile instrumente de excludere - aplicații de încredere. Funcționarea Kaspersky Endpoint Security este optimizată, astfel încât absența excluderilor individuale de telemetrie EDR nu vor provoca încărcarea suplimentară a computerului dvs. în comparație cu Kaspersky Endpoint Agent. Kaspersky Endpoint Security folosește telemetria nu numai pentru EDR (KATA), ci și pentru funcționarea componentelor de protecție a aplicațiilor. Prin urmare, nu este nevoie să transferați excluderile de telemetrie EDR individuale. Dacă experimentați o scădere a performanței computerului, verificați funcționarea aplicației (consultați pasul 7 Verificarea erformanței).

3 Licențierea funcționalității EDR (KATA)

Pentru a activa Kaspersky Endpoint Security ca parte a soluției Kaspersky Anti Targeted Attack Platform, aveți nevoie de o licență separată pentru suplimentul Kaspersky Endpoint Detection and Response (KATA). Puteți adăuga cheia utilizând activitatea *Add key*. Ca rezultat, două chei vor fi adăugate la aplicație: *Kaspersky Endpoint Security* și *Kaspersky Endpoint Detection and Response (KATA)*.

Licențierea suplimentul Kaspersky Endpoint Detection and Response (KATA) pe computere cu funcțiile EDR Optimum sau EDR Expert activate anterior implică următoarele considerații speciale:

- Dacă utilizați un *fișier cheie* pentru licențierea Kaspersky Endpoint Security cu funcțiile EDR Optimum sau EDR Expert, nu puteți adăuga o cheie separată pentru suplimentul Kaspersky Endpoint Detection and Response (KATA). Puteți fie să comutați la utilizarea unui cod de activare pentru licențiere, fie să contactați furnizorul de servicii pentru a obține un nou fișier cheie pentru activarea funcțiilor Kaspersky Endpoint Security și EDR. Furnizorul de servicii va furniza unul sau mai multe fișiere cheie pentru licențiere.

- Dacă utilizați un *fișier cheie* pentru a licenția Kaspersky Endpoint Security fără funcțiile EDR Optimum sau EDR Expert, puteți adăuga o cheie separată pentru suplimentul Kaspersky Endpoint Detection and Response (KATA) fără a fi emise din nou fișierele cheie.

- Dacă utilizați un *cod de activare* pentru licențiere, serverul de activare Kaspersky va emite din nou automat cheile, iar funcțiile EDR (KATA) vor deveni automat disponibile. În acest caz, EDR Optimum și EDR Expert vor fi dezactivate.

- Kaspersky Endpoint Security vă permite să adăugați până la două chei active: Cheia Kaspersky Endpoint Security și cheia tip supliment. De asemenea, puteți adăuga până la două chei de rezervă. O cheie de rezervă Kaspersky Endpoint Security și o cheie de rezervă de tip supliment.

4 Instalarea/efectuarea upgrade-ului aplicației Kaspersky Endpoint Security

Pentru a migra funcționalitatea EDR (KATA) în timpul instalării sau efectuării upgrade-ului unei aplicații, se recomandă utilizarea activității de instalare la distanță. Când creați o activitate de instalare la distanță, trebuie să selectați componenta EDR (KATA) în setările pachetului de instalare.

De asemenea, puteți face upgrade aplicației utilizând următoarele metode:

- Utilizând serviciul de actualizare Kaspersky.

- Local, folosind Expertul de configurare.

Kaspersky Endpoint Security acceptă selectarea automată a componentelor atunci când se face upgrade-ul unei aplicații pe un computer pe care este instalată aplicația Kaspersky Endpoint Agent. Selectarea automată a componentelor depinde de permisiunile contului de utilizator care face upgrade-ul aplicației.

Dacă faceți upgrade pentru Kaspersky Endpoint Security utilizând fișierul EXE sau MSI din contul de sistem (SYSTEM), Kaspersky Endpoint Security obține acces la licențele curente ale soluțiilor Kaspersky. Prin urmare, dacă pe computer este instalat Kaspersky Endpoint Agent și soluția EDR (KATA) este activată, programul de instalare Kaspersky Endpoint Security configurează automat setul de componente și selectează componenta EDR (KATA). Acest lucru determină componenta Kaspersky Endpoint Security să treacă la utilizarea agentului încorporat și elimină Kaspersky Endpoint Agent. Executarea programului de instalare MSI din contul de sistem (SYSTEM) este efectuată, de obicei, atunci când se face upgrade prin intermediul serviciului de actualizare Kaspersky sau când se implementează un pachet de instalare prin Kaspersky Security Center.

Dacă faceți upgrade pentru Kaspersky Endpoint Security utilizând un fișier MSI dintr-un cont de utilizator fără privilegii, Kaspersky Endpoint Security nu obține acces la licențele curente ale soluțiilor Kaspersky. În acest caz, Kaspersky Endpoint Security selectează automat componente pe baza unui set de componente ale Kaspersky Endpoint Agent. Ulterior, componenta Kaspersky Endpoint Security comută la utilizarea agentului încorporat și elimină Kaspersky Endpoint Agent.

Kaspersky Endpoint Security acceptă efectuarea upgrade-ului fără repornirea computerului. Puteți selecta modul de efectuare a upgrade-ului aplicației în proprietățile politicii.

5 Verificarea funcționării aplicației

Dacă după instalarea sau efectuarea upgrade-ului aplicației, computerul are starea *Critical* în consola Kaspersky Security Center:

- asigurați-vă că Agentul de rețea versiunea 13.2 sau o versiune ulterioară este instalată pe computer.
- Verificați starea de funcționare a agentului încorporat, vizualizând *Report on status of application components*. Dacă o componentă are starea *Not installed*, instalați componenta, utilizând activitatea *Change application components*. Dacă o componentă are starea *Nu este acoperită de licență*, asigurați-vă că ați activat funcționalitatea agentului încorporat.
- Asigurați-vă că acceptați Declarația Kaspersky Security Network în noua politică a Kaspersky Endpoint Security for Windows.

6 Verificarea conexiunii la serverul Kaspersky Anti Targeted Attack Platform

Verificați conexiunea la serverul Kaspersky Anti Targeted Attack Platform. Pentru aceasta:

1. Verificați dacă aveți un certificat valabil.
2. Verificați setările de conectare la server.
3. Verificați jurnalul de evenimente.

   Dacă se stabilește o conexiune la server, aplicația trimite evenimentul *Successful connection to the EDR Expert server*. Dacă nu există niciun eveniment de conectare reușită și nu există evenimente cu erori de conectare, verificați setările jurnalului de evenimente și activați trimiterea evenimentelor pentru Endpoint Detection and Response (KATA).

Starea conexiunii la server nu afectează starea computerului în consola Kaspersky Security Center. Prin urmare, dacă nu există nicio conexiune la server, computerul poate avea în continuare starea *OK*. Verificați jurnalul de evenimente pentru a verifica conexiunea la server.

7 Verificarea performanței

Dacă performanța computerului dvs. a încetinit după instalarea sau actualizarea unei aplicații, puteți optimiza transferul de date. Pentru aceasta:

1. Dezactivați componenta EDR (KATA) și verificați dacă degradarea performanței se datorează componentei EDR (KATA).
2. Pentru aplicațiile de încredere, dezactivați colectarea de telemetrie la operațiunile de intrare în consolă (activată în mod implicit).
3. Adăugați aplicații care reduc performanța computerului în lista de aplicații de încredere.
4. Contactați Suportul tehnic Kaspersky. Experții departamentului Suport vă vor ajuta să configurați filtrarea telemetriei în Kaspersky Anti Targeted Attack Platform. Acest lucru va reduce volumul traficului. Dacă performanța computerului dvs. este afectată de o anumită aplicație, atașați la cerere pachetul de distribuție al acelei aplicații.

Endpoint Detection and Response Expert (on-premises)

Kaspersky Endpoint Security for Windows acceptă integrarea cu soluția Kaspersky Endpoint Detection and Response Expert (on-premises). *Kaspersky Endpoint Detection and Response Expert (on-premises)* este o soluție de securitate cibernetică pentru companii care include aplicații Kaspersky ce permit unei organizații să se apere împotriva majorității tipurilor de riscuri cibernetice și să acopere cele mai importante scenarii de propagare a amenințărilor. Componentele EDR Expert (on-premises) sunt implementate pe Open Single Management Platform (OSMP). Această platformă execută scenarii multiplatformă într-o singură interfață și permite integrarea aplicațiilor Kaspersky cu aplicații terțe într-un sistem de securitate complet.

Unul dintre elementele centrale ale soluției este *SIEM*. SIEM urmărește evenimentele provenite de la toate componentele și corelează aceste evenimente între ele, folosind reguli definite de producător și de utilizator. EDR Expert (on-premises) analizează jurnalele și datele de telemetrie primite de la infrastructura corporativă pentru a detecta automat atacurile și permite investigarea incidentelor utilizând un grafic de investigare unificat, care combină toate evenimentele colectate în EDR Expert (on-premises), inclusiv evenimentele din aplicațiile Kaspersky și produsele de securitate a informațiilor de la terți.

Pentru a răspunde la incidente avansate, EDR Expert (on-premises) utilizează scenarii prestabilite și definite de utilizator. De asemenea, poți utiliza acțiuni de răspuns de la aplicații terțe și scenarii de răspuns care implică mai multe aplicații.

Instrumente Threat Intelligence

Kaspersky Endpoint Detection and Response utilizează următoarele instrumente Threat Intelligence:

- Integrarea cu Portalul Kaspersky Threat Intelligence, care conține și afișează informații despre reputația fișierelor și a adreselor web.
- Baza de date Kaspersky Threats.
- Infrastructura serviciului clould al Kaspersky Security Network (denumit în continuare „KSN”), care oferă acces la informații în timp real despre reputația fișierelor, site-urilor web și a software-urilor din baza de cunoștințe Kaspersky. Utilizarea datelor de la Kaspersky Security Network asigură răspunsul mai rapid al aplicațiilor Kaspersky la amenințări, îmbunătățește performanța unor componente de protecție și reduce posibilitatea alarmelor false.

Principiul de funcționare al soluției

Kaspersky Endpoint Security este instalat pe computere individuale din infrastructura IT corporativă și monitorizează continuu procesele, conexiunile la rețea deschise și fișierele care sunt modificate.

Când este instalat în modul standard în infrastructura VDI, Kaspersky Endpoint Security acceptă integrarea cu EDR Expert (on-premises). Totuși, operabilitatea celorlalte funcționalități ale aplicației nu este garantată. Pentru a proteja mașinile virtuale din infrastructura VDI, îți recomandăm să utilizezi Kaspersky Endpoint Security în modul Light Agent.

Informațiile despre evenimentele de pe computer (telemetrie) sunt trimise către serverul EDR Expert (on-premises). În acest caz, Kaspersky Endpoint Security trimite și informații despre amenințările descoperite de aplicație, precum și informații despre rezultatele procesării acestor amenințări către serverele de colectare a datelor de telemetrie.

Integrarea EDR Expert (on-premises) este configurată pe consola Kaspersky Security Center. Agentul integrat este apoi gestionat utilizând Open Single Management Platform (OSMP), inclusiv executarea activităților, gestionarea obiectelor carantinate, vizualizarea rapoartelor și alte acțiuni.

Configurațiile Kaspersky Endpoint Security pentru lucrul cu EDR Expert (on-premises)

Următoarele configurații pot fi utilizate pentru a lucra cu EDR Expert (on-premises):

- **[KES+agent încorporat]**. În această configurație, Kaspersky Endpoint Security acționează atât ca aplicație care asigură securitatea computerului, cât și ca aplicație pentru lucrul cu EDR Expert (on-premises). Agentul încorporat pentru EDR Expert (on-premises) este disponibil în Kaspersky Endpoint Security 12.11 for Windows sau versiunile ulterioare.
- **[EPP terță+agent EPP+EDR]**. În această configurație, securitatea infrastructurii IT este asigurată de platforma de componenta terță Endpoint Protection Platform (EPP). Interacțiunea cu EDR Expert (on-premises) este asigurată de Kaspersky Endpoint Security în configurația Endpoint Detection and Response Agent (EDR Agent). În această configurație, EDR Agent este compatibil cu aplicațiile EPP terțe. EDR Agent pentru EDR Expert (on-premises) este disponibil în Kaspersky Endpoint Security 12.11 for Windows sau versiunile ulterioare.

Integrarea agentului încorporat cu EDR Expert (on-premises)

Pentru integrarea cu soluția Kaspersky Endpoint Detection and Response Expert (on-premises), trebuie să adaugi componenta Endpoint Detection and Response Expert (on-premises) și să configurezi Kaspersky Endpoint Security.

Componentele Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud) și Endpoint Detection and Response Expert (on-premises) nu sunt compatibile între ele.

Trebuie îndeplinite următoarele condiții pentru ca Endpoint Detection and Response Expert (on-premises) să funcționeze:

- OSMP (Open Single Management Platform) este instalat.
- Aplicația este activată și funcționalitatea este acoperită de licență.
- Componenta Endpoint Detection and Response Expert (on-premises) este activată.
- Componentele aplicației care asigură funcționarea componentei EDR Expert (on-premises) sunt activate și operaționale: Următoarele componente asigură funcționarea EDR Expert (on-premises):
  - File Threat Protection.
  - Web Threat Protection.
  - Mail Threat Protection.
  - Exploit Prevention.
  - Behavior Detection.
  - Host Intrusion Prevention.
  - Remediation Engine.
  - Control adaptiv al anomaliilor.

Configurarea integrării EDR Expert (on-premises) implică următorii pași:

1. **Instalarea componentei EDR Expert (on-premises)**

   Puteți selecta componenta EDR Expert (on-premises) în timpul instalării sau efectuării upgrade-ului, precum și utilizând activitatea *Modificare componente ale aplicației*.

   > Trebuie să reporniți computerul pentru a finaliza efectuarea upgrade-ului aplicației cu noua componentă.

2. **Activarea Kaspersky Endpoint Detection and Response Expert (on-premises)**

   Trebuie să achiziționezi o licență separată pentru EDR Expert (on-premises) (suplimentul Kaspersky Endpoint Detection and Response Expert (on-premises)).

   Funcționalitatea devine disponibilă după adăugarea unei chei separate pentru Kaspersky Endpoint Detection and Response Expert (on-premises). Ca rezultat, sunt adăugate două chei pe computer: o cheie pentru Kaspersky Endpoint Security și o cheie pentru Kaspersky Endpoint Detection and Response Expert (on-premises).

   Licențierea funcționalității individuale Endpoint Detection and Response Expert (on-premises) se realizează la fel ca licențierea componentei Kaspersky Endpoint Security.

   Asigură-te că funcționalitatea componentei EDR Expert (on-premises) este inclusă în licență și că aceasta se execută în interfața locală a aplicației.

3. **Conectarea la serverul de colectare a telemetriei și la serverul de răspuns**

Kaspersky Endpoint Detection and Response Expert (on-premises) necesită o conexiune de încredere între Kaspersky Endpoint Security și două servere:

- Un *server de colectare a telemetriei* este un server care face parte dintr-o soluție SIEM și care colectează, normalizează, corelează, analizează și stochează informații despre evenimentele care au loc pe computer.
- Un *server de răspuns* este un server pentru primirea și scanarea datelor, studierea comportamentului obiectelor și publicarea rezultatelor acestor studii.

Pentru a configura o conexiune de încredere, trebuie să utilizați un certificat TLS. Poți obține un certificat TLS pe Open Single Management Platform (consultă instrucțiunile din Ajutor pentru Kaspersky Endpoint Detection and Response Expert (on-premises)). Apoi, trebuie să adăugați certificatul TLS la Kaspersky Endpoint Security (consultați instrucțiunile de mai jos).

În mod implicit, Kaspersky Endpoint Security verifică doar certificatul TLS al serverelor. Pentru a face conexiunea mai sigură, poți activa suplimentar verificarea computerului pe server (autentificare mutuală). Pentru a activa această verificare, trebuie să activezi autentificarea mutuală în setările serverului și ale Kaspersky Endpoint Security. Pentru a utiliza autentificarea mutuală, veți avea nevoie și de un cripto-container. Un *cripto-container* este o arhivă PFX cu un certificat și o cheie privată. Poți obține un container crypto pe Open Single Management Platform (consultă instrucțiunile din Ajutor pentru Kaspersky Endpoint Detection and Response Expert (on-premises)).

Cum conectezi un computer Kaspersky Endpoint Security la EDR Expert (on-premises) utilizând Web Console

1. În fereastra principală a Web Console, selectați fila **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (on-premises)**.
5. Duceți comutatorul **Endpoint Detection and Response Expert (on-premises) ENABLED** la poziția activat.
6. Pentru a configura EDR Expert (on-premises), selectează **Endpoint Detection and Response Expert (version 8.0 or later)** din lista de soluții.
7. Configurează conexiunea la *serverele de colectare a telemetriei*:

   a. În blocul **Connection to telemetry collection servers**, faceți clic pe linkul **Connection settings**.

   b. Configurează conexiunea la serverele de colectare a telemetriei:

   - **Timeout (sec)**. Expirarea timpului maxim de răspuns al serverului. Când timpul de expirare se termină, Kaspersky Endpoint Security încearcă să se conecteze la un alt server.
   - **Server certificate**. Certificat TLS pentru stabilirea unei conexiuni de încredere cu serverul. Poți obține un certificat TLS pe Open Single Management Platform (consultă instrucțiunile din Ajutor pentru Kaspersky Endpoint Detection and Response Expert (on-premises)).

- **Use two-way authentication**. Autentificare mutuală la stabilirea unei conexiuni securizate între Kaspersky Endpoint Security și server. Pentru a utiliza autentificarea mutuală, trebuie să activezi autentificarea mutuală în setările serverului, apoi să obții un container crypto și să setezi o parolă pentru a proteja containerul crypto. Un *cripto-container* este o arhivă PFX cu un certificat și o cheie privată. Poți obține un container crypto pe Open Single Management Platform (consultă instrucțiunile din Ajutor pentru Kaspersky Endpoint Detection and Response Expert (on-premises)). După configurarea setărilor serverului, trebuie să activezi autentificarea mutuală și în setările Kaspersky Endpoint Security și să încarci un container crypto protejat prin parolă.

  > Criptocontainerul trebuie să fie protejat prin parolă. Nu este posibil să adăugați un criptocontainer cu o parolă necompletată.

c. Fă clic pe **OK**.

d. Adaugă servere de colectare a telemetriei. Pentru a face acest lucru, specificați adresa serverului (IPv4, IPv6) și portul de conectare la server.

Poți adăuga mai multe adrese de server de colectare a datelor de telemetrie. Kaspersky Endpoint Security încearcă să se conecteze la server la prima adresă IP. Dacă nu se poate stabili o conexiune, Kaspersky Endpoint Security încearcă să se conecteze la a doua adresă IP din listă și așa mai departe.

e. Dacă este necesar, configurează telemetria.

8. Configurează conexiunea la *serverele de răspuns*:

a. În blocul **Connection to response servers**, configurează setările pentru **Send sync request to server every (min)**. Frecvența solicitărilor de sincronizare trimise către serverul. În timpul sincronizării, Kaspersky Endpoint Security primește sarcini de răspuns la amenințări și trimite rezultatele sarcinilor.

b. Faceți clic pe linkul **Connection settings**.

c. Configurează conexiunea la serverele de răspuns:

- **Timeout (sec)**. Expirarea timpului maxim de răspuns al serverului. Când timpul de expirare se termină, Kaspersky Endpoint Security încearcă să se conecteze la un alt server.

- **Server certificate**. Certificat TLS pentru stabilirea unei conexiuni de încredere cu serverul. Poți obține un certificat TLS pe Open Single Management Platform (consultă instrucțiunile din Ajutor pentru Kaspersky Endpoint Detection and Response Expert (on-premises)).

- **Use two-way authentication**. Autentificare mutuală la stabilirea unei conexiuni securizate între Kaspersky Endpoint Security și server. Pentru a utiliza autentificarea mutuală, trebuie să activezi autentificarea mutuală în setările serverului, apoi să obții un container crypto și să setezi o parolă pentru a proteja containerul crypto. Un *cripto-container* este o arhivă PFX cu un certificat și o cheie privată. Poți obține un container crypto pe Open Single Management Platform (consultă instrucțiunile din Ajutor pentru Kaspersky Endpoint Detection and Response Expert (on-premises)). După configurarea setărilor serverului, trebuie să activezi autentificarea mutuală și în setările Kaspersky Endpoint Security și să încarci un container crypto protejat prin parolă.

  > Criptocontainerul trebuie să fie protejat prin parolă. Nu este posibil să adăugați un criptocontainer cu o parolă necompletată.

d. Fă clic pe **OK**.

e. Adaugă servere de răspuns. Pentru a face acest lucru, specificați adresa serverului (IPv4, IPv6) și portul de conectare la server.

Poți adăuga mai multe adrese de servere de răspuns. Kaspersky Endpoint Security încearcă să se conecteze la server la prima adresă IP. Dacă nu se poate stabili o conexiune, Kaspersky Endpoint Security încearcă să se conecteze la a doua adresă IP din listă și așa mai departe.

9. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Prin urmare, computerul este adăugat la lista dispozitivelor gestionate din cadrul Open Single Management Platform (OSMP). Verificați starea de funcționare a componentei, vizualizând *Report on status of application components*. De asemenea, puteți vizualiza starea de funcționare a unei componente în rapoarte, în interfața locală a Kaspersky Endpoint Security. Componenta **Endpoint Detection and Response Expert (on-premises)** va fi adăugată la lista componentelor Kaspersky Endpoint Security.

Configurarea setărilor de telemetrie EDR Expert (on-premises)

Telemetrie este o listă de evenimente care au avut loc pe computerul protejat. Kaspersky Endpoint Security analizează datele de telemetrie și le trimite către serverele de colectare a telemetriei în timpul sincronizării. Evenimentele de telemetrie ajung pe server aproape continuu. Kaspersky Endpoint Security inițiază sincronizarea cu serverul atunci când este îndeplinită oricare dintre următoarele condiții:

- intervalul de sincronizare a expirat;
- numărul de evenimente din memoria tampon depășește limita superioară.

Prin urmare, în mod implicit, aplicația se sincronizează la fiecare 30 de secunde sau ori de câte ori memoria tampon conține 1024 de evenimente. Puteți configura comportamentul de sincronizare în politica Kaspersky Endpoint Security și puteți selecta valorile optime care să corespundă încărcării rețelei dvs. (consultați instrucțiunile de mai jos).

Dacă nu există nicio conexiune între Kaspersky Endpoint Security și server, aplicația pune în coadă evenimentele noi. Când conexiunea este restabilită, Kaspersky Endpoint Security trimite evenimentele din coadă către server în ordinea corespunzătoare. Pentru a evita supraîncărcarea serverului, Kaspersky Endpoint Security poate sări peste unele evenimente. Pentru a activa acest lucru, puteți optimiza setările de transmitere a evenimentelor, de exemplu, puteți seta o valoare maximă pentru numărul evenimentelor pe oră (consultați instrucțiunile de mai jos).

Pentru a configura setările de telemetrie, urmează pașii de mai jos:

1. În fereastra principală a Web Console, selectați fila **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (on-premises)**.
5. Pentru a configura EDR Expert (on-premises), selectează **Endpoint Detection and Response Expert (version 8.0 or later)** din lista de soluții.
6. Asigură-te că ai bifat caseta de selectare **Send telemetry to telemetry collection servers** din blocul **Data transmission settings**.

7. Dacă este necesar, bifați caseta de selectare **Send telemetry with IOA only**. *Indicatorul de atac (IOA)* este o regulă care conține o descriere a comportamentului suspect din sistem, care poate indica un atac țintit. Aplicația compară comportamentul curent din sistem cu aceste reguli și înregistrează în jurnal evenimentele care indică un atac țintit. Aplicația utilizează tehnologia *scanare în flux* care permite urmărirea în timp real a acestor evenimente.

8. Dacă este necesar, configurează sincronizarea cu setările serverului în blocul **Data transmission settings**:

   - **Maximum event transmission delay (sec)**. Aplicația se sincronizează cu serverul pentru a trimite evenimente după expirarea intervalului de sincronizare. Valoarea implicită este 30 de secunde.

   - **Maximum number of event packages**. Aplicația se sincronizează cu serverul atunci când memoria tampon este umplută cu evenimente. Valoarea implicită este de 1024 de evenimente.

9. Dacă este necesar, debifează caseta de selectare **Enable request throttling** din blocul **Request throttling**.

   Această caracteristică ajută la optimizarea încărcării serverului. Dacă această funcționalitate este activată, aplicația restricționează transmiterea evenimentului. Dacă numărul de evenimente depășește limitele configurate, Kaspersky Endpoint Security oprește trimiterea evenimentelor. Această opțiune este activată în mod implicit.

10. Configurați setările de optimizare pentru trimiterea evenimentelor către server:

    - **Maximum number of events per hour**. Aplicația analizează fluxul de date de telemetrie și restricționează trimiterea evenimentelor dacă fluxul de evenimente depășește limita de evenimente pe oră configurată. Kaspersky Endpoint Security reia trimiterea evenimentelor după o oră. Valoarea implicită este de 3000 de evenimente pe oră. Dacă aplicația este instalată pe un server, fluxul de date de telemetrie este mai mare. Pentru servere, se recomandă creșterea valorii la 60.000 de evenimente pe oră.

    - **Percentage of event limit excess**. Aplicația sortează evenimentele după tip (de exemplu, evenimente „modificări în registry") și restricționează transmiterea evenimentelor dacă raportul dintre evenimente de același tip și numărul total de evenimente depășește limita configurată în procente. Kaspersky Endpoint Security reia trimiterea evenimentelor atunci când raportul dintre alte evenimente și numărul total de evenimente devine din nou suficient de mare. Valoarea implicită este 15%.

11. În blocul **Connection to response servers**, introdu o valoare pentru parametrul **Send sync request to server every (min)**.

12. Frecvența solicitărilor de sincronizare trimise către serverul. În timpul sincronizării, Kaspersky Endpoint Security trimite informații despre setările și activitățile modificate ale aplicației.

13. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Excluderi telemetrie EDR Expert (on-premises)

Pentru a îmbunătăți performanța și a optimiza transmiterea datelor către serverul de telemetrie, poți adăuga excluderi de telemetrie. De exemplu, poți alege să nu trimiți date de comunicare în rețea pentru aplicații individuale.

Utilizarea unui număr prea mare de reguli poate crește încărcarea pe serverul de colectare a telemetriei și poate reduce performanța computerului. Îți recomandăm să adaugi doar regulile necesare.

Pentru a crea o excludere de telemetrie în Web Console și în Cloud Console:

1. În fereastra principală a Web Console, selectați fila **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.
   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **General Settings** → **Telemetry Settings**.
5. Selectați fila **EDR Expert (on-premises) telemetry**.
6. În blocul **General exclusions**, fă clic pe butonul **Add**.
   Se deschide fereastra **Add exclusion rule**.
7. Dacă este necesar, modifică starea regulii. În mod implicit, regula este activată.
8. Introdu un nume pentru regulă.
9. Selectează o acțiune care va fi efectuată atunci când este declanșată regula:
   - **Do not collect**. Evenimentul filtrat va fi exclus din datele de telemetrie trimise.
   - **Exclude IOA**. Evenimentul de declanșare a regulii IOA va fi exclus din datele de telemetrie trimise.
10. Dacă opțiunea **Exclude IOA** este selectată, specifică regulile IOA care vor fi adăugate la excluderi:
    - **Exclude all**. Când condiția specificată este îndeplinită, aplicația va exclude din telemetrie evenimentele generate pe baza tuturor regulilor IOA.
    - **Exclude by GUID**. Specifică GUID-ul regulii IOA. Poți specifica mai multe GUID-uri utilizând `,`. Pentru mai multe detalii privind regulile IOA, consultă Ajutor pentru EDR Expert (on-premises).
11. Specifică condiția de filtrare:
    a. Selectează numele câmpului care va fi utilizat pentru filtrare.
    b. Selectează un operator (consultă tabelul de mai jos) și specifică valoarea cu care va fi comparată valoarea câmpului din eveniment.

Lista operatorilor condiționali

Operator	Descriere
<	Dacă valoarea câmpului este mai mică decât valoarea specificată în condiție, evenimentul va fi filtrat.
≤	Dacă valoarea câmpului este mai mică sau egală cu valoarea specificată în condiție, evenimentul va fi filtrat.
=	Dacă valoarea câmpului este egală cu valoarea specificată în condiție, evenimentul va fi filtrat.
≥	Dacă valoarea câmpului este mai mare sau egală cu valoarea specificată în condiție, evenimentul va fi filtrat.
>	Dacă valoarea câmpului este mai mare decât valoarea specificată în condiție, evenimentul va fi filtrat.
≠	Dacă valoarea câmpului nu este egală cu valoarea specificată în condiție, evenimentul va fi filtrat.
is like	Dacă valoarea câmpului corespunde cu masca specificată în condiție, evenimentul va fi filtrat. Aplicația acceptă caracterele `*` și `?` la introducerea unei măști:

Operator	Descriere
is not like	Dacă valoarea câmpului nu corespunde măștii specificate în condiție, evenimentul va fi filtrat. Aplicația acceptă caracterele `*` și `?` la introducerea unei măști:
one of	Dacă valoarea câmpului corespunde uneia dintre valorile din lista specificată în condiție, evenimentul este considerat filtrat.
none of	Dacă valoarea câmpului nu corespunde niciuneia dintre valorile din lista specificată în condiție, evenimentul este considerat filtrat.
is like one of	Dacă valoarea câmpului corespunde uneia dintre măștile specificate în condiție, evenimentul va fi filtrat. Aplicația acceptă caracterele * și ? la introducerea unei măști.
is not like one of	Dacă valoarea câmpului nu corespunde niciuneia dintre măștile specificate în condiție, evenimentul va fi filtrat. Aplicația acceptă caracterele * și ? la introducerea unei măști.
exists	În cazul în care câmpul specificat în condiție este prezent în eveniment, evenimentul va fi filtrat.
not exists	În cazul în care câmpul specificat în condiție nu este prezent în eveniment, evenimentul va fi filtrat.
contains	Dacă valoarea specificată în condiție este prezentă în valoarea câmpului, evenimentul va fi filtrat.
is equal to	Dacă valoarea câmpului este egală cu valoarea specificată în condiție, evenimentul va fi filtrat. Scanarea ține cont de majuscule/minuscule.
bitwise AND	Dacă rezultatul operației Bitwise AND (&) între valoarea câmpului și valoarea specificată în condiție este 1, evenimentul va fi filtrat.

12. Dacă este necesar, poți crea criterii de filtrare complexe adăugând mai multe condiții de filtrare și grupuri de condiții. De asemenea, poți adăuga condiții imbricate și grupuri de condiții la un grup de condiții. Poți folosi următorii operatori:

    - **AND** înseamnă că filtrul selectează evenimente care îndeplinesc toate condițiile specificate.
    - **OR** înseamnă că filtrul selectează evenimente care îndeplinesc una dintre condițiile specificate.
    - **NOT** (pentru a utiliza acest operator, selectează opțiunea **Add NOT before**) înseamnă că filtrul selectează evenimente care nu îndeplinesc niciuna dintre condițiile specificate.

    Condițiile și grupurile de condiții de primul nivel sunt combinate cu operatorul **AND**.

13. Dacă pe computer se execută Open Single Management Platform (OSMP), poți scana regula de filtrare pe care ai creat-o. Pentru a executa scanarea, fă clic pe butonul **Check rule**.

    În fereastra care se deschide, va fi afișat un tabel cu evenimentele filtrate după regula creată. Pentru detalii, consultă Ajutor pentru EDR Expert (on-premises).

14. Dacă este necesar, în **All event types**, adaugă excluderi de telemetrie după tipul de eveniment.

    a. Fă clic pe numele tipului de eveniment.

    b. În fereastra care se deschide, faceți clic pe butonul **Set up manually**.

    c. Dacă este necesar, configurează transmiterea telemetriei pentru tipul de eveniment selectat, utilizând comutatorul **Send event**. În mod implicit, transmiterea telemetriei este activată pentru toate tipurile de evenimente.

    d. În blocul **Exclusion rules**, fă clic pe butonul **Add**.

    Se deschide fereastra **Add exclusion rule**.

    e. Efectuează acțiunile descrise în pașii 7–13 pentru fiecare regulă pe care o adaugi.

15. Pentru anumite tipuri de evenimente, poți adăuga și reguli de includere pentru a extinde telemetria colectată:

    a. În blocul **Inclusion rules**, fă clic pe butonul **Add**.

    Se deschide fereastra **Add inclusion rules**.

    b. Introdu un nume pentru regulă.

    c. În **Condition**, introdu valori pentru câmpurile afișate. Tipul de câmpuri disponibile depinde de evenimentul selectat.

    Regulile de excludere au prioritate față de regulile de includere.

16. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Exportarea și importarea filtrelor de evenimente EDR Expert (on-premises)

Poți exporta lista de excluderi într-un fișier JSON. Apoi, poți modifica fișierul pentru a adăuga, de exemplu, un număr mare de înregistrări de ID-uri de evenimente. De asemenea, poți utiliza funcția de export/import pentru a face o copie de rezervă a filtrelor pentru evenimente sau pentru a migra lista pe un alt server.

Utilizarea unui număr prea mare de reguli poate crește încărcarea pe serverul de colectare a telemetriei și poate reduce performanța computerului. Îți recomandăm să adaugi doar regulile necesare.

Cum se exportă și se importă filtrele pentru evenimente în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați **Policies**.
3. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
4. În fereastra politicii, selectați **Setări generale** → **Excluderi și tipuri de obiecte**.
5. În blocul **Setări telemetrie** → **Telemetrie EDR Expert (on-premises)**, fă clic pe butonul **Setări**.
6. Pentru a exporta filtrele pentru evenimente:

    a. Fă clic pe **Exportă**.

    În fereastra care se deschide, specifică numele fișierului JSON în care dorești să exporți filtrele pentru evenimente și selectează directorul în care dorești să salvezi acest fișier.

    b. Salvați fișierul.

    Kaspersky Endpoint Security exportă filtrele pentru evenimente în fișierul JSON.

7. Pentru a importa filtrele pentru evenimente:

   a. Fă clic pe **Importă**.

   b. În fereastra care se deschide, selectează fișierul JSON din care dorești să importi filtrele pentru evenimente.

   c. Deschideți fișierul.

      Dacă există deja reguli de filtrare a evenimentelor pe computer, Kaspersky Endpoint Security le înlocuiește în momentul importului.

8. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se exportă și se importă filtre pentru evenimente în Web Console

1. În fereastra principală a Web Console, selectați fila **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **General Settings** → **Telemetry Settings**.

5. Selectați fila **EDR Expert (on-premises) telemetry**.

6. Pentru a exporta filtrele pentru evenimente:

   a. Fă clic pe **Export**.

   b. În fereastra care se deschide, specifică numele fișierului JSON în care dorești să exporți filtrele pentru evenimente și selectează directorul în care dorești să salvezi acest fișier.

   c. Salvați fișierul.

      Kaspersky Endpoint Security exportă filtrele pentru evenimente în fișierul JSON.

7. Pentru a importa filtrele pentru evenimente:

   a. Fă clic pe **Import**.

   b. În fereastra care se deschide, selectează fișierul JSON din care dorești să importi filtrele pentru evenimente.

   c. Selectează modul în care dorești să fie importate regulile de filtrare a evenimentelor: prin adăugarea la regulile existente sau prin eliminarea regulilor existente și înlocuirea acestora cu altele noi.

   d. Deschideți fișierul.

8. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

De asemenea, poți exporta sau importa filtrele pentru evenimente în linia de comandă.

Aspecte speciale la utilizarea profilurilor de politici pentru a configura integrarea cu EDR Expert (on-premises) și EDR (KATA)

Pentru a configura integrarea cu EDR (KATA) pentru anumite grupuri administrative și cu Expert EDR (on-premises) pentru altele, ca parte a unei singure politici, va trebui să utilizezi profiluri de politică. Trebuie să configurezi setările de integrare EDR (KATA) în proprietățile politicii, iar integrarea EDR Expert (on-premises) pentru grupurile de administrare selectate trebuie configurată în proprietățile profilului politicii.

Utilizarea profilurilor de politici pentru configurarea integrării cu EDR Expert (on-premises) are următoarele limitări:

- Dacă configurezi integrarea cu EDR Expert (on-premises) în proprietățile politicii, aceste setări se vor aplica tuturor grupurilor de administrare; setările de integrare din profilurile de politici nu vor fi aplicate.
- Când utilizezi profiluri de politici pentru a configura integrarea cu EDR Expert (on-premises), nu poți utiliza Consola de administrare (MMC) pentru a gestiona politicile. Când deschizi proprietățile politicii în Consola de administrare, setările integrării EDR Expert (on-premises) din profilurile politicilor vor fi suprascrise de setările din politică, ceea ce va duce la funcționarea incorectă a componentei. Va trebui să resetezi setările componentei Endpoint Detection and Response Expert (on-premises) conform instrucțiunilor de mai jos.
- Când utilizezi profiluri de politici pentru a configura integrarea cu EDR Expert (on-premises), nu poți utiliza politici secundare.

Dacă ai deja o politică configurată într-o versiune anterioară a plug-inului web, trebuie să resetezi setările pentru componenta Endpoint Detection and Response Expert (on-premises) pentru a aplica setările de integrare EDR Expert (on-premises) dispozitivelor gestionate din profilurile politicilor.

Pentru a reseta setările componentei:

1. În fereastra principală a Web Console, selectați fila **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (on-premises)**.
5. Schimbă modul de funcționare de la **Endpoint Detection and Response Expert (version 7.1 or earlier)** la **Modul Endpoint Detection and Response Expert (versiunea 8.0 sau o versiune anterioară)**.
6. Revino la **Endpoint Detection and Response Expert (version 7.1 or earlier)**.
7. Salvați-vă modificările.

Endpoint Detection and Response Expert (cloud)

Integrarea Kaspersky Endpoint Security for Windows cu Kaspersky Endpoint Detection and Response Expert (cloud) este temporar indisponibilă. Această funcționalitate este planificată să fie acceptată până la sfârșitul anului 2026. Urmărește notele noastre de lansare pentru a fi la curent cu actualizările și noile caracteristici ale aplicației.

Kaspersky Endpoint Security for Windows acceptă integrarea cu soluția Kaspersky Endpoint Detection and Response Expert (cloud). *Kaspersky Endpoint Detection and Response Expert (cloud)* este o soluție de securitate cibernetică pentru companii bazată în cloud care include aplicații Kaspersky ce permit unei organizații să se apere împotriva majorității tipurilor de riscuri cibernetice și să acopere cele mai importante scenarii de propagare a amenințărilor. Componentele EDR Expert (cloud) sunt implementate pe Open Single Management Platform (OSMP). Această platformă execută scenarii multiplatformă într-o singură interfață și permite integrarea aplicațiilor Kaspersky cu aplicații terțe într-un sistem de securitate complet.

Integrarea cu Kaspersky Endpoint Detection and Response Expert (cloud) nu este acceptată pe computerele bazate pe arhitectura ARM.

Unul dintre elementele centrale ale soluției este *SIEM*. SIEM urmărește evenimentele provenite de la toate componentele și corelează aceste evenimente între ele, folosind reguli definite de producător și de utilizator. EDR Expert (cloud) analizează jurnalele și datele de telemetrie primite de la infrastructura corporativă pentru a detecta automat atacurile și permite investigarea incidentelor utilizând un grafic de investigare unificat, care combină toate evenimentele colectate în EDR Expert (cloud), inclusiv evenimentele din aplicațiile Kaspersky și produsele de securitate a informațiilor de la terți.

Pentru a răspunde la incidente avansate, EDR Expert (cloud) utilizează scenarii prestabilite și definite de utilizator. De asemenea, poți utiliza acțiuni de răspuns de la aplicații terțe și scenarii de răspuns care implică mai multe aplicații.

Instrumente Threat Intelligence

Kaspersky Endpoint Detection and Response utilizează următoarele instrumente Threat Intelligence:

- Integrarea cu Portalul Kaspersky Threat Intelligence, care conține și afișează informații despre reputația fișierelor și a adreselor web.
- Baza de date Kaspersky Threats.
- Infrastructura serviciului clould al Kaspersky Security Network (denumit în continuare „KSN"), care oferă acces la informații în timp real despre reputația fișierelor, site-urilor web și a software-urilor din baza de cunoștințe Kaspersky. Utilizarea datelor de la Kaspersky Security Network asigură răspunsul mai rapid al aplicațiilor Kaspersky la amenințări, îmbunătățește performanța unor componente de protecție și reduce posibilitatea alarmelor false.

Principiul de funcționare al soluției

Kaspersky Endpoint Security este instalat pe computere individuale din infrastructura IT corporativă și monitorizează continuu procesele, conexiunile la rețea deschise și fișierele care sunt modificate.

Informațiile despre evenimentele de pe computer (telemetrie) sunt trimise către serverul EDR Expert (cloud). În acest caz, Kaspersky Endpoint Security trimite și informații despre amenințările descoperite de aplicație, precum și informații despre rezultatele procesării acestor amenințări către serverele de colectare a datelor de telemetrie.

Integrarea EDR Expert (cloud) este configurată pe consola Kaspersky Security Center. Agentul integrat este apoi gestionat utilizând Open Single Management Platform (OSMP), inclusiv executarea activităților, gestionarea obiectelor carantinate, vizualizarea rapoartelor și alte acțiuni.

Integrarea agentului încorporat cu EDR Expert (cloud)

Pentru a configura integrarea cu soluția Kaspersky Endpoint Detection and Response (cloud), trebuie să instalezi componenta Endpoint Detection and Response Expert (cloud) și să configurezi Kaspersky Endpoint Security.

Componentele Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud) și Endpoint Detection and Response Expert (on-premises) nu sunt compatibile între ele.

Condiții de funcționare EDR Expert (cloud)

Pentru ca EDR Expert (cloud) să funcționeze, trebuie îndeplinite următoarele condiții:

- Infrastructura Kaspersky Endpoint Detection and Response Expert (cloud) să fie disponibilă în regiunea ta. Pentru informații despre disponibilitatea infrastructurii EDR Expert (cloud) în regiunea ta, contactează Asistența tehnică.
- OSMP (Open Single Management Platform) este instalat.
- Kaspersky Endpoint Security instalat în modul standard.
- Aplicația Kaspersky Endpoint Security este activată și funcționalitatea este acoperită de licență.
- Ai acceptat termenii Acordului de procesare a datelor Kaspersky Endpoint Detection and Response Expert (cloud).
- Componenta Endpoint Detection and Response Expert (cloud) este activată.
- Componentele aplicației care asigură funcționarea componentei EDR Expert (cloud) sunt activate și operaționale:
  - File Threat Protection.
  - Web Threat Protection.
  - Mail Threat Protection.
  - Exploit Prevention.
  - Behavior Detection.
  - Host Intrusion Prevention.

- Remediation Engine.
- Control adaptiv al anomaliilor.

Pași pentru integrarea cu EDR Expert (cloud)

Configurarea integrării EDR Expert (cloud) implică următorii pași:

1. **Instalarea componentei Endpoint Detection and Response Expert (cloud)**

   Poți selecta componenta Endpoint Detection and Response Expert (cloud) în timpul instalării sau efectuării upgrade-ului, precum și utilizând activitatea *Modificare componente ale aplicației*.

   > Trebuie să reporniți computerul pentru a finaliza efectuarea upgrade-ului aplicației cu noua componentă.

2. **Activarea Kaspersky Endpoint Detection and Response Expert (cloud)**

   Trebuie să achiziționezi o licență separată pentru Kaspersky Endpoint Detection and Response Expert (cloud).

   Funcționalitatea devine disponibilă după adăugarea unei chei separate pentru Kaspersky Endpoint Detection and Response Expert (cloud). Ca rezultat, sunt adăugate două chei pe computer: o cheie pentru Kaspersky Endpoint Security și o cheie pentru Kaspersky Endpoint Detection and Response Expert (cloud).

   Licențierea funcționalității individuale Endpoint Detection and Response Expert (cloud) se realizează la fel ca licențierea componentei Kaspersky Endpoint Security.

   Asigură-te că funcționalitatea componentei EDR Expert (cloud) este inclusă în licență și că aceasta se execută în interfața locală a aplicației.

3. **Conectarea la serverul de colectare a telemetriei și la serverul de răspuns**

   Kaspersky Endpoint Detection and Response Expert (cloud) necesită o conexiune de încredere între Kaspersky Endpoint Security și două servere:

   - Un *server de colectare a telemetriei* este un server care face parte dintr-o soluție SIEM și care colectează, normalizează, corelează, analizează și stochează informații despre evenimentele care au loc pe computer.
   - Un *server de răspuns* este un server pentru primirea și scanarea datelor, studierea comportamentului obiectelor și publicarea rezultatelor acestor studii.

   Cum conectezi un computer Kaspersky Endpoint Security la EDR Expert (cloud) utilizând Web Console

   1. În fereastra principală a Web Console, selectați fila **Asset management** → **Policies**.
   2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

      Se deschide fereastra de proprietăți a politicii.
   3. Selectați fila **Application settings**.
   4. Accesați **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (cloud)**.
   5. Activează componenta folosind comutatorul **Endpoint Detection and Response Expert (cloud) DISABLED**.

6. Dacă politica curentă este o politică secundară, iar politica principală interzice modificările aduse setărilor de integrare EDR Expert (cloud) („lacăt" închis), poți configura moștenirea setărilor în secțiunea **Inheritance**:

   - **Inherit connection settings from the policy** (valoare implicită). Setările de conectare vor fi moștenite de la politica părinte. Nu vei putea edita setările.
   - **Use custom connection settings**. Poți configura manual setările de conectare.

7. Fila **Response server** afișează numele de domeniu complet și portul serverului de răspuns, care sunt preluate automat. Dacă politica de securitate din infrastructura ta nu îți permite să te conectezi direct la serverele EDR Expert (cloud), poți configura o conexiune printr-un tunel TCP:

   a. Bifați caseta de selectare **Use a TCP tunnel for response**.

   b. Specifică adresa serverului (IPv4, IPv6) și portul pentru conectarea la tunel.

8. Dacă este necesar, setează frecvența de trimitere a solicitărilor de sincronizare către server în câmpul **Send sync request to server every (min)**. În timpul sincronizării, Kaspersky Endpoint Security primește sarcini de răspuns la amenințări și trimite rezultatele sarcinilor.

9. Accesați fila **Telemetry collection server**.

10. Configurează setările conexiunii la serverul de colectare a datelor de telemetrie:

    a. Faceți clic pe linkul **Edit**.

    b. În fereastra care se deschide, selectează serverul de colectare a datelor de telemetrie din listă. Colectorul KUMA servește drept server de colectare a datelor de telemetrie în EDR Expert (cloud). Pentru mai multe detalii, consultă Ajutor Kaspersky Unified Monitoring and Analysis Platform.

    Dacă apare o eroare în timpul conectării la serverul de colectare a telemetriei, selectează un alt server. Dacă nu te poți conecta la serverul de colectare a datelor de telemetrie, contactează Asistența tehnică.

    c. Dacă este necesar, poți configura o conexiune la serverul de colectare a telemetriei printr-un tunel TCP, la fel cum ai face pentru serverul de răspuns.

11. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Prin urmare, computerul este adăugat la lista dispozitivelor gestionate din cadrul Open Single Management Platform (OSMP). Verificați starea de funcționare a componentei, vizualizând *Report on status of application components*. De asemenea, puteți vizualiza starea de funcționare a unei componente în rapoarte, în interfața locală a Kaspersky Endpoint Security. Componenta **Endpoint Detection and Response Expert (cloud)** va fi adăugată la lista componentelor Kaspersky Endpoint Security.

Configurarea setărilor de telemetrie EDR Expert (cloud)

Telemetrie este o listă de evenimente care au avut loc pe computerul protejat. Kaspersky Endpoint Security analizează datele de telemetrie și le trimite către serverele de colectare a telemetriei în timpul sincronizării. Evenimentele de telemetrie ajung pe server aproape continuu. Kaspersky Endpoint Security inițiază sincronizarea cu serverul atunci când este îndeplinită oricare dintre următoarele condiții:

- intervalul de sincronizare a expirat;
- numărul de evenimente din memoria tampon depășește limita superioară.

Prin urmare, în mod implicit, aplicația se sincronizează la fiecare 30 de secunde sau ori de câte ori memoria tampon conține 1024 de evenimente. Puteți configura comportamentul de sincronizare în politica Kaspersky Endpoint Security și puteți selecta valorile optime care să corespundă încărcării rețelei dvs. (consultați instrucțiunile de mai jos).

Dacă nu există nicio conexiune între Kaspersky Endpoint Security și server, aplicația pune în coadă evenimentele noi. Când conexiunea este restabilită, Kaspersky Endpoint Security trimite evenimentele din coadă către server în ordinea corespunzătoare. Pentru a evita supraîncărcarea serverului, Kaspersky Endpoint Security poate sări peste unele evenimente. Pentru a activa acest lucru, puteți optimiza setările de transmitere a evenimentelor, de exemplu, puteți seta o valoare maximă pentru numărul evenimentelor pe oră (consultați instrucțiunile de mai jos).

Pentru a configura setările de telemetrie, urmează pașii de mai jos:

1. În fereastra principală a Web Console, selectați fila **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (cloud)**.
5. În fereastra care se deschide, selectează fila **Data transmission settings**.
6. Asigurați-vă că este selectată caseta de validare **Sending telemetry ENABLED**.
7. Dacă este necesar, bifați caseta de selectare **Send telemetry with IOA only**. *Indicatorul de atac (IOA)* este o regulă care conține o descriere a comportamentului suspect din sistem, care poate indica un atac țintit. Aplicația compară comportamentul curent din sistem cu aceste reguli și înregistrează în jurnal evenimentele care indică un atac țintit. Aplicația utilizează tehnologia *scanare în flux* care permite urmărirea în timp real a acestor evenimente.
8. Dacă este necesar, configurează setările de sincronizare a serverului:

   - **Maximum event transmission delay (sec)**. Aplicația se sincronizează cu serverul pentru a trimite evenimente după expirarea intervalului de sincronizare. Valoarea implicită este 30 de secunde.
   - **Maximum number of event packages**. Aplicația se sincronizează cu serverul atunci când memoria tampon este umplută cu evenimente. Valoarea implicită este de 1024 de evenimente.
9. Accesați fila **Request throttling**.

10. Dacă este necesar, dezactivează limitarea solicitărilor folosind comutatorul **Request throttling ENABLED**.

    Această caracteristică ajută la optimizarea încărcării serverului. Dacă această funcționalitate este activată, aplicația restricționează transmiterea evenimentului. Dacă numărul de evenimente depășește limitele configurate, Kaspersky Endpoint Security oprește trimiterea evenimentelor. Această opțiune este activată în mod implicit.

11. Configurați setările de optimizare pentru trimiterea evenimentelor către server:

    - **Maximum number of events per hour**. Aplicația analizează fluxul de date de telemetrie și restricționează trimiterea evenimentelor dacă fluxul de evenimente depășește limita de evenimente pe oră configurată. Kaspersky Endpoint Security reia trimiterea evenimentelor după o oră. Valoarea implicită este de 3000 de evenimente pe oră. Dacă aplicația este instalată pe un server, fluxul de date de telemetrie este mai mare. Pentru servere, se recomandă creșterea valorii la 60.000 de evenimente pe oră.

    - **Percentage of event limit excess (%)**. Aplicația sortează evenimentele după tip (de exemplu, evenimente „modificări în registry") și restricționează transmiterea evenimentelor dacă raportul dintre evenimente de același tip și numărul total de evenimente depășește limita configurată în procente. Kaspersky Endpoint Security reia trimiterea evenimentelor atunci când raportul dintre alte evenimente și numărul total de evenimente devine din nou suficient de mare. Valoarea implicită este 15%.

12. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Excluderi telemetrie EDR Expert (cloud)

Pentru a îmbunătăți performanța și a optimiza transmiterea datelor către serverul de telemetrie, poți adăuga excluderi de telemetrie. De exemplu, poți alege să nu trimiți date de comunicare în rețea pentru aplicații individuale.

> Utilizarea unui număr prea mare de reguli poate crește încărcarea pe serverul de colectare a telemetriei și poate reduce performanța computerului. Îți recomandăm să adaugi doar regulile necesare.

Pentru a crea o excludere de telemetrie în Web Console și în Cloud Console:

1. În fereastra principală a Web Console, selectați fila **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **General Settings** → **Telemetry Settings**.
5. Selectați fila **EDR Expert (cloud) telemetry**.
6. În blocul **General exclusions**, fă clic pe butonul **Add**.

   Se deschide fereastra **Add exclusion rule**.
7. Dacă este necesar, modifică starea regulii. În mod implicit, regula este activată.
8. Introdu un nume pentru regulă.

9. Selectează o acțiune care va fi efectuată atunci când este declanșată regula:

   - **Do not collect**. Evenimentul filtrat va fi exclus din datele de telemetrie trimise.
   - **Exclude IOA**. Evenimentul de declanșare a regulii IOA va fi exclus din datele de telemetrie trimise.

10. Dacă opțiunea **Exclude IOA** este selectată, specifică regulile IOA care vor fi adăugate la excluderi:

    - **Exclude all**. Când condiția specificată este îndeplinită, aplicația va exclude din telemetrie evenimentele generate pe baza tuturor regulilor IOA.
    - **Exclude by GUID**. Specifică GUID-ul regulii IOA. Poți specifica mai multe GUID-uri utilizând `,`. Pentru mai multe detalii privind regulile IOA, consultă Ajutor pentru EDR Expert (cloud).

11. Specifică condiția de filtrare:

    a. Selectează numele câmpului care va fi utilizat pentru filtrare.

    b. Selectează un operator (consultă tabelul de mai jos) și specifică valoarea cu care va fi comparată valoarea câmpului din eveniment.

Lista operatorilor condiționali

Operator	Descriere
<	Dacă valoarea câmpului este mai mică decât valoarea specificată în condiție, evenimentul va fi filtrat.
≤	Dacă valoarea câmpului este mai mică sau egală cu valoarea specificată în condiție, evenimentul va fi filtrat.
=	Dacă valoarea câmpului este egală cu valoarea specificată în condiție, evenimentul va fi filtrat.
≥	Dacă valoarea câmpului este mai mare sau egală cu valoarea specificată în condiție, evenimentul va fi filtrat.
>	Dacă valoarea câmpului este mai mare decât valoarea specificată în condiție, evenimentul va fi filtrat.
≠	Dacă valoarea câmpului nu este egală cu valoarea specificată în condiție, evenimentul va fi filtrat.
is like	Dacă valoarea câmpului corespunde cu masca specificată în condiție, evenimentul va fi filtrat. Aplicația acceptă caracterele `*` și `?` la introducerea unei măști:
is not like	Dacă valoarea câmpului nu corespunde măștii specificate în condiție, evenimentul va fi filtrat. Aplicația acceptă caracterele `*` și `?` la introducerea unei măști:
one of	Dacă valoarea câmpului corespunde uneia dintre valorile din lista specificată în condiție, evenimentul este considerat filtrat.
none of	Dacă valoarea câmpului nu corespunde niciuneia dintre valorile din lista specificată în condiție, evenimentul este considerat filtrat.
is like one of	Dacă valoarea câmpului corespunde uneia dintre măștile specificate în condiție, evenimentul va fi filtrat. Aplicația acceptă caracterele * și ? la introducerea unei măști.
is not like one of	Dacă valoarea câmpului nu corespunde niciuneia dintre măștile specificate în condiție, evenimentul va fi filtrat. Aplicația acceptă caracterele * și ? la introducerea unei măști.
exists	În cazul în care câmpul specificat în condiție este prezent în eveniment, evenimentul va fi filtrat.
not exists	În cazul în care câmpul specificat în condiție nu este prezent în eveniment, evenimentul va fi filtrat.
contains	Dacă valoarea specificată în condiție este prezentă în valoarea câmpului, evenimentul va fi filtrat.
is equal to	Dacă valoarea câmpului este egală cu valoarea specificată în condiție, evenimentul va fi filtrat. Scanarea ține cont de majuscule/minuscule.
bitwise AND	Dacă rezultatul operației Bitwise AND (&) între valoarea câmpului și valoarea specificată în condiție este 1, evenimentul va fi filtrat.

12. Dacă este necesar, poți crea criterii de filtrare complexe adăugând mai multe condiții de filtrare și grupuri de condiții. De asemenea, poți adăuga condiții imbricate și grupuri de condiții la un grup de condiții. Poți folosi următorii operatori:

    - **AND** înseamnă că filtrul selectează evenimente care îndeplinesc toate condițiile specificate.
    - **OR** înseamnă că filtrul selectează evenimente care îndeplinesc una dintre condițiile specificate.
    - **NOT** (pentru a utiliza acest operator, selectează opțiunea **Add NOT before**) înseamnă că filtrul selectează evenimente care nu îndeplinesc niciuna dintre condițiile specificate.

    Condițiile și grupurile de condiții de primul nivel sunt combinate cu operatorul **AND**.

13. Pentru a scana regula de filtrare creată, fă clic pe butonul **Check rule**.

    În fereastra care se deschide, va fi afișat un tabel cu evenimentele filtrate după regula creată. Pentru detalii, consultă Ajutor pentru EDR Expert (cloud).

14. Dacă este necesar, în **All event types**, adaugă excluderi de telemetrie după tipul de eveniment.

    a. Fă clic pe numele tipului de eveniment.

    b. În fereastra care se deschide, faceți clic pe butonul **Set up manually**.

    c. Dacă este necesar, configurează transmiterea telemetriei pentru tipul de eveniment selectat, utilizând comutatorul **Send event**. În mod implicit, transmiterea telemetriei este activată pentru toate tipurile de evenimente.

    d. În blocul **Exclusion rules**, fă clic pe butonul **Add**.

    Se deschide fereastra **Add exclusion rule**.

    e. Efectuează acțiunile descrise în pașii 7–13 pentru fiecare regulă pe care o adaugi.

15. Pentru anumite tipuri de evenimente, poți adăuga și reguli de includere pentru a extinde telemetria colectată:

    a. În blocul **Inclusion rules**, fă clic pe butonul **Add**.

    Se deschide fereastra **Add inclusion rules**.

    b. Introdu un nume pentru regulă.

    c. În **Condition**, introdu valori pentru câmpurile afișate. Tipul de câmpuri disponibile depinde de evenimentul selectat.

    Regulile de excludere au prioritate față de regulile de includere.

16. Pentru a aplica politica pe computere, asigură-te că lacătele sunt închise (🔒) și salvează modificările.

Exportarea și importarea filtrelor de evenimente EDR Expert (cloud)

Poți exporta lista de excluderi într-un fișier JSON. Apoi, poți modifica fișierul pentru a adăuga, de exemplu, un număr mare de înregistrări de ID-uri de evenimente. De asemenea, poți utiliza funcția de export/import pentru a face o copie de rezervă a filtrelor pentru evenimente sau pentru a migra lista pe un alt server.

Utilizarea unui număr prea mare de reguli poate crește încărcarea pe serverul de colectare a telemetriei și poate reduce performanța computerului. Îți recomandăm să adaugi doar regulile necesare.

Pentru a exporta și importa filtre pentru evenimente în Web Console:

1. În fereastra principală a Web Console, selectați fila **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **General Settings** → **Telemetry Settings**.
5. Selectați fila **EDR Expert (cloud) telemetry**.
6. Pentru a exporta filtrele pentru evenimente:
   a. Fă clic pe **Export**.
   b. În fereastra care se deschide, specifică numele fișierului JSON în care dorești să exporți filtrele pentru evenimente și selectează directorul în care dorești să salvezi acest fișier.
   c. Salvați fișierul.

      Kaspersky Endpoint Security exportă filtrele pentru evenimente în fișierul JSON.
7. Pentru a importa filtrele pentru evenimente:
   a. Fă clic pe **Import**.
   b. În fereastra care se deschide, selectează fișierul JSON din care dorești să importi filtrele pentru evenimente.
   c. Selectează modul în care dorești să fie importate regulile de filtrare a evenimentelor: prin adăugarea la regulile existente sau prin eliminarea regulilor existente și înlocuirea acestora cu altele noi.
   d. Deschideți fișierul.

8. Pentru a aplica politica pe computere, asigură-te că lacătele sunt închise (🔒) și salvează modificările.

1. În fereastra principală a Web Console, selectați fila **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **General Settings** → **Telemetry Settings**.
5. Selectați fila **EDR Expert (cloud) telemetry**.
6. Pentru a exporta filtrele pentru evenimente:

   a. Fă clic pe **Export**.

   b. În fereastra care se deschide, specifică numele fișierului JSON în care dorești să exporți filtrele pentru evenimente și selectează directorul în care dorești să salvezi acest fișier.

   c. Salvați fișierul.

   Kaspersky Endpoint Security exportă filtrele pentru evenimente în fișierul JSON.
7. Pentru a importa filtrele pentru evenimente:

   a. Fă clic pe **Import**.

   b. În fereastra care se deschide, selectează fișierul JSON din care dorești să importi filtrele pentru evenimente.

   c. Selectează modul în care dorești să fie importate regulile de filtrare a evenimentelor: prin adăugarea la regulile existente sau prin eliminarea regulilor existente și înlocuirea acestora cu altele noi.

   d. Deschideți fișierul.
8. Pentru a aplica politica pe computere, asigură-te că lacătele sunt închise (🔒) și salvează modificările.

Gestionarea carantinei

Carantină este un spațiu de stocare locală special de pe computer. Utilizatorul poate pune în carantină fișierele pe care le consideră periculoase pentru computer. Fișierele introduse în carantină sunt stocate într-o stare criptată și nu amenință securitatea dispozitivului. Kaspersky Endpoint Security utilizează Carantina numai atunci când este integrată cu soluțiile Kaspersky Detection and Response. În alte cazuri, Kaspersky Endpoint Security plasează fișierul relevant în Copie de rezervă. Pentru detalii privind gestionarea funcției Carantină ca parte a soluțiilor, consultă Kaspersky Sandbox Help, Kaspersky Endpoint Detection and Response Optimum Help, Kaspersky Endpoint Detection and Response Expert Help, Kaspersky Anti Targeted Attack Platform Help, and Kaspersky Endpoint Detection and Response Expert (on-premises) Help.

Kaspersky Endpoint Security utilizează contul de sistem (SYSTEM) pentru a pune în carantină fișierele.

Puteți configura setările carantinei numai în Consola Kaspersky Security Center. De asemenea, puteți utiliza Consola Kaspersky Security Center pentru a gestiona obiecte aflate în carantină (restaurare, ștergere, adăugare etc). La nivel local, pe computer, poți doar restaura obiectul folosind linia de comandă.

Configurarea dimensiunii maxime a Carantinei

În mod implicit, dimensiunea directorului Carantină este limitată la 1024 MO. Atunci când directorul Carantină atinge dimensiunea maximă, Kaspersky Endpoint Security oprește trimiterea fișierelor și generează evenimentul *Spațiu insuficient în spațiul de stocare Carantină*. Pentru a împiedica epuizarea spațiului pe disk pentru carantină, poți seta un prag la care Kaspersky Endpoint Security generează un eveniment *Spațiul de stocare pentru Carantină este aproape plin*. Nu poți configura o perioadă de păstrare pentru fișierele carantinate pentru a le elimina automat.

Dacă soluția Kaspersky Anti Targeted Attack Platform (EDR) este implementată în organizația dvs., vă recomandăm să creșteți dimensiunea Carantinei. Când faceți o scanare YARA, aplicația poate întâmpina un dump de memorie. Dacă dimensiunea dump-ului de memorie depășește dimensiunea Carantinei, scanarea YARA se termină cu o eroare și dump-ul memoriei nu este pus în carantină. Recomandăm setarea dimensiunii directorului Carantină egală cu dimensiunea totală a memoriei RAM de pe computer (de exemplu, 8 GO) sau dezactivarea limitei de dimensiune pentru Carantină.

Cum se configurează dimensiunea maximă a carantinei în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Setări generale** → **Rapoarte și Spații de stocare**.
4. În blocul **Carantină**, configurați dimensiunea pentru Carantină:
   - **Limitare dimensiune Carantină la N MO**. În cazul în care caseta de selectare este bifată, dimensiunea maximă a directorului Carantină este limitată la valoarea definită. În mod implicit, dimensiunea maximă este de 1024 MO. Când directorul Carantină atinge dimensiunea maximă, Kaspersky Endpoint Security trimite evenimentul *Spațiu insuficient în spațiul de stocare Carantină* către Kaspersky Security Center și publică evenimentul în Jurnalul de evenimente Windows. Între timp, aplicația nu mai pune în carantină obiecte noi. Trebuie să goliți directorul Carantină manual.

     Dacă este debifată caseta de selectare, dimensiunea directorului Carantină este limitată de spațiul liber disponibil pe disc.

   - **Notifică atunci când spațiul de stocare Carantină atinge N %**. Valoarea pragului pentru Carantină. De exemplu, puteți seta pragul pentru Carantină la 50%. Când directorul Carantină atinge pragul, Kaspersky Endpoint Security trimite evenimentul corespunzător către Kaspersky Security Center și publică evenimentul în Jurnalul de evenimente Windows. Între timp, aplicația continuă să pună în carantină obiecte noi.

     Dacă această casetă de selectare este debifată, aplicația nu generează evenimente atunci când este atins pragul directorului Carantină.
5. Salvați-vă modificările.

Cum se configurează dimensiunea maximă a Carantinei în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **General Settings** → **Reports and Storage**.

5. În blocul **Quarantine**, configurați dimensiunea pentru Carantină:

   - **Limit the size of Quarantine**. În cazul în care caseta de selectare este bifată, dimensiunea directorului Carantină este limitată la valoarea specificată. Dacă este debifată caseta de selectare, dimensiunea directorului Carantină este limitată de spațiul liber disponibil pe disc. Acest lucru poate fi necesar pentru Scanare YARA deoarece aplicația poate salva un fișier de imagine de memorie de dimensiuni mari.

   - **Maximum size of Quarantine (MB)**. În cazul în care caseta de selectare este bifată, dimensiunea maximă a directorului Carantină este limitată la valoarea definită. În mod implicit, dimensiunea maximă este de 1024 MO. Când directorul Carantină atinge dimensiunea maximă, Kaspersky Endpoint Security trimite evenimentul *Spațiu insuficient în spațiul de stocare Carantină* către Kaspersky Security Center și publică evenimentul în Jurnalul de evenimente Windows. Între timp, aplicația nu mai pune în carantină obiecte noi. Trebuie să goliți directorul Carantină manual.

     Dacă este debifată caseta de selectare, dimensiunea directorului Carantină este limitată de spațiul liber disponibil pe disc.

   - **Notify when the Quarantine storage reaches (%)**. Valoarea pragului pentru Carantină. De exemplu, puteți seta pragul pentru Carantină la 50%. Când directorul Carantină atinge pragul, Kaspersky Endpoint Security trimite evenimentul corespunzător către Kaspersky Security Center și publică evenimentul în Jurnalul de evenimente Windows. Între timp, aplicația continuă să pună în carantină obiecte noi.

6. Salvați-vă modificările.

Trimiterea datelor despre fișierele carantinate către Kaspersky Security Center

Pentru a efectua acțiuni cu obiecte carantinate în Web Console, trebuie să activați trimiterea datelor fișierelor carantinate către Serverul de administrare. De exemplu, poți descărca un fișier din carantină pentru analiză în Web Console. Trimiterea datelor fișierelor carantinate trebuie să fie activată pentru toate funcționalitățile Kaspersky Sandbox și Kaspersky Endpoint Detection and Response ca să funcționeze.

Cum se activează transferul datelor fișierelor carantinate în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.

2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

3. În fereastra politicii, selectați **Setări generale** → **Rapoarte și Spații de stocare**.

4. În blocul **Transfer de date pe serverul de administrare**, fă clic pe butonul **Setări**.

5. În fereastra care se deschide, bifați caseta de selectare **Fișiere carantină**.

6. Salvați-vă modificările.

Cum se activează transferul datelor fișierelor carantinate în Web Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **General Settings** → **KSC Integration**.
5. În blocul **Data transfer to Administration Server**, bifați caseta de selectare **About Quarantine files**.
6. Salvați-vă modificările.

Ca rezultat, puteți vizualiza o listă de fișiere, carantinate pe computer, în Consola Kaspersky Security Center. De asemenea, puteți utiliza Consola Kaspersky Security Center pentru a gestiona obiectele carantinate (restaurare, ștergere, adăugare etc). Pentru mai multe detalii desprelucrul cu Carantina, consultați Ajutor pentru Kaspersky Security Center.

Restaurarea fișierelor din Carantină

În mod implicit, Kaspersky Endpoint Security restaurează fișierele în directorul lor original. Dacă directorul de destinație a fost șters sau utilizatorul nu are drepturi de acces la acel director, aplicația plasează fișierul în directorul `%DataRoot%\QB\Restored`. Apoi, trebuie să mutați manual fișierul în folderul destinație.

Pentru restaurarea fișierelor din Carantină:

1. În fereastra principală a componentei Web Console, selectați **Operations** → **Repositories** → **Quarantine**.
2. Se deschide lista de fișiere în Carantină; în lista respectivă, selectați fișierele pe care doriți să le restaurați și faceți clic pe **Restore**.

   Kaspersky Endpoint Security restaurează fișierul. Dacă directorul de destinație conține deja un fișier cu același nume, aplicația anulează restaurarea fișierului. Pentru soluțiile EDR Optimum și EDR Expert, aplicația șterge fișierul după restaurare. Pentru alte soluții, aplicațiile păstrează o copie a fișierului în Carantină.

Monitorizarea acțiunilor EDR

Kaspersky Endpoint Security for Windows 12.9 introduce centrul de monitorizare a acțiunilor EDR. *Centrul de monitorizare a acțiunilor EDR* este o consolă în care poți vizualiza istoricul de Răspuns la amenințări pentru toate soluțiile Kaspersky Detection and Response. Dacă organizația are implementate multiple soluții Detection and Response (de exemplu, EDR Optimum și MDR), Kaspersky Endpoint Security afișează istoricul de Răspuns la amenințări pentru toate soluțiile. Aceasta permite analizarea performanței soluțiilor de detectare și răspuns pe un computer separat și optimizarea setărilor acestor soluții.

Centrul de monitorizare oferă următoarele informații:

- Informații despre sarcinile de răspuns la amenințare (de exemplu, *Termină procesul* sarcină)
- Modificări ale regulilor de izolare a rețelei și de prevenire a execuției

Dacă răspunsul la amenințare întâmpină o eroare legată de accesul la o partajare de rețea, o astfel de eroare este omisă din istoricul de răspuns la amenințări afișat.

Pentru a naviga la centrul de monitorizare a acțiunilor EDR:

1. În fereastra principală a Web Console, selectați **Asset management** → **Assets (Devices)**.
2. Selectează computerul pentru care dorești să configurezi setări locale pentru aplicație.

   Se vor deschide proprietățile computerului.
3. Selectați fila **Applications**.
4. Fă clic pe **Kaspersky Endpoint Security for Windows**.

   Se vor deschide setările locale pentru aplicație.
5. Selectați fila **Application settings**.
6. Accesați **Detection and Response** → **Response history**.

   Aceasta deschide consola centrală de monitorizare a acțiunii EDR. Poți utiliza consola pentru a vedea stările activității de Răspuns la amenințare, durata sarcinii, modificările regulilor și detaliile inițiatorului.

Kaspersky Unified Monitoring and Analysis Platform (KUMA)



Kaspersky Endpoint Security for Windows acceptă soluția Kaspersky Unified Monitoring and Analysis Platform. *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* este o soluție de management al informațiilor și evenimentelor de securitate (SIEM) pentru infrastructura IT a organizațiilor. KUMA permite detectarea, analizarea și atenuarea amenințărilor de securitate înainte ca acestea să poată provoca daune.

Kaspersky Endpoint Security este instalat pe computere individuale din infrastructura IT corporativă și monitorizează continuu procesele, conexiunile la rețea deschise și fișierele care sunt modificate. Informațiile despre evenimentele de pe computer (telemetrie) sunt trimise către serverul Kaspersky Unified Monitoring and Analysis Platform (KUMA). În consola sa, KUMA afișează evenimentele ca o listă fără marcaj, similară jurnalului de evenimente Windows.

Kaspersky Endpoint Security nu oferă toate funcționalitățile unui agent pentru KUMA. Aplicația trimite numai evenimente către KUMA fără indicatori. Pentru a avea acces la toate funcționalitățile KUMA, trebuie să cumpărați o licență și să implementați soluția în conformitate cu Ghidul administratorului KUMA.

Integrarea Kaspersky Endpoint Security cu KUMA

Pentru a utiliza KUMA, trebuie îndeplinite următoarele condiții:

- Kaspersky Security Center versiunea 14.2 sau o versiune ulterioară. În versiunile anterioare ale Kaspersky Security Center, este imposibil de activat funcționalitatea de integrare KUMA.
- Aplicația este activată și funcționalitatea este acoperită de licență.
- Componenta de integrare KUMA este activată.

Configurarea integrării KUMA implică următorii pași:

1. **Instalarea componentei de integrare KUMA**

   Puteți selecta componenta de integrare KUMA în timpul instalării sau efectuării upgrade-ului aplicației, precum și utilizând activitatea *Modificare componente ale aplicației*.

   Trebuie să reporniți computerul pentru a finaliza efectuarea upgrade-ului aplicației cu noua componentă.

2. **Activare KUMA**

   Pe lângă o licență a aplicației Kaspersky Endpoint Security (de exemplu, Kaspersky Endpoint Security for Business Standard), aveți nevoie de o licență separată pentru integrarea Kaspersky Endpoint Security cu KUMA (suplimentul de integrare Kaspersky Endpoint Security for Windows KUMA).

Dacă instalezi aplicația în modul EDR Agent, ai nevoie de o licență pentru integrarea Kaspersky Endpoint Security cu KUMA și o licență Kaspersky Anti Targeted Attack Platform (KATA) sau o licență Kaspersky Managed Detection and Response (MDR). Nu poți implementa EDR Agent numai pentru KUMA.

Funcționalitatea devine disponibilă după adăugarea cheii KUMA separată. Ca rezultat, va exista o altă cheie activă pe computer pentru integrarea Kaspersky Endpoint Security cu KUMA.

Licențierea funcționalității individuale KUMA se realizează la fel ca licențierea componentei Kaspersky Endpoint Security.

Asigurați-vă că funcționalitatea componentei KUMA este inclusă în licență și că aceasta funcționează în interfața locală a aplicației.

3 Conectarea la KUMA

Pentru a conecta computerul cu soluția Kaspersky Endpoint Security la soluția KUMA:

1. În politica Kaspersky Endpoint Security, adăugați adresele serverului KUMA și specificați setările de rețea ale conexiunii.
2. În consola KUMA, adăugați un colector cu conectori de tip tcp sau udp și specificați setările de bază ale rețelei pentru conexiune. Pentru detalii despre gestionarea colectorilor, consultați Ajutor Kaspersky Unified Monitoring and Analysis Platform.

Puteți stabili o conexiune de încredere între serverele Kaspersky Endpoint Security și KUMA. Pentru a configura o conexiune de încredere, trebuie să utilizați un certificat TLS. Puteți obține un certificat TLS pe serverul KUMA Core (consultați setările pentru conectorul de tip tcp în Ajutor Kaspersky Unified Monitoring and Analysis Platform). Apoi, trebuie să adăugați certificatul TLS la Kaspersky Endpoint Security (consultați instrucțiunile de mai jos).

Pentru a face conexiunea mai sigură, puteți activa suplimentar verificarea computerului în KUMA (autentificare mutuală). Pentru a activa această verificare, trebuie să activați autentificarea mutuală în setările KUMA și Kaspersky Endpoint Security. Pentru a utiliza autentificarea mutuală, veți avea nevoie și de un cripto-container. Un *cripto-container* este o arhivă PFX cu un certificat și o cheie privată. Trebuie să generați un certificat cu cheia privată în formatul containerului PKCS#12 într-o autoritate de certificare externă. Apoi, trebuie să adăugați arhiva PFX în consola KUMA și în Kaspersky Endpoint Security (consultați setările pentru conectorul de tip tcp în Ajutor Kaspersky Unified Monitoring and Analysis Platform).

Cum conectați un computer Kaspersky Endpoint Security la KUMA utilizând Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Integrare KUMA**.
4. Bifați caseta de selectare **Integrare KUMA**.
5. În blocul **Setări integrare**, bifați caseta de selectare **Activează transmiterea evenimentelor Windows către un server KUMA**.
6. Dacă este necesar, bifați caseta de selectare **Utilizează criptarea TLS** din blocul **Setări pentru conectarea la serverele KUMA**.

7. Configurează conexiunea de încredere:

   a. Fă clic pe **Setări pentru conectarea la serverele KUMA**.

   b. Configurați conexiunea la server:

   - **Expirare (sec)**. Expirarea timpului maxim de răspuns al serverului KUMA. Când timpul de expirare se termină, Kaspersky Endpoint Security încearcă să se conecteze la un alt server KUMA.
   - **Certificat TLS server**. Certificatul TLS pentru stabilirea unei conexiuni de încredere cu serverul KUMA. Poți obține un certificat TLS în consola Kaspersky Unified Monitoring and Analysis Platform (consultă instrucțiunile din Kaspersky Unified Monitoring and Analysis Platform).

     Pentru a stabili o conexiune de încredere, în consola KUMA, în setările conectorului tcp, trebuie să selectați modul TLS **With verification** (consultați setările pentru conectorul de tip tcp în Ajutor Kaspersky Unified Monitoring and Analysis Platform).
   - **Utilizează autentificarea mutuală**. Autentificare mutuală la stabilirea unei conexiuni securizate între Kaspersky Endpoint Security și KUMA. Pentru a utiliza autentificarea mutuală, în consola KUMA, în setările conectorului tcp, trebuie să selectați modul TLS **Custom PFX** (consultați setările pentru conectorul de tip tcp în Ajutor Kaspersky Unified Monitoring and Analysis Platform). Apoi trebuie să obțineți un criptocontainer și să setați o parolă pentru a proteja criptocontainerul. Un *cripto-container* este o arhivă PFX cu un certificat și o cheie privată. După configurarea setărilor KUMA, trebuie să activați și autentificarea mutuală în setările Kaspersky Endpoint Security și să încărcați un container crypto protejat prin parolă.

     > Criptocontainerul trebuie să fie protejat prin parolă. Nu este posibil să adăugați un criptocontainer cu o parolă necompletată.

   c. Fă clic pe **OK**.

8. Adaugă servere KUMA:

   a. Fă clic pe **Adaugă**.

   Această acțiune deschide formularul în care poți adăuga un server KUMA.

   b. Selectați protocolul pentru conectarea la serverele KUMA: **HTTP / HTTPS**, **TCP**, **UDP**.

   Dacă selectezi protocolul **HTTP / HTTPS** protocol, în mod implicit, aplicația utilizează HTTPS pentru conectarea la serverele KUMA. Pentru a utiliza HTTP, trebuie să specifici manual acest protocol în adresa serverului (de exemplu, `http://server.com`).

   c. Introdu adresa serverului (IPv4, IPv6) și portul de conectare la server.

   d. Fă clic pe **OK**.

   Kaspersky Endpoint Security se conectează la primul server KUMA din listă. Dacă conexiunea eșuează, Kaspersky Endpoint Security se conectează la al doilea server KUMA din listă și așa mai departe.

9. Dacă este necesar, configurați setarea **Întârziere maximă între transmiterea evenimentelor (sec)** în blocul **Setări transmitere date**. Când expiră timpul specificat, Kaspersky Endpoint Security încearcă să se conecteze la același server sau se conectează la următorul server din listă dacă există mai multe servere. Valoarea implicită este 30 de secunde.

10. Salvați-vă modificările.

Cum conectați un computer Kaspersky Endpoint Security la KUMA utilizând Web Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Built-in Agents Configuration** → **KUMA Integration**.
5. Duceți comutatorul **KUMA Integration ENABLED** la poziția activat.
6. Dacă este necesar, activează comutatorul **Use TLS encryption** în blocul **Server connection settings**.
7. Configurează conexiunea de încredere:

   a. Fă clic pe **Connection settings**.

   b. Configurați conexiunea la server:

   - **Timeout (sec)**. Expirarea timpului maxim de răspuns al serverului KUMA. Când timpul de expirare se termină, Kaspersky Endpoint Security încearcă să se conecteze la un alt server KUMA.
   - **Server TLS certificate**. Certificatul TLS pentru stabilirea unei conexiuni de încredere cu serverul KUMA. Poți obține un certificat TLS în consola Kaspersky Unified Monitoring and Analysis Platform (consultă instrucțiunile din Kaspersky Unified Monitoring and Analysis Platform).

     Pentru a stabili o conexiune de încredere, în consola KUMA, în setările conectorului tcp, trebuie să selectați modul TLS **With verification** (consultați setările pentru conectorul de tip tcp în Ajutor Kaspersky Unified Monitoring and Analysis Platform).
   - **Use two-way authentication**. Autentificare mutuală la stabilirea unei conexiuni securizate între Kaspersky Endpoint Security și KUMA. Pentru a utiliza autentificarea mutuală, în consola KUMA, în setările conectorului tcp, trebuie să selectați modul TLS **Custom PFX** (consultați setările pentru conectorul de tip tcp în Ajutor Kaspersky Unified Monitoring and Analysis Platform). Apoi trebuie să obțineți un criptocontainer și să setați o parolă pentru a proteja criptocontainerul. Un *cripto-container* este o arhivă PFX cu un certificat și o cheie privată. După configurarea setărilor KUMA, trebuie să activați și autentificarea mutuală în setările Kaspersky Endpoint Security și să încărcați un container crypto protejat prin parolă.

     > Criptocontainerul trebuie să fie protejat prin parolă. Nu este posibil să adăugați un criptocontainer cu o parolă necompletată.

   c. Fă clic pe **OK**.
8. Adaugă servere KUMA:

   a. Fă clic pe **Add**.

   Această acțiune deschide formularul în care poți adăuga un server KUMA.

b. Selectați protocolul pentru conectarea la serverele KUMA: **HTTP/HTTPS**, **TCP**, **UDP**.

Dacă selectezi protocolul **HTTP/HTTPS** protocol, în mod implicit, aplicația utilizează HTTPS pentru conectarea la serverele KUMA. Pentru a utiliza HTTP, trebuie să specifici manual acest protocol în adresa serverului (de exemplu, `http://server.com`).

c. Introdu adresa serverului (IPv4, IPv6) și portul de conectare la server.

d. Fă clic pe **OK**.

Kaspersky Endpoint Security se conectează la primul server KUMA din listă. Dacă conexiunea eșuează, Kaspersky Endpoint Security se conectează la al doilea server KUMA din listă și așa mai departe.

9. Dacă este necesar, configurați setarea **Maximum delay when sending events (sec)** în blocul **Server connection settings**. Când expiră timpul specificat, Kaspersky Endpoint Security încearcă să se conecteze la același server sau se conectează la următorul server din listă dacă există mai multe servere. Valoarea implicită este 30 de secunde.

10. Salvați-vă modificările.

Poți verifica dacă integrarea KUMA este configurată corect în consola KUMA (pentru detalii consultă Ajutor Kaspersky Unified Monitoring and Analysis Platform). Verificați starea de funcționare a componentei vizualizând *Report on status of application components* în consola Kaspersky Security Center. De asemenea, puteți vizualiza starea de funcționare a unei componente în rapoarte, în interfața locală a Kaspersky Endpoint Security. Componenta **Integrare KUMA** va fi adăugată la lista componentelor Kaspersky Endpoint Security.

4 **Activarea trimiterii datelor de telemetrie către serverul KUMA**

În mod implicit, trimiterea evenimentelor către serverul KUMA este dezactivată. Pentru a vă asigura că KUMA funcționează corect, trebuie să activați transmiterea datelor de telemetrie. Puteți selecta o sursă a evenimentului dintre jurnalele standard: *Application*, *Security* sau *System*.

Cum se activează trimiterea datelor de telemetrie către serverul KUMA în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.

2. În arborele consolei, selectați **Policies**.

3. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

4. În fereastra politicii, selectați **Setări generale → Excluderi și tipuri de obiecte**.

5. În blocul **Setări telemetrie → Telemetrie KUMA**, fă clic pe butonul **Setări**.

6. Selectați jurnalele de evenimente pe care doriți să le utilizați ca surse de evenimente: *Application*, *Security* sau *System*.

   Pe lângă jurnalele standard, puteți specifica un jurnalul al unei aplicații terțe.

7. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se activează trimiterea datelor de telemetrie către serverul KUMA în Web Console

1. În fereastra principală a Web Console, selectați fila **Asset management → Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **General Settings** → **Telemetry Settings**.

5. Selectați fila **KUMA telemetry**.

6. Selectați jurnalele de evenimente pe care doriți să le utilizați ca surse de evenimente: *Application*, *Security* sau *System*.

   Pe lângă jurnalele standard, puteți specifica un jurnalul al unei aplicații terțe.

7. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Filtrarea evenimentelor care urmează să fie trimise către KUMA

În mod implicit, trimiterea evenimentelor către serverul KUMA este dezactivată. Pentru a vă asigura că KUMA funcționează corect, trebuie să activați transmiterea datelor de telemetrie. Puteți selecta o sursă a evenimentului dintre jurnalele standard: *Application*, *Security* sau *System*. Pentru a îmbunătăți performanța și a optimiza transmiterea datelor către serverul KUMA, poți adăuga sau exclude manual evenimente individuale din telemetrie. De exemplu, poți exclude evenimentele Sysmon.

Cum să creezi o listă de evenimente care urmează să fie trimise către KUMA în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.

2. În arborele consolei, selectați **Policies**.

3. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.

4. În fereastra politicii, selectați **Setări generale** → **Excluderi și tipuri de obiecte**.

5. În blocul **Setări telemetrie** → **Telemetrie KUMA**, fă clic pe butonul **Setări**.

6. În fereastra care se afișează, configurează filtrele pentru evenimente care urmează să fie trimise către KUMA.

   Poți configura filtrarea evenimentelor pentru jurnalele standard *Application*, *Security*, *System* sau poți adăuga manual alt jurnal:

   a. Deschide proprietățile jurnalului sau fă clic pe butonul **Adaugă** și introdu numele jurnalului.

   b. Selectează un mod de trimitere a evenimentelor:

   - **Trimite toate evenimentele**. În acest mod, aplicația trimite toate evenimentele din jurnalul Windows, cu excepția evenimentelor adăugate la regulile de excludere.

   - **Trimite numai evenimentele selectate**. În acest mod, aplicația trimite numai evenimentele adăugate în regulile de includere.

c. Creează liste de reguli de excludere sau reguli de includere pentru modul de transmitere a evenimentelor relevant.

Pentru a adăuga reguli, trebuie să specifici ID-ul evenimentului în jurnalul de evenimente Windows. Poți lista mai multe ID-uri de evenimente într-o regulă. Pentru a specifica mai multe ID-uri de evenimente, utilizează caracterul virgulă (,).

d. Dacă este necesar, activează înregistrarea în jurnal a evenimentelor utilizând caseta de selectare de lângă numele jurnalului.

7. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum să creezi o listă de evenimente care urmează să fie trimise către KUMA în Web Console

1. În fereastra principală a Web Console, selectați fila **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **General Settings** → **Telemetry Settings**.

5. Selectați fila **KUMA telemetry**.

6. În fereastra care se afișează, configurează filtrele pentru evenimente care urmează să fie trimise către KUMA.

Poți configura filtrarea evenimentelor pentru jurnalele standard *Application*, *Security*, *System* sau poți adăuga manual alt jurnal:

a. Deschide proprietățile jurnalului sau fă clic pe butonul **Add** și introdu numele jurnalului.

b. Selectează un mod de trimitere a evenimentelor:

- **Send all events**. În acest mod, aplicația trimite toate evenimentele din jurnalul Windows, cu excepția evenimentelor adăugate la regulile de excludere.
- **Send only selected events**. În acest mod, aplicația trimite numai evenimentele adăugate în regulile de includere.

c. Creează liste de reguli de excludere sau reguli de includere pentru modul de transmitere a evenimentelor relevant.

Pentru a adăuga reguli, trebuie să specifici ID-ul evenimentului în jurnalul de evenimente Windows. Poți lista mai multe ID-uri de evenimente într-o regulă. Pentru a specifica mai multe ID-uri de evenimente, utilizează caracterul virgulă (,).

d. Dacă este necesar, activați înregistrarea în jurnal a evenimentelor utilizând comutatorul de lângă numele jurnalului.

7. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Exportarea și importarea filtrelor pentru evenimente KUMA

Poți exporta lista de excluderi într-un fișier JSON. Apoi, poți modifica fișierul pentru a adăuga, de exemplu, un număr mare de înregistrări de ID-uri de evenimente. De asemenea, poți utiliza funcția de export/import pentru a face o copie de rezervă a filtrelor pentru evenimente sau pentru a migra lista pe un alt server.

Utilizarea unui număr prea mare de reguli poate crește încărcarea serverului KUMA și poate reduce performanța computerului. Îți recomandăm să adaugi doar regulile necesare.

Cum se exportă și se importă filtrele pentru evenimente în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectați **Policies**.
3. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
4. În fereastra politicii, selectați **Setări generale** → **Excluderi și tipuri de obiecte**.
5. În blocul **Setări telemetrie** → **Telemetrie KUMA**, fă clic pe butonul **Setări**.
6. Pentru a exporta filtrele pentru evenimente:
   a. Selectează jurnalele de evenimente cu filtrele pe care dorești să le exporți.
   b. Fă clic pe butonul → **Exportă**.
   c. În fereastra care se deschide, specifică numele fișierului JSON în care dorești să exporți filtrele pentru evenimente și selectează directorul în care dorești să salvezi acest fișier.
   d. Salvați fișierul.
      Kaspersky Endpoint Security exportă filtrele pentru evenimente în fișierul JSON.
7. Pentru a importa filtrele pentru evenimente:
   a. Fă clic pe butonul → **Importă**.
   b. În fereastra care se deschide, selectează fișierul JSON din care dorești să importi filtrele pentru evenimente.
   c. Deschideți fișierul.
      Dacă există deja reguli de filtrare a evenimentelor pe computer, Kaspersky Endpoint Security le înlocuiește în momentul importului.
8. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se exportă și se importă filtre pentru evenimente în Web Console

1. În fereastra principală a Web Console, selectați fila **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **General Settings** → **Telemetry Settings**.
5. Selectați fila **KUMA telemetry**.
6. Pentru a exporta filtrele pentru evenimente:
   a. Selectează jurnalele de evenimente cu filtrele pe care dorești să le exporți.
   b. Fă clic pe butonul → **Export**.
   c. În fereastra care se deschide, specifică numele fișierului JSON în care dorești să exporți filtrele pentru evenimente și selectează directorul în care dorești să salvezi acest fișier.
   d. Salvați fișierul.

      Kaspersky Endpoint Security exportă filtrele pentru evenimente în fișierul JSON.
7. Pentru a importa filtrele pentru evenimente:
   a. Fă clic pe butonul → **Import**.
   b. În fereastra care se deschide, selectează fișierul JSON din care dorești să importi filtrele pentru evenimente.
   c. Deschideți fișierul.

      Dacă există deja reguli de filtrare a evenimentelor pe computer, Kaspersky Endpoint Security le înlocuiește în momentul importului.
8. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

De asemenea, poți exporta sau importa filtrele pentru evenimente în linia de comandă.

Ghid de migrare KSWS la KES

Începând cu versiunea 11.8.0, Kaspersky Endpoint Security for Windows acceptă funcționalitatea de bază a soluției Kaspersky Security for Windows Server (KSWS). *Kaspersky Security for Windows Server* protejează serverele care execută sisteme de operare Microsoft Windows și spațiile de stocare atașate la rețea împotriva virușilor și a altor amenințări la securitatea computerelor la care sunt expuse serverele și spațiile de stocare atașate la rețea în timpul schimbului de fișiere. Pentru informații detaliate despre modul în care funcționează soluțiile, consultați pagina Ajutor Kaspersky Security for Windows Server. Începând cu Kaspersky Endpoint Security 11.8.0, puteți migra de la Kaspersky Security for Windows Server la Kaspersky Endpoint Security for Windows și puteți utiliza aceeași soluție pentru a proteja stațiile de lucru și serverele.

Cerințe software

Înainte de a începe migrarea de la KSWS la KES, asigurați-vă că serverul dvs. îndeplinește cerințele hardware și software ale Kaspersky Endpoint Security for Windows. Listele cu versiunile de sisteme de operare acceptate sunt diferite pentru KES și KSWS. De exemplu, KES nu este compatibil cu serverele care rulează Windows Server 2003.

Cerințe minime de software pentru migrarea de la KSWS la KES:

- Kaspersky Endpoint Security pentru Windows 12.0.
- Kaspersky Security 11.0.1 for Windows Server.

  Dacă ai instalată o versiune anterioară a Kaspersky Security for Windows Server, îți recomandăm să actualizezi aplicația la cea mai recentă versiune. Expertul de conversie a politicilor și sarcinilor nu acceptă versiunile anterioare ale Kaspersky Security for Windows Server.
- Kaspersky Security Center 14.2

  Dacă aveți instalată o versiune anterioară a Kaspersky Security Center, actualizați-o la 14.2 sau la o versiune ulterioară. În această versiune a Kaspersky Security Center, expertul de conversie în bloc a politicilor și sarcinilor vă permite să migrați politicile într-un profil, mai degrabă decât într-o politică. În această versiune a Kaspersky Security Center, expertul de conversie în loc a politicilor și sarcinilor vă permite, de asemenea, să migrați o gamă mai largă de setări de politici.
- Kaspersky Endpoint Agent 3.10.

  Dacă aveți instalată o versiune anterioară a Kaspersky Endpoint Agent, vă recomandăm să actualizați aplicația la cea mai recentă versiune. Kaspersky Endpoint Security acceptă migrarea unei configurații [KSWS+KEA] către [KES+agent încorporat] începând cu Kaspersky Endpoint Agent 3.10.

Recomandări de migrare

Când migrați de la KSWS la KES, respectați următoarele recomandări:

- Planificați din timp migrarea de la KSWS la KES. Alegeți o perioadă în care serverele funcționează cu cea mai mică încărcare, de exemplu, în timpul weekendului.
- După migrare, porniți treptat componentele aplicației. Adică, de exemplu, începeți prin a activa doar componenta File Threat Protection, apoi activați alte componente de protecție, apoi activați componentele de control și așa mai departe. La fiecare etapă, trebuie să vă asigurați că aplicația funcționează corect și să monitorizați performanța serverului. Arhitectura KES diferă de cea a KSWS, prin urmare și sistemul de operare se poate comporta diferit.
- Efectuați migrarea treptat. Mai întâi migrați un singur server, apoi mai multe servere, apoi efectuați migrarea pe toate serverele organizației.
- Migrați separat diferite tipuri de servere. Adică, de exemplu, migrați mai întâi serverele de baze de date, apoi serverele de e-mail și așa mai departe.
- Migrarea pe serverele cu încărcare mare implică unele considerații speciale.

Etapele de migrare

Migrarea de la KSWS la KES se realizează în mod semiautomat. Acest lucru este necesar din cauza arhitecturilor diferite ale aplicațiilor. Pentru a migra setările de politici, trebuie să executați Expertul de conversie în bloc a politicilor și activităților (expertul de migrare). După migrarea setărilor de politici, trebuie să configurați manual setările pe care expertul de migrare nu le poate migra automat (de exemplu, setările de protecție prin parolă). După migrare, se recomandă, de asemenea, să verificați dacă expertul de migrare a migrat corect toate setările.

Migrează de la KSWS la KES în următoarea ordine:

1. **Migrați activitățile și politicile KSWS**

   După migrarea politicilor și a activităților, trebuie să efectuați pași de configurare suplimentari. De asemenea, vă recomandăm să vă asigurați că Kaspersky Endpoint Security oferă nivelul necesar de securitate după migrarea de la KSWS.

   > Expertul de conversie în bloc a politicilor și activităților pentru Kaspersky Security for Windows Server este disponibil numai în Consola de administrare (MMC). Politica și setările activităților nu pot fi migrate în Web Console și în Kaspersky Security Center Cloud Console.

2. **Instalați Kaspersky Endpoint Security**

Puteți instala Kaspersky Endpoint Security în următoarele moduri:

- Instalarea KES după îndepărtarea KSWS (recomandat).

  Utilitarul kavremover nu acceptă gestionarea KSWS.

- Instalarea KES peste KSWS.

3. Activarea KES cu o cheie KSWS

4. **Confirmați că aplicația este în stare de funcționare după migrare**

   După migrarea de la KSWS la KES, asigurați-vă că aplicația funcționează corect. Verificați starea serverului în consolă (ar trebui să fie *OK*). Asigurați-vă că nu sunt raportate erori pentru aplicație, verificați, de asemenea, ora ultimei conexiuni la serverul de administrare, ora ultimei actualizări a bazei de date și starea de protecție a serverului.

   Acordați o atenție deosebită migrării listelor de excludere, aplicațiilor de încredere, adreselor web de încredere, regulilor Application Control.

Corespondența dintre componentele KSWS și KES

La migrarea de la KSWS la KES, setul de componente este migrat numai atunci când aplicația este instalată local.

Corespondența dintre componentele Kaspersky Security for Windows Server și Kaspersky Endpoint Security for Windows

Componenta Kaspersky Security for Windows Server	Componenta Kaspersky Endpoint Security for Windows
Basic functionality	Nucleu aplicație
Log Inspection	Inspecție jurnal
Device Control	Control dispozitive
Firewall Management	*(nu sunt acceptate)* Funcțiile KSWS Firewall sunt realizate de Firewall-ul la nivel de sistem. În KES, o componentă separată este responsabilă pentru funcționalitatea Firewall. După migrare, puteți configura Kaspersky Endpoint Security Firewall.
File Integrity Monitor	Monitorizare integritate sistem
Exploit Prevention	Exploit Prevention
System Tray Icon	*(nu sunt acceptate)* Puteți configura interacțiunea utilizatorului în setările interfeței aplicației.
Integration with Kaspersky Security Center	Conector agent de rețea
Endpoint Agent	*(nu sunt acceptate)* În Kaspersky Endpoint Security 11.9.0, pachetul de distribuție Kaspersky Endpoint Agent nu mai face parte din kitul de distribuție al Kaspersky Endpoint Security. Trebuie să descarci separat pachetul de distribuție Kaspersky Endpoint Agent.
Network Threat Protection	Network Threat Protection
Anti-Cryptor	Behavior Detection
Anti-Cryptor for NetApp	*(nu sunt acceptate)*

Componenta Kaspersky Security for Windows Server	Componenta Kaspersky Endpoint Security for Windows
Traffic Security	Web Threat Protection Mail Threat Protection Control Web
On-Demand Scan	Nucleu aplicație
ICAP Network Storage Protection	*(nu sunt acceptate)* Kaspersky Endpoint Security nu acceptă componentele Protecția spațiilor de stocare atașate la rețea. Dacă aveți nevoie de aceste componente, puteți continua să utilizați Kaspersky Security for Windows Server.
RPC Network Storage Protection	*(nu sunt acceptate)* Kaspersky Endpoint Security nu acceptă componentele Protecția spațiilor de stocare atașate la rețea. Dacă aveți nevoie de aceste componente, puteți continua să utilizați Kaspersky Security for Windows Server.
Real-Time File Protection	File Threat Protection
Script Monitoring	*(nu sunt acceptate)* Componenta Monitorizare script este gestionată de alte componente, de exemplu, Protecție AMSI.
KSN Usage	Kaspersky Security Network
Applications Launch Control	Application Control
Performance counters	*(nu sunt acceptate)*

Corespondența setărilor KSWS și KES

La migrarea politicilor și activităților, KES este configurat în conformitate cu setările KSWS. Setările componentelor aplicației pe care KSWS nu le are sunt setate la valorile implicite.

Application settings

Scalability, interface and scanning settings

Setările aplicației nu sunt acceptate în Kaspersky Endpoint Security for Windows.

Setări aplicație

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Scalability settings	*(nu migrează)* Kaspersky Endpoint Security gestionează toate procesele de lucru.
Show System Tray Icon	*(nu migrează)* Pe un computer client, fereastra principală a Kaspersky Endpoint Security și pictograma din zona de notificare Windows sunt disponibile implicit. În meniul contextual al pictogramei, utilizatorul poate efectua operații cu Kaspersky Endpoint Security. Kaspersky Endpoint Security afișează, de asemenea, notificări deasupra pictogramei aplicației. Puteți configura interacțiunea utilizatorului în setările interfeței aplicației.
Restore file attributes after scanning	*(nu migrează)* Kaspersky Endpoint Security restaurează automat atributele fișierului după scanarea unui fișier.
Limit CPU usage for scanning threads	*(nu migrează)* Kaspersky Endpoint Security nu limitează utilizarea CPU în timpul scanării. Puteți configura ca activitatea să fie executată atunci când computerul funcționează la încărcare minimă.

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Folder for temporary files created during scanning	*(nu migrează)* Kaspersky Endpoint Security plasează fișierele temporare în directorul `C:\Windows\Temp`.
HSM system settings	*(nu migrează)* Kaspersky Endpoint Security nu acceptă sisteme HSM.

Security and reliability

Setările de securitate KSWS sunt migrate în secțiunea **Setări generale**, subsecțiunile **Setări aplicație** și **Interfață**.

Setări securitate aplicație

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Protect application processes from external threats	**Activează Autoprotecție** (subsecțiunea **Setări aplicație**)
Apply password protection	*(nu migrează)* Kaspersky Endpoint Security are o funcție încorporată de Protecție prin parolă (consultați subsecțiunea **Interfață**).
Perform task recovery	*(nu migrează)* Kaspersky Endpoint Security restaurează automat doar activitățile *Scanare malware*. Kaspersky Endpoint Security execută alte activități conform unei planificări.
Do not start scheduled scan tasks	**Amână activități planificate la funcționarea cu alimentare de la baterie** (subsecțiunea **Setări aplicație**)
Stop current scan tasks	*(nu migrează)* Când computerul este alimentat de un UPS, Kaspersky Endpoint Security nu oprește activitățile de scanare care se execută deja.

Connection settings

Setările de interacțiune cu Serverul de administrare sunt migrate în secțiunea **Setări generale**, subsecțiunile **Setări rețea** și **Setări aplicație**.

Setări interacțiune cu Serverul de administrare

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Proxy server settings	**Setări server proxy** (subsecțiunea **Setări rețea**)
Do not use proxy server for local addresses	**Ocolește serverul proxy pentru adrese locale** (subsecțiunea **Setări rețea**)
Proxy server authentication settings	**Utilizează autentificarea serverului proxy** (subsecțiunea **Setări rețea**) Parola de autentificare a serverului proxy nu este migrată. După migrarea unei politici, parola trebuie introdusă manual.
Use Kaspersky Security Center as a proxy server when activating the application	**Utilizează Kaspersky Security Center ca server proxy pentru activare** (subsecțiunea **Setări aplicație**)

Run local system tasks

Kaspersky Endpoint Security ignoră setările pentru executarea activităților locale de sistem ale Kaspersky Security for Windows Server. Puteți configura utilizarea activităților locale KES în **Activități locale**, **Gestionare activități**. De asemenea, puteți configura un program pentru executarea activităților *Scanare malware* și *Actualizarea modulelor bazelor de date și ale aplicațiilor* în proprietățile acestor activități.

Supplementary

Trusted zone

Setările zonei de încredere KSWS sunt migrate în secțiunea **Setări generale**, subsecțiunea **Excluderi**.

Setări zonă de încredere

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Object to scan (Exclusions)	**Excluderi de la scanare** (Excluderi de la scanare) Metodele folosite de KSWS și KES pentru selectarea obiectelor diferă. În timpul migrării, KES acceptă excluderile definite ca fișiere individuale sau căi către fișier/director. Dacă KSWS are excluderi configurate ca zonă predefinită sau un URL de script, aceste excluderi nu sunt migrate. După migrare, trebuie să adăugați manual astfel de excluderi. Excluderile ca zone predefinite trebuie să fie configurate în setările activității *Scanare malware*. Excluderile ca adrese web de script trebuie adăugate la adresele web de încredere pentru componenta Web Threat Protection.
Apply also to subfolders (Exclusions)	**Include subdirectoarele** (Excluderi de la scanare)
Objects to detect (Exclusions)	**Tipul obiectului detectat** (Excluderi de la scanare)
Exclusion usage scope (Exclusions)	**Componente de protecție** (Excluderi de la scanare) Dacă cel puțin o componentă este selectată în KSWS, KES aplică excluderile tuturor componentelor aplicației.
Comment (Exclusions)	**Comentariu** (Excluderi de la scanare)
Trusted process (Trusted process)	**Aplicații de încredere** Metodele de selectare a proceselor/aplicațiilor de încredere diferă în KSWS și KES. În timpul migrării, KES acceptă aplicații de încredere configurate ca o cale către fișierul executabil o mască. Dacă KSWS are procese de încredere configurate ca un hash fișier, astfel de procese de încredere nu sunt migrate. După migrare, trebuie să adăugați manual aceste procese de încredere.
Do not check file backup operations (Trusted process)	**Nu monitoriza activitatea aplicației** (Aplicații de încredere)

Removable drives scan

Setările Scanare unități amovibile sunt migrate în secțiunea **Activități locale**, subsecțiunea **Scanare unități amovibile**.

Setări Scanare unități amovibile

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Scan removable drives on connection via USB	**Acțiune la conectarea unei unități amovibile**
Scan removable drives if its stored data volume does not exceed (MB)	**Dimensiune maximă unitate amovibilă**

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Scan with security level: • **Maximum protection** • **Recommended** • **Maximum performance**	**Acțiune la conectarea unei unități amovibile**: • **Protecție maximă** • **Recomandat** Nivelurile de securitate KSWS corespund modurilor de scanare KES, după cum urmează: • Maximum protection – Protecție maximă • Recommended – Recomandat • Maximum performance – Recomandat

User permissions for application management

Kaspersky Endpoint Security nu acceptă alocarea permisiunilor de acces a utilizatorului pentru gestionarea aplicației și gestionarea serviciului aplicației. Puteți configura setările de acces pentru utilizatori și grupuri de utilizatori pentru gestionarea aplicației în Kaspersky Security Center.

User access permissions for Kaspersky Security Service management

Kaspersky Endpoint Security nu acceptă alocarea permisiunilor de acces a utilizatorului pentru gestionarea aplicației și gestionarea serviciului aplicației. Puteți configura setările de acces pentru utilizatori și grupuri de utilizatori pentru gestionarea aplicației în Kaspersky Security Center.

Storages

Setările spațiului de stocare KSWS sunt migrate în secțiunea **Setări generale**, subsecțiunea **Rapoarte și Spații de stocare** și în secțiunea **Essential Threat Protection**, subsecțiunea **Network Threat Protection**.

Setări spații de stocare

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Backup folder	*(nu migrează)* Kaspersky Endpoint Security salvează copiile de rezervă ale fișierelor în directorul `C:\ProgramData\Kaspersky Lab\KES.14.1\QB`.
Maximum Backup size (MB)	**Limitare dimensiune Copie de rezervă la N MO** (secțiunea **Setări generale** → **Rapoarte și Spații de stocare**)
Threshold value for space available (MB)	*(nu migrează)* Kaspersky Endpoint Security înregistrează în jurnal evenimentul *Spațiul de stocare pentru Carantină este aproape plin* când se atinge pragul de 50%.
Target folder for restoring objects	*(nu migrează)* Kaspersky Endpoint Security restaurează fișierele în directorul lor original.
Quarantine folder	*(nu migrează)* Kaspersky Endpoint Security salvează copiile de rezervă ale fișierelor în directorul `C:\ProgramData\Kaspersky Lab\KES.14.1\QB`.
Maximum Quarantine size (MB)	*(nu migrează)* Kaspersky Endpoint Security folosește Copie de rezervă pentru a stoca obiecte probabil infectate. În timpul migrării, Kaspersky Endpoint Security ignoră setările pentru Carantină.
Threshold value for space available (MB)	*(nu migrează)* Kaspersky Endpoint Security folosește Copie de rezervă pentru a stoca obiecte probabil infectate. În timpul migrării, Kaspersky Endpoint Security ignoră setările pentru Carantină.
Target folder for restoring objects	*(nu migrează)* Kaspersky Endpoint Security restaurează fișierele în directorul lor original.
Unblock automatically in N	**Blochează dispozitivele atacatoare timp de N min** (secțiunea **Essential Threat Protection** → **Network Threat Protection**)

Real-time server protection

Real-Time File Protection

Setările KSWS Real-Time File Protection sunt migrate în secțiunea **Essential Threat Protection**, subsecțiunea **File Threat Protection**.

Setări Protecție a fișierelor în timp real

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Objects protection mode: • **Smart mode** • **When run** • **On access** • **On access and modification**	**Mod de scanare**: • **Mod inteligent** • **La executare** • **La accesare** • **La accesare și modificare**
Deeper analysis of launching processes	*(nu migrează)* Kaspersky Endpoint Security acceptă un singur mod de analiză, modul Optimal.
Heuristic analyzer: • **Light** • **Medium** • **Deep**	**Analiză euristică**: • **Scanare ușoară** • **Scanare medie** • **Scanare profundă**
Apply Trusted Zone	*(nu migrează)* Kaspersky Endpoint Security aplică zona de încredere tuturor componentelor. Puteți configura excluderile în setări zonă de încredere.
Use KSN for protection	*(nu migrează)* Kaspersky Endpoint Security utilizează KSN pentru toate componentele aplicației.
Block access to network shared resources for the hosts that show malicious activity	*(nu migrează)* În mod implicit, Kaspersky Endpoint Security blochează accesul la resursele partajate în rețea pentru gazdele care prezintă activitate rău intenționată.
Launch critical areas scan when active infection is detected	*(nu migrează)* Kaspersky Endpoint Security nu lansează activitatea de scanare a zonelor critice atunci când este detectată o infecție activă.
Use Kaspersky Sandbox for protection	*(nu migrează)* În mod implicit, Kaspersky Endpoint Security trimite obiecte pentru scanare către Kaspersky Sandbox.
Protection scope	**Domeniu de protecție**
Schedule settings	*(nu migrează)* Kaspersky Endpoint Security folosește propria planificare pentru punerea în pauză a componentei File Threat Protection.

KSN Usage

Setările KSWS pentru Kaspersky Security Network sunt migrate în secțiunea **Advanced Threat Protection**, subsecțiunea **Kaspersky Security Network**.

Setări pentru Kaspersky Security Network

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
I confirm that I have fully read, understood, and accept the terms of participation in Kaspersky Security Network	**Declarația Kaspersky Security Network** Kaspersky Endpoint Security solicită acordul pentru Declarația Kaspersky Security Network atunci când aplicația este instalată, este creată o nouă politică sau este activată utilizarea Kaspersky Security Network.
Send data about scanned files	*(nu migrează)* Kaspersky Endpoint Security trimite automat date despre fișierele scanate dacă KSN este activat.

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Send data about requested URLs	*(nu migrează)* Kaspersky Endpoint Security trimite automat date despre URL-urile scanate dacă KSN este activat.
Send Kaspersky Security Network statistics	**Activează modul KSN extins**
Accept the terms of the Kaspersky Managed Protection Statement	*(nu migrează)* Kaspersky Endpoint Security nu include serviciul KMP.
Action to perform on KSN untrusted objects	*(nu migrează)* Puteți configura Acțiune la detectarea amenințărilor în setările componentei Protecție și în setările activității de scanare.
Do not calculate checksum before sending to KSN if file size exceeds N MB	*(nu migrează)* Puteți configura restricții de scanare a fișierelor mari în setările componentei Protecție și în setările activității de scanare.
Use Kaspersky Security Center as KSN Proxy	**Utilizează Serverul de administrare ca server proxy KSN**
Schedule settings	*(nu migrează)* Nu este posibilă configurarea unei planificări separate pentru componentă. Componenta este întotdeauna activată în timp ce Kaspersky Endpoint Security este operațional.

Traffic Security

Setările KSWS Traffic Security sunt migrate în secțiunea **Essential Threat Protection**, subsecțiunile **Web Threat Protection** și **Mail Threat Protection**, secțiunea **Security Controls**, subsecțiunea **Control Web**, secțiunea **Setări generale**, subsecțiunea **Setări rețea**.

Setări Securitate trafic

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Apply URL-based rules	**Control Web** (subsecțiunea **Control Web**) Regulile bazate pe URL sunt migrate în reguli separate în Kaspersky Endpoint Security.
Apply certificate-based rules	*(nu migrează)* Kaspersky Endpoint Security nu acceptă reguli bazate pe certificate.
Apply rules for web traffic category control	**Control Web** (subsecțiunea **Control Web**) Regulile de blocare pentru controlul categoriei trafic web sunt migrate într-o singură regulă de blocare în Kaspersky Endpoint Security. Kaspersky Endpoint Security ignoră regulile de permitere pentru controlul categoriilor. Corespondența dintre categoriile KSWS și KES este listată mai jos.
Allow access if the web page can not be categorized	*(nu migrează)* Kaspersky Endpoint Security permite accesul dacă pagina web nu poate fi clasificată.
Allow access to legitimate web resources that can be used to damage a protected device	*(nu migrează)* Kaspersky Endpoint Security permite accesul la resurse web legitime care pot fi utilizate pentru a deteriora un dispozitiv protejat
Allow access to legitimate advertisement	*(nu migrează)* Puteți gestiona accesul la reclame legitime folosind categoria de resurse web *Bannere* din setările componentei Control Web.
Operation mode: • **Driver Interceptor** • **Redirector** • **External Proxy**	*(nu migrează)* Kaspersky Endpoint Security acceptă doar modul Driver Interceptor.
ICAP-service connection settings	*(nu migrează)* Kaspersky Endpoint Security nu acceptă ICAP Network Storage Protection.
Check safe connections through the HTTPS protocol	Modul **Scanează conexiunile criptate** / **Scanează întotdeauna conexiunile criptate** (subsecțiunea **Setări rețea**)

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Use TLS protocol version	*(nu migrează)* Kaspersky Endpoint Security scanează traficul de rețea criptat transmis prin următoarele protocoale: • SSL 3.0. • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. În plus, puteți bloca conexiunile SSL 2.0 în setări scanare conexiuni criptate.
Do not trust web-servers with invalid certificate	**Adresă** (subsecțiunea **Setări rețea**)
Intercept ports (Interception area)	**Porturi monitorizate** (subsecțiunea **Setări rețea**) În timpul migrării, KES debifează casetele de selectare **Monitorizează toate porturile pentru aplicațiile din lista recomandată de Kaspersky** și **Monitorizare toate porturile pentru aplicații specificate**.
Exclude ports (Interception area)	*(nu migrează)*
Exclude IP addresses (Interception area)	**Configurează adresele de încredere** (subsecțiunea **Setări rețea**)
Exclude processes (Interception area)	**Configurează aplicațiile de încredere** (subsecțiunea **Setări rețea**) În timpul migrării, KES configurează următoarele setări pentru aplicația de încredere: • caseta de selectare **Nu scana traficul de rețea** este bifată. KES nu scanează traficul de rețea pentru nicio adresă IP la distanță și niciun port. • Celelalte casete de selectare din setările aplicației de încredere sunt debifate.
Security port	*(nu migrează)*
Use malicious URL database to scan web links	**Verifică adresa web în baza de date cu adrese web rău intenționate** (subsecțiunea **Web Threat Protection**)
Use anti-phishing database to scan web pages	**Verifică adresa web în baza de date cu adrese web de phishing** (subsecțiunea **Web Threat Protection**)
Use KSN for protection	*(nu migrează)* Kaspersky Endpoint Security utilizează KSN pentru toate componentele aplicației.
Use Trusted Zone	*(nu migrează)* Kaspersky Endpoint Security aplică zona de încredere tuturor componentelor. Puteți configura excluderile în setări zonă de încredere.
Use heuristic analyzer	**Utilizează analiza euristică** (subsecțiunile **Web Threat Protection** și **Mail Threat Protection**)
Security level	*(nu migrează)* Kaspersky Endpoint Security are propriile niveluri de securitate pentru componentele Web Threat Protection și Mail Threat Protection. În mod implicit, Kaspersky Endpoint Security setează nivelul de securitate recomandat.
Enable mail threat protection	**Mail Threat Protection** (subsecțiunea **Mail Threat Protection**) **Conectează extensia Microsoft Outlook** **Numai mesajele primite** (Domeniu de protecție) **Scanează la primire** (Protecție pentru e-mail)
Schedule settings	*(nu migrează)* Nu este posibilă configurarea unei planificări separate pentru componentă. Componenta este întotdeauna activată în timp ce Kaspersky Endpoint Security este operațional.

Exploit Prevention

Setările KSWS Exploit Prevention sunt migrate în secțiunea **Advanced Threat Protection**, subsecțiunea **Exploit Prevention**.

Setări Exploit Prevention

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Prevent vulnerable processes exploit: • **Terminate on exploit** • **Notify only**	**La detectarea exploatării**: • **Blochează** • **Informează**

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Notify about abused processes via Terminal Service	*(nu migrează)* Kaspersky Endpoint Security nu acceptă Terminal Services.
Prevent vulnerable processes exploit even if Kaspersky Security Service is disabled	*(nu migrează)* Kaspersky Endpoint Security previne constant exploatările proceselor vulnerabile.
Protected processes	**Activează protecția memoriei pentru procese de sistem** Kaspersky Endpoint Security nu acceptă selectarea proceselor protejate. Puteți activa doar protecția memoriei pentru procese de sistem.
Exploit prevention techniques: • **Apply all available exploit prevention techniques** • **Apply selected exploit prevention techniques**	*(nu migrează)* Kaspersky Endpoint Security aplică toate tehnicile disponibile de prevenire a exploatării.

Network Threat Protection

Setările KSWS Network Threat Protection sunt migrate în secțiunea **Essential Threat Protection**, subsecțiunea **Network Threat Protection**.

Setări Network Threat Protection

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Operation mode: • **Pass-through** • **Only inform about network attacks** • **Block connections when attack is detected**	**Network Threat Protection** Dacă este selectat modul **Pass-through**, componenta Network Threat Protection este dezactivată. Dacă este selectat modul **Only inform about network attacks** sau **Block connections when attack is detected**, componenta Network Threat Protection este activată. Kaspersky Endpoint Security funcționează întotdeauna în modul **Block connections when attack is detected**.
Do not stop traffic analysis when the task is not running	*(nu migrează)* Kaspersky Endpoint Security analizează continuu traficul dacă componenta este activată.
Do not control excluded IP addresses	**Excluderi**
Schedule settings	*(nu migrează)* Nu este posibilă configurarea unei planificări separate pentru componentă. Componenta este întotdeauna activată în timp ce Kaspersky Endpoint Security este operațional.

Script Monitoring

Kaspersky Endpoint Security nu acceptă componenta Monitorizare script. Componenta Monitorizare script este gestionată de alte componente, de exemplu, Protecție AMSI.

Website categories

Kaspersky Endpoint Security nu acceptă toate categoriile componentei Kaspersky Security for Windows Server. Categoriile care nu există în Kaspersky Endpoint Security nu sunt migrate. Prin urmare, regulile de clasificare a resurselor web cu categorii neacceptate nu sunt migrate.

Categorii de site-uri web

Categorii Kaspersky Security for Windows Server	Categorii Kaspersky Endpoint Security for Windows
Wargaming	Jocuri video
Abortion	*(nu migrează)*
Lotteries (extended)	Jocuri de noroc, loterii, pronosport
Alcohol	Alcool, tutun, narcotice
Anonymous proxy servers	Instrumente de anonimizare
Anorexia	*(nu migrează)*
Rentals for real estate	*(nu migrează)*

Categorii Kaspersky Security for Windows Server	Categorii Kaspersky Endpoint Security for Windows
Audio, video and software	Software, audio, video
Banks	Bănci
Blogs	Bloguri
Military	Arme, explozibili, subiecte pe teme militare
For children	*(nu migrează)*
Discrimination	Violență, intoleranță
Home and family	*(nu migrează)*
Hosting and domain services	Comunicare pe internet
Pets and animals	*(nu migrează)*
Law and politics	Interzis de legile regionale
Restricted by Roskomnadzor (RF)	Interzis de legile din Federația Rusă
Restricted by Federal Law 436 (RF)	Interzis de legile din Federația Rusă
Restricted by RF legislation	Interzis de legile din Federația Rusă
Restricted by global legislation	Interzis de legile regionale
Adult dating	Conținut pentru adulți
Internet services	*(nu migrează)*
Sex shops	Conținut pentru adulți
Information technologies	*(nu migrează)*
Casinos, card games	Jocuri de noroc, loterii, pronosport
Books and writing	*(nu migrează)*
Computer games	Jocuri video
Health and beauty	*(nu migrează)*
Culture and society	*(nu migrează)*
LGBT	Conținut pentru adulți
Lotteries	Jocuri de noroc, loterii, pronosport
Medicine	*(nu migrează)*
Fashion	*(nu migrează)*
Music	*(nu migrează)*
Drugs	Alcool, tutun, narcotice
Violence	Violență, intoleranță
Discontent	*(nu migrează)*
Illegal drugs	Alcool, tutun, narcotice
Hate and discrimination	Violență, intoleranță
Obscene vocabulary	Limbaj blasfemator sau obscen
Lingerie	Conținut pentru adulți
News	Medii de știri
Nudism	Conținut pentru adulți
Education	*(nu migrează)*
Online shopping	Magazine online
All communication media	Comunicare pe internet
Payment by credit cards	Sisteme de plată

Categorii Kaspersky Security for Windows Server	Categorii Kaspersky Endpoint Security for Windows
Online shopping (own payment system)	Magazine online
Online encyclopedias	*(nu migrează)*
Online banking	Bănci
Weapons	Arme, explozibili, subiecte pe teme militare
Fishing and hunting	*(nu migrează)*
Payment systems	Sisteme de plată
Job search	Căutare locuri de muncă
Search engines	*(nu migrează)*
Police decision (JP)	Interzis de Poliția din Japonia
Trusted by KPSN	*(nu migrează)*
Untrusted by KPSN	*(nu migrează)*
Porn	Conținut pentru adulți
Media hosting and streaming	Medii de știri
Web Mail	E-mail bazat pe web
Traveling	*(nu migrează)*
TV and radio	Medii de știri
Teasers and ads services	Bannere
Religion	Religii, asociații religioase
Restaurants, cafe and food	*(nu migrează)*
Dating sites	Site-uri matrimoniale
Sex education	Conținut pentru adulți
Social networks	Rețele de socializare
Sport	*(nu migrează)*
Betting	Jocuri de noroc, loterii, pronosport
Suicide	Violență, intoleranță
Tobacco	Alcool, tutun, narcotice
Torrents	Torrente
Mentioned in Federal list of extremists (RF)	Interzis de legile din Federația Rusă
File sharing	Partajare fișiere
Pharmacy	*(nu migrează)*
Hobby and entertainment	*(nu migrează)*
Chats and forums	Chaturi, forumuri, MI
Schools and universities pages	*(nu migrează)*
Astrology and esoterica	*(nu migrează)*
Extremism and racism	Violență, intoleranță
E-commerce	Magazine online
Erotic	Conținut pentru adulți
Humor	*(nu migrează)*

Local activity control

Applications Launch Control

Setările componentei Control aplicații a KSWS sunt migrate în secțiunea **Security Controls**, subsecțiunea Application Control.

Setările componentei Control lansare aplicații

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Operation mode: • **Statistics only** • **Active**	**Acțiune** (Application Control): • **Testează regulile**. • **Aplica reguli**.
Repeat action taken for the first file launch on all the subsequent launches for this file	*(nu migrează)* Kaspersky Endpoint Security scanează aplicația de fiecare dată când încearcă să se execute.
Deny the command interpreters launch with no command to execute	*(nu migrează)* Kaspersky Endpoint Security permite executarea interpreților comenzii dacă nu sunt interzișii de Application Control.
Rules	**Reguli Application Control** *(compatibil cu limitări)* Kaspersky Endpoint Security 11.11.0 introduce suport pentru migrarea regulilor Control lansare aplicații. Funcționalitatea de migrare a regulilor Control lansare aplicații are unele limitări. În mod implicit, Control lansare aplicații KSWS include două reguli: • **Allow scripts and MSI by OS-trusted certificate** • **Allow executable by OS-trusted certificate** Dacă cel puțin o regulă KSWS sursă are tipul **Allow**, în timpul migrării KES creează o nouă regulă de permitere, **Applications with trusted root certificates**. Adică, KES Application Control folosește o singură regulă pentru a permite executarea scripturilor de încredere, a pachetelor MSI și a fișierelor executabile. Dacă ambele reguli KSWS sursă au tipul **Deny**, KES nu adaugă reguli pentru gestionarea aplicațiilor cu certificate rădăcină de încredere.
Apply rules to executable files	*(nu migrează)* Domeniul de aplicare al regulilor nu poate fi configurat în setările KES Application Control. KES Application Control aplică reguli tuturor tipurilor de fișiere: fișiere executabile, scripturi și pachete MSI. Dacă toate tipurile de fișiere sunt incluse în domeniul de aplicare al regulilor în KSWS, în timpul migrării, KES transferă regulile KSWS. Dacă un anumit tip de fișier este exclus din domeniul de aplicare al regulilor în KSWS, în timpul migrării, KES transferă și regulile KSWS, dar **Testează regulile** este selectată ca acțiune Application Control.
Monitor loading of DLL modules	**Monitorizați încărcarea modulelor DLL (crește semnificativ sarcina asupra sistemului)**
Apply rules to scripts and MSI packages	*(nu migrează)* Domeniul de aplicare al regulilor nu poate fi configurat în setările KES Application Control. KES Application Control aplică reguli tuturor tipurilor de fișiere: fișiere executabile, scripturi și pachete MSI. Dacă toate tipurile de fișiere sunt incluse în domeniul de aplicare al regulilor în KSWS, în timpul migrării, KES transferă regulile KSWS. Dacă un anumit tip de fișier este exclus din domeniul de aplicare al regulilor în KSWS, în timpul migrării, KES transferă regulile KSWS, dar **Testează regulile** este selectată ca acțiune Application Control.
Deny applications untrusted by KSN	*(nu migrează)* Kaspersky Endpoint Security nu ține cont de reputația aplicațiilor și permite sau refuză executarea aplicațiilor în conformitate cu regulile.
Allow applications trusted by KSN	În timpul migrării, KES adaugă o nouă regulă de permitere. Categoria KL **Alt software\Aplicații, considerate de încredere în funcție de reputația din KSN** este specificată ca fiind condiția de declanșare a regulii.
Users and / or user groups allowed to run applications trusted by KSN	**Utilizatori și drepturile lor** într-o regulă de permitere Application Control care include categoria KL **Alt software\Aplicații, considerate de încredere în funcție de reputația din KSN**.
Automatically allow software distribution via applications and packages listed	Software Distribution Control în KSWS și KES funcționează diferit. În timpul migrării, KES adaugă noi reguli de permitere pentru aplicațiile care au permisă distribuirea automată a software-ului. Hash-ul fișierului este specificat drept condiție de declanșare a regulii.

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Always allow software distribution via Windows Installer	Software Distribution Control în KSWS și KES funcționează diferit. În timpul migrării, KES adaugă noi reguli de permitere pentru aplicațiile care au permisă distribuirea automată a software-ului (**Software distribution applications and packages allowed**). Hash-ul fișierului este specificat drept condiție de declanșare a regulii. În proprietățile contului, este bifată caseta de selectare **Programe de actualizare de încredere**.
Always allow software distribution via SCCM using the Background Intelligent Transfer Service	*(nu migrează)*
Software distribution applications and packages allowed	Software Distribution Control în KSWS și KES funcționează diferit. În timpul migrării, KES adaugă noi reguli de permitere pentru aplicațiile care au permisă distribuirea automată a software-ului. Hash-ul fișierului este specificat drept condiție de declanșare a regulii. În proprietățile contului, este bifată caseta de selectare **Programe de actualizare de încredere**.
Schedule settings	*(nu migrează)* Dacă o programare este configurată pentru componentă în setările KSWS, componenta Application Control este activată după migrare. Dacă o programare nu este configurată pentru componentă în setările KSWS, componenta Application Control este dezactivată după migrare. Nu este posibilă configurarea unei planificări separate pentru componentă. Componenta este întotdeauna activată în timp ce Kaspersky Endpoint Security este operațional.

Device Control

Setările componentei Control dispozitive a KSWS sunt migrate în secțiunea **Security Controls**, subsecțiunea Control dispozitive.

Setări Control dispozitive

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Operation mode: • **Active** • **Statistics only**	*(nu migrează)* Application Control funcționează în modul *Active*. Statisticile de conectare a dispozitivului sunt furnizate în mod continuu de Audit.
Allow using all external devices when the Device Control task is not running	*(nu migrează)* Componenta Control dispozitive este întotdeauna activată în timp ce Kaspersky Endpoint Security este în execuâie.
Device Control rules	**Dispozitive de încredere** În timpul migrării, Kaspersky Endpoint Security ignoră regulile KSWS dezactivate.
Schedule settings	*(nu migrează)* Kaspersky Endpoint Security utilizează propria planificare pentru obținerea accesului la anumite tipuri de dispozitive.

Network-Attached Storages Protection

RPC Network Storage Protection

Kaspersky Endpoint Security nu acceptă componentele Protecția spațiilor de stocare atașate la rețea. Dacă aveți nevoie de aceste componente, puteți continua să utilizați Kaspersky Security for Windows Server.

ICAP Network Storage Protection

Kaspersky Endpoint Security nu acceptă componentele Protecția spațiilor de stocare atașate la rețea. Dacă aveți nevoie de aceste componente, puteți continua să utilizați Kaspersky Security for Windows Server.

Anti-Cryptor for NetApp

Kaspersky Endpoint Security nu acceptă Anti-Cryptor pentru NetApp. Funcționalitatea Anti-Cryptor este furnizată de alte componente ale aplicației, cum ar fi Behavior Detection.

Network activity control

Firewall Management

Kaspersky Endpoint Security nu acceptă KSWS Firewall Management. Funcțiile KSWS Firewall sunt realizate de Firewall-ul la nivel de sistem. După migrare, puteți configura Kaspersky Endpoint Security Firewall.

Anti-Cryptor

Setările Network Threat Protection sunt migrate în secțiunea **Advanced Threat Protection**, subsecțiunea **Behavior Detection**.

Setări Anti-Cryptor

Setări KSWS	Setări KES
Operation mode: • **Statistics only** • **Active**	**La detectarea criptării externe a directoarelor partajate**: • **Informează** • **Blochează**
Heuristic analyzer	*(nu migrează)* Kaspersky Endpoint Security nu utilizează analiza euristică pentru Behavior Detection.
Configuration of protection scope: • **All shared network folders on the protected device** • **Only specified shared folders**	*(nu migrează)* Kaspersky Endpoint Security împiedică criptarea tuturor directoarelor de rețea partajate ale computerului protejat.
Exclusions	*(nu migrează)* Kaspersky Endpoint Security are propriile excluderi pentru componenta Behavior Detection. Puteți adăuga manual excluderi după migrare.
Schedule settings	*(nu migrează)* Nu este posibilă configurarea unei planificări separate pentru componentă. Componenta este întotdeauna activată în timp ce Kaspersky Endpoint Security este operațional.

System Inspection

File Integrity Monitor

Setări File Integrity Monitor din KSWS sunt migrate în secțiunea **Security Controls**, subsecțiunea **Monitorizare integritate sistem**.

Setări File Integrity Monitor

Setări KSWS	Setări KES
Log information about file operations that appear during the monitor interruption period	*(nu migrează)* Kaspersky Endpoint Security nu înregistrează în jurnal evenimente pentru operațiunile de fișiere efectuate în perioada de întrerupere a monitorizării.
Block attempts to compromise the USN log	*(nu migrează)* Kaspersky Endpoint Security nu blochează încercările de a compromite jurnalul USN.
Monitoring scope	**Domeniu monitorizare** → **Fișier** *(acceptat cu limitări)* Înregistrările domeniului de monitorizare dezactivate nu sunt migrate la KES. Kaspersky Endpoint Security adaugă doar înregistrările activate la domeniul de monitorizare.

Setări KSWS	Setări KES
Trusted users	**Utilizatori și/sau grupuri de utilizatori de încredere**
File operation markers	**Markeri operațiune cu fișiere**
Calculate checksum for the file if possible	**Hashing**
Exclusions	**Excluderi → Fișier**

Log Inspection

Setările Setări Inspecție jurnal din KSWS sunt migrate în secțiunea **Security Controls**, subsecțiunea **Inspecție jurnal**.

Setări Inspecție jurnal

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Apply custom rules for log inspection	*(nu migrează)* Kaspersky Endpoint Security aplică toate regulile personalizate activate.
Custom rules	**Reguli personalizate** Regula predefinită **A service was installed in the system (for Server 2003 OS)** nu este migrată în KES.
Apply predefined rules for log inspection	*(nu migrează)* Kaspersky Endpoint Security aplică toate regulile predefinite activate.
Predefined rules	**Reguli predefinite**
Password brute-force detection	**Detectare atac prin forță brută**
Network logon detection	**Detectare conectare la rețea**
Exclusions (IP addresses)	**Excluderi** (Adresă IP)
Exclusions (users)	**Excluderi** (Utilizatori)
Schedule settings	*(nu migrează)* Nu este posibilă configurarea unei planificări separate pentru componentă. Componenta este întotdeauna activată în timp ce Kaspersky Endpoint Security este operațional.

Logs and notifications

Task logs

Setările jurnalelor KSWS sunt migrate în secțiunea **Setări generale**, subsecțiunile **Interfață** și **Rapoarte și Spații de stocare**.

Setări Jurnale

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Event logging	**Notificări** (subsecțiunea **Interfață**)
Logs folder	*(nu migrează)* Kaspersky Endpoint Security salvează rapoartele în directorul `C:\ProgramData\Kaspersky Lab\KES.14.1\Report`.
Remove task logs older than N day(s)	*(nu migrează)* Puteți configura perioada de stocare pentru rapoartele KES în **Setări generale**, **Rapoarte și Spații de stocare**.

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Remove from the audit log events N day(s)	*(nu migrează)* Kaspersky Endpoint Security aplică limitările de stocare a rapoartelor tuturor rapoartelor, inclusiv rapoartelor de audit de sistem.
Integration with SIEM	*(nu migrează)* Poți configura integrarea SIEM în Kaspersky Security Center.

Event notifications

Setările notificărilor KSWS sunt migrate în secțiunea **Setări generale**, subsecțiunea **Interfață**.

Setări notificări

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Notifications	**Notificări**
Notify users: • **By using terminal service** • **By using Windows Messenger Service command**	*(nu migrează)* Kaspersky Endpoint Security nu acceptă modificarea textului notificării. Kaspersky Endpoint Security afișează notificări standard.
Notify administrators: • **By using Windows Messenger Service command** • **By running executable file** • **By sending email**	Doar setările de notificare prin e-mail sunt migrate la Kaspersky Endpoint Security – **Setări notificare e-mail** (blocul **Notificări**). Alte metode de notificare a administratorilor nu sunt acceptate.
Application database is out of date	**Trimite notificarea "Baze de date învechite" dacă nu s-au actualizat bazele de date**
Application database is extremely out of date	**Trimite notificarea "Baze de date extrem de învechite" dacă nu s-au actualizat bazele de date**
Critical areas scan has not been performed for a long time	*(nu migrează)* Kaspersky Endpoint Security generează un eveniment de scanare a zonelor critice ratat după trei zile.

Interaction with Administration Server

Setările de interacțiune cu Server de administrare KSWS sunt migrate în secțiunea **Setări generale**, subsecțiunea **Rapoarte și Spații de stocare**.

Setări interacțiune cu Serverul de administrare

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Quarantined files	**Fișiere carantină**
Backed up files	**Fișiere copiate de rezervă**
Blocked hosts	*(nu migrează)* Kaspersky Endpoint Security trimite automat date despre gazdele blocate.

Tasks

Activating the application

Kaspersky Endpoint Security nu acceptă activitatea *Application activation* (KSWS). Puteți crea o activitate *Adaugă cheie* (KES), adăugați o cheie de licență la pachetul de instalare sau activați distribuția automată a cheii de licență.

Copying Updates

Setările activității *Copying Updates* (KSWS) sunt migrate în activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* (KES).

Setări activitate Copiere actualizări

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Update source: • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Sursă actualizare**: • **Kaspersky Security Center** • **Servere de actualizare ale Kaspersky** • **Specificată de utilizator**
Use Kaspersky update servers if specified servers are not available	*(nu migrează)* Kaspersky Endpoint Security permite selectarea mai multor surse de actualizare, inclusiv serverele de actualizare Kaspersky. Dacă prima sursă de actualizare nu este disponibilă, Kaspersky Endpoint Security vă permite să obțineți actualizări din altă sursă din listă.
Use proxy server settings to connect to Kaspersky update servers	*(nu migrează)* Kaspersky Endpoint Security utilizează serverul proxy pentru toate componentele. Puteți configura conexiunea la serverul proxy în opțiunile de rețea ale aplicației.
Use proxy server settings to connect to other servers	*(nu migrează)* Kaspersky Endpoint Security utilizează serverul proxy pentru toate componentele. Puteți configura conexiunea la serverul proxy în opțiunile de rețea ale aplicației.
Copying updates settings: • **Copy database updates** • **Copy critical software modules updates** • **Copy database updates and critical updates of application modules**	*(nu migrează)* Kaspersky Endpoint Security copiază actualizările bazei de date și actualizările critice ale modulelor aplicației ca un singur pachet.
Folder for local storage of copied updates	**Copiază actualizările în director**

Baseline File Integrity Monitor

Setările activității *Baseline File Integrity Monitor* (KSWS) sunt migrate la activitatea *Verificare integritate sistem* și în secțiunea politicii **Security Controls**, subsecțiunea **Monitorizare integritate sistem**.

Setările activității File Integrity Monitor

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Hash calculation algorithm: • **MD5** • **SHA256**	*(nu migrează)* Kaspersky Endpoint Security utilizează algoritmul SHA256 pentru calcularea sumei de control.
Scan scope	**Domeniu monitorizare** (subsecțiunea **Monitorizare integritate sistem**)

Database Update

Setările activității *Database Update* (KSWS) sunt migrate în activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* (KES).

Setări activitate Actualizare bază de date

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Update source: • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Sursă actualizare**: • **Kaspersky Security Center** • **Servere de actualizare ale Kaspersky** • **Specificată de utilizator**

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Use Kaspersky update servers if specified servers are not available	*(nu migrează)* Kaspersky Endpoint Security permite selectarea mai multor surse de actualizare, inclusiv serverele de actualizare Kaspersky. Dacă prima sursă de actualizare nu este disponibilă, Kaspersky Endpoint Security vă permite să obțineți actualizări din altă sursă din listă.
Use proxy server settings to connect to Kaspersky update servers	*(nu migrează)* Kaspersky Endpoint Security utilizează serverul proxy pentru toate componentele. Puteți configura conexiunea la serverul proxy în opțiunile de rețea ale aplicației.
Use proxy server settings to connect to other servers	*(nu migrează)* Kaspersky Endpoint Security utilizează serverul proxy pentru toate componentele. Puteți configura conexiunea la serverul proxy în opțiunile de rețea ale aplicației.
Lower the load on the disk I/O	*(nu migrează)*

Software modules updates

Setările activității *Software Modules Update* (KSWS) sunt migrate în activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* (KES).

Setările sarcinii de actualizare a modulelor software

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Update source: • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Sursă actualizare**: • **Kaspersky Security Center** • **Servere de actualizare ale Kaspersky** • **Specificată de utilizator**
Use Kaspersky update servers if specified servers are not available	*(nu migrează)* Kaspersky Endpoint Security permite selectarea mai multor surse de actualizare, inclusiv serverele de actualizare Kaspersky. Dacă prima sursă de actualizare nu este disponibilă, Kaspersky Endpoint Security vă permite să obțineți actualizări din altă sursă din listă.
Use proxy server settings to connect to Kaspersky update servers	*(nu migrează)* Kaspersky Endpoint Security utilizează serverul proxy pentru toate componentele. Puteți configura conexiunea la serverul proxy în opțiunile de rețea ale aplicației.
Use proxy server settings to connect to other servers	*(nu migrează)* Kaspersky Endpoint Security utilizează serverul proxy pentru toate componentele. Puteți configura conexiunea la serverul proxy în opțiunile de rețea ale aplicației.
Copy and install critical software modules updates	**Instalează actualizările critice și aprobate**
Only check for critical software updates available	*(nu migrează)* Kaspersky Endpoint Security verifică continuu disponibilitatea actualizărilor critice pentru modulele aplicației.
Allow operating system restart	*(nu migrează)* Kaspersky Endpoint Security solicită utilizatorului permisiunea de a reporni computerul.
Receive information about available scheduled software modules updates	*(nu migrează)* Kaspersky Endpoint Security afișează notificări despre actualizările modulelor software.

Rollback of Application Database Update

Setările activității *Rollback of Application Database Update* (KSWS) sunt migrate în activitatea *Derulare înapoi actualizare* (KES). Noua activitate *Derulare înapoi actualizare* (KES) are un program de începere a activității - *Manually*.

On-Demand Scan

Setările activității *On-Demand Scan* (KSWS) sunt migrate în activitatea *Scanare malware* (KES).

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Scan scope	Domeniu de scanare
Protection level: • Maximum protection • Recommended • Maximum performance	Nivel de securitate: • Ridicat • Recomandat • Redus Setările nivelului de securitate sunt diferite în KSWS și 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	Tipuri de fișiere: • Toate fișierele • Fișiere scanate după format • Fișiere scanate după extensie Kaspersky Endpoint Security nu permite crearea listelor de extensii personalizate. Kaspersky Endpoint Security înlocuiește valoarea **Objects scanned by specified list of extensions** cu valoarea **Fișiere scanate după extensie**.
Subfolders	Include subdirectoarele
Subfiles	*(nu migrează)*
Scan disk boot sectors and MBR	*(nu migrează)*
Scan alternate NTFS streams	*(nu migrează)*
Scan only new and modified files	Scanează numai fișiere noi și modificate
Scan of compound objects: • All archives • All SFX archives • All email databases • All packed objects • All plain email • All embedded OLE objects	Scanare fișiere compuse: • Scanează arhive. • Scanează arhive protejate prin parolă. • Scanează pachete de distribuție. • Scanează fișiere în format de e-mail. • Scanează fișiere în formate Microsoft Office.
Action to perform on infected and other objects: • Disinfect • Disinfect. Remove if disinfection fails • Remove • Perform recommended action • Notify only	Acțiune la detectarea amenințării: • Dezinfectează; șterge dacă dezinfectarea nu reușește. • Dezinfectează; informează dacă dezinfectarea nu reușește. • Informează.
Action to perform on probably infected objects: • Quarantine • Remove • Perform recommended action • Notify only	*(nu migrează)* Kaspersky Endpoint Security aplică acțiunea dacă este detectată vreo amenințare.
Perform actions depending on the type of object detected	*(nu migrează)*
Entirely remove compound file that cannot be modified by the application in case of embedded object detection	*(nu migrează)*
Exclude files	*(nu migrează)* Kaspersky Endpoint Security aplică zona de încredere tuturor componentelor. Puteți configura excluderile în setări zonă de încredere.
Do not detect	*(nu migrează)*
Stop scanning if it takes longer than N sec	Omite fișiere scanate mai mult de N sec
Do not scan compound objects larger than N MB	Nu dezarhiva fișierele compuse mari
Use iSwift technology	Tehnologia iSwift
Use iChecker technology	Tehnologia iChecker

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
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**	*(nu migrează)* Kaspersky Endpoint Security scanează fișierele autonome în întregime.

Application Integrity Check

Setările activității *Application Integrity Control* (KSWS) sunt migrate în activitatea *Verificare integritate aplicație* (KES).

Rule Generator for Applications Launch Control

Kaspersky Endpoint Security nu acceptă activitatea *Applications Launch Control Generator*. Puteți genera reguli în setările Application Control.

Rule Generator for Device Control

Kaspersky Endpoint Security nu acceptă activitatea *Rule Generator for Device Control*. Puteți genera reguli de acces în setările Control dispozitive.

Migrarea componentelor KSWS

Înainte de instalarea locală, Kaspersky Endpoint Security verifică prezența pe computer a aplicațiilor Kaspersky. Dacă Kaspersky Security for Windows Server este instalat pe computer, KES detectează setul de componente KSWS care sunt instalate și selectează aceleași componente pentru instalare.

Componentele KES pe care KSWS nu le are sunt instalate după cum urmează:

- AMSI Protection, Host Intrusion Prevention, Remediation Engine sunt instalate cu setările implicite.
- Componentele BadUSB Attack Prevention, Control adaptiv al anomaliilor, Data Encryption, Detection and Response sunt ignorate.

Atunci când este instalată de la distanță, aplicația KES ignoră setul de componente KSWS instalate. Programul de instalare instalează componentele pe care le selectați în proprietățile pachetului de instalare. După instalarea Kaspersky Endpoint Security și migrarea politicilor și a activităților, setările KES sunt configurate în conformitate cu setările KSWS.

Migrarea activităților și politicilor KSWS

Puteți migra setările de politici și activități KSWS în următoarele moduri:

- Utilizând Expertul de conversie a loturilor de politici și activități (denumit în continuare „Expert de migrare”).

  Expertul de migrare pentru KSWS este disponibil numai în Consola de administrare (MMC). Politica și setările activităților nu pot fi migrate în Web Console și Cloud Console.

Expertul de conversie în loturi funcționează diferit pentru diferite versiuni ale Kaspersky Security Center. Vă recomandăm să efectuați un upgrade al soluției la versiunea 14.2 sau o versiune ulterioară. În această versiune a Kaspersky Security Center, expertul de conversie în bloc a politicilor și sarcinilor vă permite să migrați politicile într-un profil, mai degrabă decât într-o politică. În această versiune a Kaspersky Security Center, expertul de conversie în loc a politicilor și sarcinilor vă permite, de asemenea, să migrați o gamă mai largă de setări de politici.

- Utilizarea Expertului pentru politici noi pentru Kaspersky Endpoint Security for Windows.

  Expertul pentru politici noi vă permite să creați o politică KES pe baza unei politici KSWS.

Procedurile de migrare a politicii KSWS sunt diferite atunci când se utilizează Expertul de migrare și Expertul de politică nouă.

Asistentul de conversie în bloc a politicilor și activităților

Expertul de migrare transferă setările politicii KSWS în profilul de politică în loc de setările politicii KES. *Profilul de politici* este un set de setări de politici care este activat pe un computer dacă acesta îndeplinește regulile de activare configurate. Eticheta dispozitivului `UpgradedFromKSWS` este selectată ca și criteriu de declanșare a profilului de politică. Kaspersky Security Center adaugă automat eticheta `UpgradedFromKSWS` la toate computerele pe care instalați KES peste KSWS prin intermediul activității de instalare la distanță. Dacă ați ales o altă metodă de instalare, puteți atribui manual eticheta dispozitivelor.

Pentru a adăuga o etichetă pe un dispozitiv:

1. Creați o nouă etichetă pentru servere — `UpgradedFromKSWS`.

   Pentru mai multe detalii despre crearea etichetelor pentru dispozitive, consultați Ajutor pentru Kaspersky Security Center.

2. Creați un nou grup de administrare în consola Kaspersky Security Center și adăugați serverele cărora doriți să le atribuiți eticheta în acest grup.

   Puteți grupa serverele cu ajutorul instrumentului de selecție. Pentru mai multe detalii despre lucrul cu selecțiile, consultați Ajutor pentru Kaspersky Security Center.

3. Selectați toate serverele din grupul de administrare în consola Kaspersky Security Center, deschideți proprietățile serverelor selectate și atribuiți eticheta.

Dacă migrați mai multe politici KSWS, fiecare politică este convertită într-un profil în cadrul unei politici generale. În cazul în care politica KSWS conține deja profiluri, aceste profiluri sunt, de asemenea, migrate ca profiluri. Ca urmare, veți obține o singură politică care include profiluri corespunzătoare tuturor politicilor KSWS.

Cum să utilizați Expertul de conversie în bloc a politicilor și activităților pentru a migra setările politicilor KSWS

1. În Consola de administrare, selectați Server de administrare și faceți clic dreapta pentru a deschide meniul contextual.

2. Selectați **All tasks** → **Policies and tasks batch conversion wizard**.

Expertul de conversie în loturi a politicilor și activităților va începe. Urmează instrucțiunile din expert.

Pasul 1. Selectarea aplicației pentru care doriți să convertiți politicile și activităților

La acest pas, trebuie să selectați Kaspersky Endpoint Security for Windows. Mergeți la pasul următor.

Pasul 2. Conversia politicilor

Expertul de migrare creează profiluri de politici KSWS în cadrul unei politici KES. Selectați politicile Kaspersky Security for Windows Server pe care doriți să le convertiți în profiluri de politici. Mergeți la pasul următor.

Expertul de migrare va începe apoi să efectueze conversia politicilor. Numele noilor profiluri de politici vor corespunde politicilor originale KSWS.

Pasul 3. Raport privind migrarea politicilor

Expertul de migrare creează un raport de migrare a politicilor. Raportul de migrare a politicilor conține data și ora la care politicile au fost convertite, numele politicii originale KSWS, numele politicii KES țintă și numele noului profil de politici.

Pasul 4. Conversia activităților

Expertul pentru migrare creează noi activități pentru Kaspersky Endpoint Security for Windows. În lista de activități, selectați activitățile KSWS pe care doriți să le creați pentru Kaspersky Endpoint Security. Noile activități vor fi denumite *<KSWS nume activitate> (convertită)*. Mergeți la pasul următor.

Pasul 5. Finalizarea expertului

Ieșiți din Expert. Ca rezultat, expertul efectuează următoarele acțiuni:

- Se adaugă noi profiluri de politici la politica Kaspersky Endpoint Security.

  Politica include profiluri cu setările Kaspersky Security for Windows Server. Noua politică are starea *Active*. Expertul lasă politicile KSWS neschimbate.

- Creează noi activități de Kaspersky Endpoint Security.

  Noile activități sunt copii ale activităților KSWS. Expertul lasă activitățile KSWS neschimbate.

Noul profil de politici cu setări KSWS va fi numit *UpgradedFromKSWS <Numele politicii Kaspersky Security for Windows Server>*. În proprietățile profilului, asistentul de migrare selectează automat eticheta dispozitivului `UpgradedFromKSWS` ca și criteriu de declanșare. Astfel, setările din profilul de politică sunt aplicate automat serverelor.

Expertul pentru crearea unei politici bazate pe o politică KSWS

Atunci când o politică KES este creată pe baza unei politici KSWS, expertul transferă setările în noua politică în mod corespunzător. Altfel spus, o politică KES va corespunde unei politici KSWS. Expertul nu convertește politica într-un profil.

Cum să utilizați Expertul pentru politici noi pentru a migra setările politicii KSWS

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Managed devices** al arborelui consolei de administrare, selectați directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectează fila **Policies**.
4. Fă clic pe **New policy**.

   Expertul de politică pornește.
5. Urmează instrucțiunile din Expertul de politică.

Pasul 1. Selectarea aplicației pentru crearea politicii de grup

Selectează aplicația **Kaspersky Endpoint Security for Windows (14.1)**.

Pasul 2. Denumirea politicii de grup

Introdu un nume pentru politica de grup, de exemplu, *Politica pentru birou*.

Bifați caseta de selectare **Use policy settings for an earlier version of the application**. Faceți clic pe **Browse** și selectați o politică KSWS.

Pasul 3. Participarea la Kaspersky Security Network

Citește și acceptă condițiile din Declarația de Securitate a Rețelei Kaspersky (KSN).

Pasul 4. Selectarea modului de utilizare a aplicației pe computere

Selectați **Modul standard pentru a proteja gazdelor**. Kaspersky Endpoint Security oferă o politică comună pentru toate modurile aplicației și toate tipurile de sisteme de operare.

Îți recomandăm să utilizezi politici diferite pentru diferite moduri și tipuri de sisteme de operare.

Pasul 5. Importarea setărilor

Acest pas este disponibil dacă selectați configurarea manuală a politicii la pasul 4.

Puteți crea o politică pe baza setărilor Kaspersky Endpoint Security dintr-un fișier de configurare CFG. Atunci când se importă un fișier de configurare a aplicației, nu toate setările politicii sunt disponibile pentru expert. De exemplu, profilurile politicii lipsesc din setările aplicației. Dacă doriți să transferați toate setările și profilurile în politică, puteți importa o altă politică dintr-un fișier KLP.

La importarea unui fișier de configurare, Kaspersky Endpoint Security nu transferă parolele pentru containerele crypto. Dacă utilizați autentificarea mutuală atunci când vă conectați la servere, trebuie să specificați de la zero parolele pentru containerele crypto.

Pasul 6 - 10. Configurarea setărilor politicii

Acest pas este disponibil dacă selectați configurarea manuală a politicii la pasul 4.

Urmați pașii pentru a gestiona setările politicii.

Pasul 11. Configurarea zonei de încredere

Configurează zona de încredere. Poți adăuga excluderi de la scanare predefinite și aplicații de încredere. Excluderile de la scanare și aplicațiile de încredere predefinite ajută la configurarea rapidă a Kaspersky Endpoint Security pe serverele SQL, serverele Microsoft Exchange și System Center Configuration Manager. Aceasta înseamnă că nu trebuie să configurați manual o zonă de încredere pentru aplicație pe servere. Excluderile de la scanare predefinite și aplicațiile de încredere te pot ajuta, de asemenea, să configurezi rapid Kaspersky Endpoint Security în modul Light Agent în mediile virtuale Citrix și VMware.

Pasul 12. Selectarea stării politicii

- **Active**. După următoarea sincronizare, politica va fi folosită drept politica activă pe computer.

  Setările unei politici active se salvează pe computerele client în timpul sincronizării. Nu poți aplica simultan mai multe politici pe un singur computer; prin urmare, poate fi activă numai o singură politică în fiecare grup.

- **Inactive**. Faceți o copie de rezervă a politicii. Dacă este necesar, o politică inactivă poate fi comutată la starea Activă.

  Poți crea un număr nelimitat de politici inactive. O politică inactivă nu afectează setările aplicației pe computerele din rețea. Politicile inactive sunt concepute ca pregătiri pentru situații de urgență, cum ar fi un atac de virus. Dacă există un atac prin intermediul unităților flash, poți activa o politică care blochează accesul la unitățile flash. În acest caz, politica activă devine automat inactivă.

- **Out-of-office**. Politica este activată atunci când un computer părăsește perimetrul rețelei organizației.

Ieșiți din Expert.

Configurarea suplimentară a politicilor și activităților după migrare

KSWS și KES au seturi diferite de componente și setări de politici, astfel încât, după migrare, trebuie să verificați dacă setările de politici îndeplinesc cerințele de securitate ale companiei dumneavoastră.

Verificați următoarele setări de bază ale politicii:

- Protecția prin parolă. Setările de protecție prin parolă KSWS nu sunt migrate. Kaspersky Endpoint Security are o funcție încorporată de Protecție prin parolă. Dacă este necesar, activați Protecția prin parolă și setați o parolă.

- Zonă de încredere. Metodele folosite de KSWS și KES pentru selectarea obiectelor diferă. În timpul migrării, KES acceptă excluderile definite ca fișiere individuale sau căi către fișier/director. Dacă KSWS are excluderi configurate ca zonă predefinită sau un URL de script, aceste excluderi nu sunt migrate. După migrare, trebuie să adăugați manual astfel de excluderi.

  > Pentru a vă asigura că Kaspersky Endpoint Security funcționează corect pe servere, se recomandă să adăugați fișierele importante pentru funcționarea serverului în zona de încredere. Pentru serverele SQL, trebuie să adăugați fișiere de baze de date MDF și LDF. Pentru serverele Microsoft Exchange, trebuie să adăugați fișiere CHK, EDB, JRS, LOG și JSL. Puteți utiliza măști, de exemplu, `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

  > Începând cu Kaspersky Endpoint Security 12.6 for Windows, excluderile de scanare și aplicații de încredere sunt adăugate la zona de încredere. Excluderile de la scanare și aplicațiile de încredere predefinite ajută la configurarea rapidă a Kaspersky Endpoint Security pe serverele SQL, serverele Microsoft Exchange și System Center Configuration Manager. Aceasta înseamnă că nu trebuie să configurați manual o zonă de încredere pentru aplicație pe servere.

- Firewall. Funcțiile KSWS Firewall sunt realizate de Firewall-ul la nivel de sistem. În KES, o componentă separată este responsabilă pentru funcționalitatea Firewall. După migrare, puteți configura Kaspersky Endpoint Security Firewall.

- Kaspersky Security Network. Kaspersky Endpoint Security nu acceptă configurarea KSN pentru componente individuale. Kaspersky Endpoint Security utilizează KSN pentru toate componentele aplicației. Pentru a utiliza KSN, trebuie să acceptați noile termene și condiții din Declarația Kaspersky Security Network.

- Control Web. Regulile de blocare pentru controlul categoriei trafic web sunt migrate într-o singură regulă de blocare în Kaspersky Endpoint Security. Kaspersky Endpoint Security ignoră regulile de permitere pentru controlul categoriilor. Kaspersky Endpoint Security nu acceptă toate categoriile componentei Kaspersky Security for Windows Server. Categoriile care nu există în Kaspersky Endpoint Security nu sunt migrate. Prin urmare, regulile de clasificare a resurselor web cu categorii neacceptate nu sunt migrate. Dacă este necesar, adaugă reguli de Control Web.

- Server proxy. Parola de conexiune a serverului proxy nu este migrată. Introduceți parola care va fi utilizată pentru conectarea manuală la serverul proxy.

- Programele componentelor individuale. Kaspersky Endpoint Security nu acceptă configurarea programelor pentru componente individuale. Componentele sunt întotdeauna activată în timp ce Kaspersky Endpoint Security este operațional.

- Set de componente. Setul de caracteristici disponibile ale aplicației Kaspersky Endpoint Security depinde de tipul sistemului de operare: stație de lucru sau server. De exemplu, dintre instrumentele de criptare, doar BitLocker Drive Encryption este disponibil pe servere.

- Atribut . Starea atributului nu este migrată. Atributul va avea valoarea implicită. În mod implicit, aproape toate setările din noua politică au o interdicție de modificare a setărilor din politicile copilului și din interfața aplicației locale. Atributul are valoarea pentru setările politicii în secțiunea **Managed Detection and Response (Industrial CyberSecurity)** și în grupul de setări **Asistență utilizator** (secțiunea **Interfață**). Dacă este necesar, configurați moștenirea setărilor din politica principală.

- Cum se lucrează cu amenințările active. Tehnologia Dezinfectare avansată funcționează diferit în cazul serverelor și stațiilor de lucru. Puteți configura tehnologia Dezinfectare avansată în setările activității *Scanare malware* și în setările aplicației.

- Efectuarea upgrade-ului aplicației. Pentru a instala actualizări majore și patch-uri fără a reporni, trebuie să modificați modul de actualizare a aplicației. În mod implicit, funcția Instalează actualizările aplicației fără repornire este dezactivată.

- Kaspersky Endpoint Agent. Kaspersky Endpoint Security are un agent încorporat pentru lucrul cu soluțiile Detection and Response. Dacă este necesar, transferați setările politicii Kaspersky Endpoint Agent în politica Kaspersky Endpoint Security.

- Activități *Actualizarea modulelor bazelor de date și ale aplicațiilor*. Asigurați-vă că setările din activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* au fost migrate corect. În locul celor trei sarcini ale KSWS, KES utilizează o singură sarcină KES. Puteți optimiza sarcinile *Actualizarea modulelor bazelor de date și ale aplicațiilor* și elimina activitățile inutile.

- Alte activități. Componentele Application Control, Control dispozitive și File Integrity Monitor funcționează diferit în KSWS și KES. KES nu utilizează activitățile *Baseline File Integrity Monitor*, *Applications Launch Control Generator*, *Rule Generator for Device Control*. Prin urmare, aceste sarcini nu sunt migrate. După migrare, puteți configura componentele File Integrity Monitor, Application Control, Control dispozitive.

Migrarea zonei de încredere KSWS

O *zonă de încredere* este o listă de obiecte și aplicații configurate de administratorul de sistem, pe care Kaspersky Endpoint Security nu le monitorizează când este activ. Poți migra obiectele zonei de încredere de la KSWS la KES utilizând *Asistentul de conversie în bloc a politicilor și activităților* sau *expertul pentru crearea unei noi politici KES pe baza politicii KSWS*. KSWS și KES au seturi diferite de componente și caracteristici, astfel încât, după migrare, trebuie să verifici dacă excluderile îndeplinesc cerințele de securitate ale companiei tale. Metodele de adăugare a excluderilor în zona de încredere sunt, de asemenea, diferite pentru KES și KSWS. Expertul de migrare nu dispune de instrumente pentru a migra toate excluderile KSWS. Acest lucru înseamnă că, după migrare, trebuie să adaugi manual unele dintre excluderile KSWS.

Pentru a vă asigura că Kaspersky Endpoint Security funcționează corect pe servere, se recomandă să adăugați fișierele importante pentru funcționarea serverului în zona de încredere. Pentru serverele SQL, trebuie să adăugați fișiere de baze de date MDF și LDF. Pentru serverele Microsoft Exchange, trebuie să adăugați fișiere CHK, EDB, JRS, LOG și JSL. Puteți utiliza măști, de exemplu, `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

Începând cu Kaspersky Endpoint Security 12.6 for Windows, excluderile de scanare și aplicații de încredere sunt adăugate la zona de încredere. Excluderile de la scanare și aplicațiile de încredere predefinite ajută la configurarea rapidă a Kaspersky Endpoint Security pe serverele SQL, serverele Microsoft Exchange și System Center Configuration Manager. Aceasta înseamnă că nu trebuie să configurați manual o zonă de încredere pentru aplicație pe servere.

Metode de creare a zonelor de încredere KES și KSWS.

KSWS		KES
Object to scan		
• Predefined scope	*(nu migrează)*	
• Disk, folder or network location	→	**Fișier sau director**
• File	→	**Fișier sau director**
• Script file or web address	*(nu migrează)*	
Detected object	→	**Tipul obiectului detectat**
Trusted processes	→	**Aplicații de încredere**

Migrarea obiectelor scanate

Excluderile KSWS care au metoda **Object to scan** selectată în proprietățile lor sunt migrate la excluderile KES care au metoda **Fișier sau director** selectată în proprietățile lor, cu unele limitări. Migrarea unei excluderi depinde de metoda de selectare a obiectului:

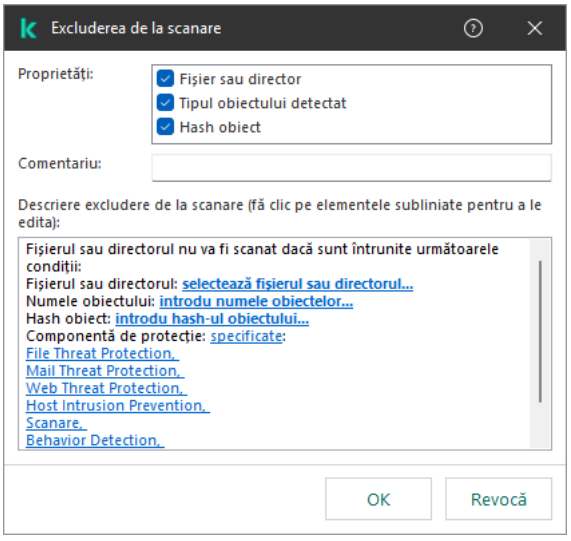
- Predefined scope – *nu migrează*.

  După migrare, trebuie să adăugați manual astfel de excluderi. Excluderile ca zone predefinite trebuie să fie configurate în setările activității *Scanare malware*.

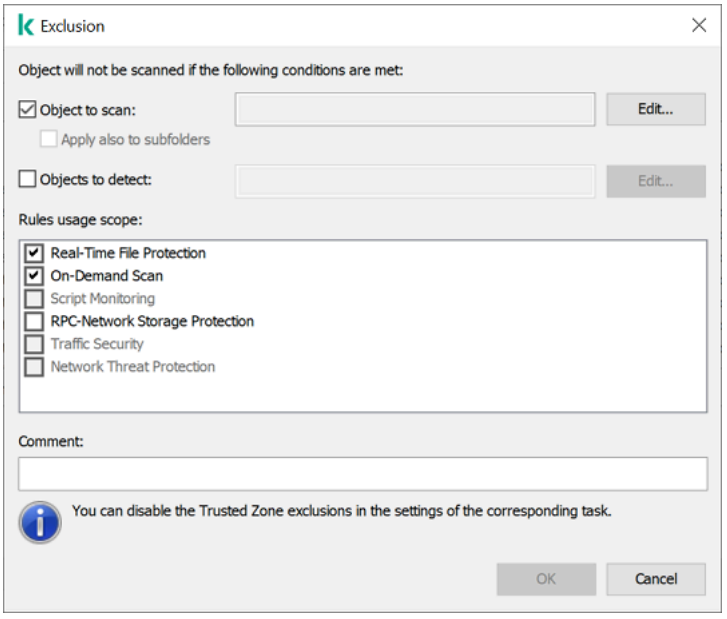
- Disk, folder or network location – migrează la excluderile KES care au metoda „Fișier sau director” selectată în proprietăți.
- File – migrează la excluderile KES care au metoda „Fișier sau director” selectată în proprietăți.
- Script file or web address – *nu migrează*.

  După migrare, trebuie să adăugați manual astfel de excluderi. Excluderile ca adrese web de script trebuie adăugate la adresele web de încredere pentru componenta Web Threat Protection.

Dacă este bifată caseta de selectare **Apply also to subfolders** pentru obiectul scanat, această setare este migrată la excluderile KES (caseta de selectare **Include subdirectoarele**).



Setări excluderi KES



Setări excluderi KSWS

Migrarea obiectelor detectate

Excluderile KSWS care au metoda **Detected object** selectată în proprietățile lor sunt migrate la excluderile KES care au metoda **Tipul obiectului detectat** selectată în proprietățile lor. Numele obiectului detectat corespunde clasificării din Enciclopedia Kaspersky (de exemplu, `Email-Worm`, `Rootkit` sau `RemoteAdmin`). Kaspersky Endpoint Security acceptă măști cu semnul întrebării `?` (se potrivește cu orice caracter) și asterisc `*` (se potrivește cu orice succesiune de caractere).

Migrarea domeniului de utilizare a excluderii

Domeniul de utilizare al unei excluderi este un set de componente cărora li se aplică excluderea. KES și KSWS au seturi diferite de componente, astfel că Expertul de migrare nu poate migra domeniul de utilizare a excluderii. Prin urmare, dacă cel puțin o componentă este selectată în domeniul de utilizare KSWS, KES aplică excluderea tuturor componentelor aplicației.

Poți configura domeniul de utilizare KSWS în setările zonei de încredere și, de asemenea, în setările componentelor de protecție KSWS. Pentru aceasta, poți bifa sau debifa caseta de selectare **Apply Trusted Zone** din secțiunea corespunzătoare a politicii. Setările componentelor de protecție KES nu includ o astfel de casetă de selectare. Acest lucru înseamnă că starea zonei de încredere din setările componentelor individuale se pierde în timpul migrării. După finalizarea migrării, selectează componentele cărora li se aplică excluderea în setările zonei de încredere din politica KES.

Migrarea comentariilor

Comentariile din zona de încredere KSWS sunt migrate în comentariile excluderii KES fără modificări.

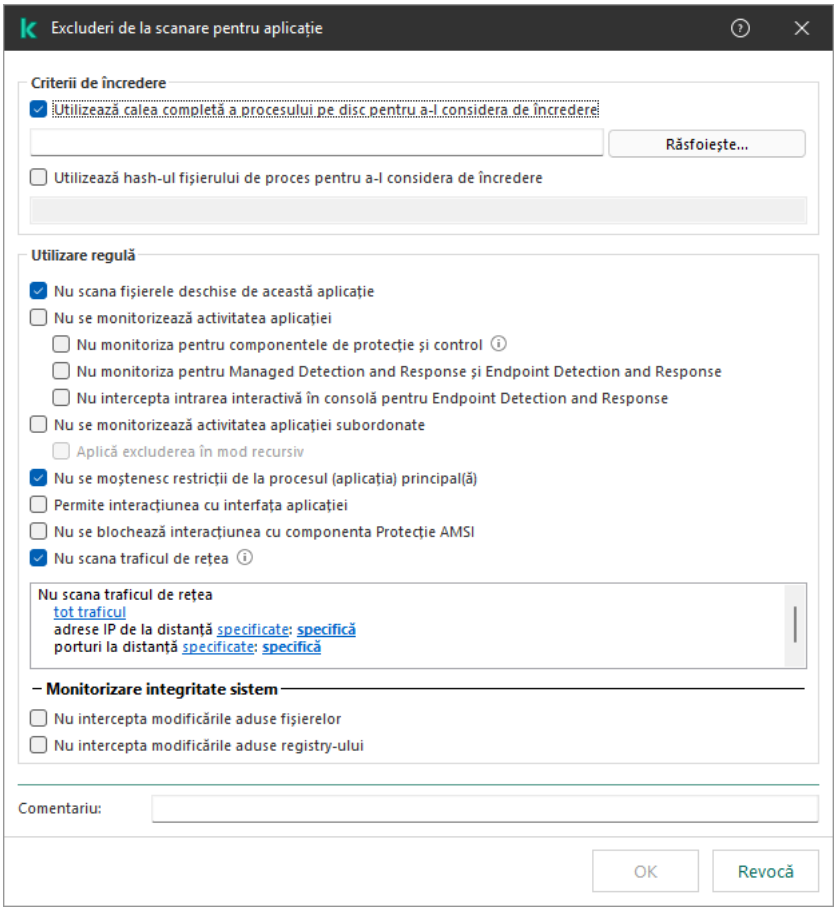
Migrarea proceselor de încredere

Procesele de încredere KSWS sunt migrate în procese de încredere KES cu anumite limitări. Migrarea proceselor de încredere depinde de metoda de selectare a obiectelor:

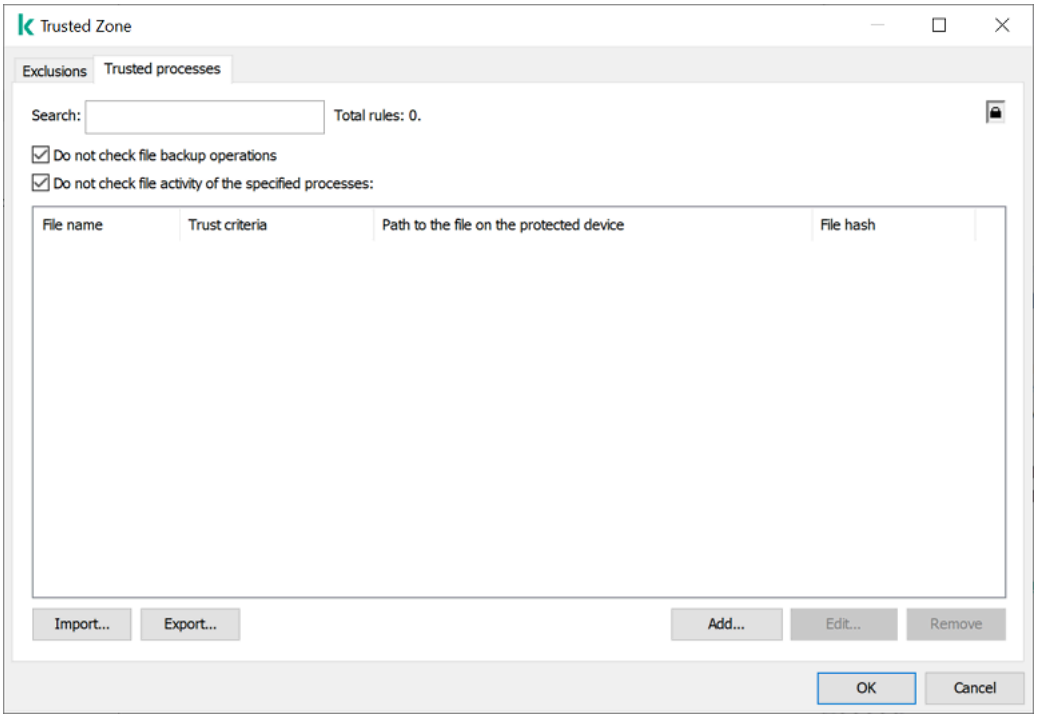
- Path to the file on the protected device – migrează la aplicațiile de încredere KES.
- File hash – *nu migrează*.

Dacă KSWS are procese de încredere configurate ca un hash fișier, astfel de procese de încredere nu sunt migrate. După migrare, trebuie să adăugați manual aceste procese de încredere.

Dacă este bifată caseta de selectare **Do not check file backup operations** în setările proceselor de încredere, această setare este migrată în aplicațiile de încredere KES (caseta de selectare **Nu monitoriza activitatea aplicației**).



Setările aplicației de încredere KES



Setările procesului de încredere KSWS

Migrarea regulilor Control lansare aplicații KSWS

Componenta Control lansare aplicații KSWS este blocată implicit. Adică, componenta Control lansare aplicații blochează automat toate aplicațiile care nu sunt specificate în reguli ca aplicații permise. Prin urmare, expertul de migrare pentru componenta Application Control a KES setează automat modul de control **Listă permise** care corespunde principiului blochează în mod implicit.

Poți migra reguli de la KSWS la KES utilizând *Asistentul de conversie în bloc a politicilor și activităților* sau *expertul pentru crearea unei noi politici KES pe baza politicii KSWS*.

Migrarea modului pentru Control lansare aplicații

Modul Control lansare aplicații KSWS migrează la Control lansare aplicații KES după cum urmează:

- **Statistics only** → **Testează regulile**;
- **Active** → **Aplica reguli**.

Migrarea regulilor predefinite Control lansare aplicații KSWS

În mod implicit, Control lansare aplicații KSWS include două reguli:

- **Allow scripts and MSI by OS-trusted certificate**
- **Allow executable by OS-trusted certificate**

Regulile predefinite permit executarea *scripturilor*, a *pachetelor MSI* și a *fișierelor executabile* semnate cu un certificat rădăcină de încredere. Dacă cel puțin o regulă KSWS predefinită are tipul **Allow**, expertul de migrare creează o nouă regulă de permitere, **Applications with trusted root certificates**. Adică, KES Application Control folosește o singură regulă pentru a permite executarea scripturilor de încredere, a pachetelor MSI și a fișierelor executabile.

Dacă ambele reguli predefinite KSWS sunt de tipul **Deny**, KES ignoră regulile predefinite.

Migrarea regulilor personalizate Control lansare aplicații KSWS

Regulile Control lansare aplicații KSWS reglementează execuția fișierelor în conformitate cu următoarele criterii:

- semnătură cu certificat digital;
- hash SHA256;
- cale fișier.

Regulile sunt create diferit în KSWS și KES, prin urmare expertul de migrare creează *categorii de aplicații* care includ condiții și excluderi din regulile KSWS și adaugă aceste categorii de aplicații la regulile KES. Expertul folosește condițiile **Certificat**, **Cale către director** și **Hash fișier** în categoriile de aplicații. Noile categorii de aplicații sunt disponibile în Consola de administrare a Kaspersky Security Center din secțiunea **Application management** → **Application categories**.

Expertul de migrare grupează regulile KSWS după tip și după utilizator. Apoi, expertul creează categorii de aplicații care includ condiții și excluderi de la regulile KSWS și adaugă categoriile de aplicații la noile reguli KES. Expertul specifică numele regulilor KSWS în câmpul **Descriere** al regulilor KES.

Migrarea setărilor avansate Control lansare aplicații KSWS

Principiul de funcționare al componentelor Control lansare aplicații KSWS și Control lansare aplicații KES este diferit, astfel încât expertul de migrare poate migra un subset de setări.

Setările componentei Control lansare aplicații

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Repeat action taken for the first file launch on all the subsequent launches for this file	*(nu migrează)* Kaspersky Endpoint Security scanează aplicația de fiecare dată când încearcă să se execute.
Deny the command interpreters launch with no command to execute	*(nu migrează)* Kaspersky Endpoint Security permite executarea interpreților comenzii dacă nu sunt interzișii de Application Control.
Apply rules to executable files	*(nu migrează)* Domeniul de aplicare al regulilor nu poate fi configurat în setările KES Application Control. KES Application Control aplică reguli tuturor tipurilor de fișiere: fișiere executabile, scripturi și pachete MSI. Dacă toate tipurile de fișiere sunt incluse în domeniul de aplicare al regulilor în KSWS, în timpul migrării, KES transferă regulile KSWS. Dacă un anumit tip de fișier este exclus din domeniul de aplicare al regulilor în KSWS, în timpul migrării, KES transferă și regulile KSWS, dar **Testează regulile** este selectată ca acțiune Application Control.
Monitor loading of DLL modules	**Monitorizați încărcarea modulelor DLL (crește semnificativ sarcina asupra sistemului)**
Apply rules to scripts and MSI packages	*(nu migrează)* Domeniul de aplicare al regulilor nu poate fi configurat în setările KES Application Control. KES Application Control aplică reguli tuturor tipurilor de fișiere: fișiere executabile, scripturi și pachete MSI. Dacă toate tipurile de fișiere sunt incluse în domeniul de aplicare al regulilor în KSWS, în timpul migrării, KES transferă regulile KSWS. Dacă un anumit tip de fișier este exclus din domeniul de aplicare al regulilor în KSWS, în timpul migrării, KES transferă regulile KSWS, dar **Testează regulile** este selectată ca acțiune Application Control.
Deny applications untrusted by KSN	*(nu migrează)* Kaspersky Endpoint Security nu ține cont de reputația aplicațiilor și permite sau refuză executarea aplicațiilor în conformitate cu regulile.
Allow applications trusted by KSN	În timpul migrării, KES adaugă o nouă regulă de permitere. Categoria KL **Alt software\Aplicații, considerate de încredere în funcție de reputația din KSN** este specificată ca fiind condiția de declanșare a regulii.
Users and / or user groups allowed to run applications trusted by KSN	**Utilizatori și drepturile lor** într-o regulă de permitere Application Control care include categoria KL **Alt software\Aplicații, considerate de încredere în funcție de reputația din KSN**.
Automatically allow software distribution via applications and packages listed	Software Distribution Control în KSWS și KES funcționează diferit. În timpul migrării, KES adaugă noi reguli de permitere pentru aplicațiile care au permisă distribuirea automată a software-ului. Hash-ul fișierului este specificat drept condiție de declanșare a regulii.
Always allow software distribution via Windows Installer	Software Distribution Control în KSWS și KES funcționează diferit. În timpul migrării, KES adaugă noi reguli de permitere pentru aplicațiile care au permisă distribuirea automată a software-ului (**Software distribution applications and packages allowed**). Hash-ul fișierului este specificat drept condiție de declanșare a regulii. În proprietățile contului, este bifată caseta de selectare **Programe de actualizare de încredere**.

Setări Kaspersky Security for Windows Server	Setări Kaspersky Endpoint Security for Windows
Always allow software distribution via SCCM using the Background Intelligent Transfer Service	*(nu migrează)*
Software distribution applications and packages allowed	Software Distribution Control în KSWS și KES funcționează diferit. În timpul migrării, KES adaugă noi reguli de permitere pentru aplicațiile care au permisă distribuirea automată a software-ului. Hash-ul fișierului este specificat drept condiție de declanșare a regulii. În proprietățile contului, este bifată caseta de selectare **Programe de actualizare de încredere**.
Schedule settings	*(nu migrează)* Dacă o programare este configurată pentru componentă în setările KSWS, componenta Application Control este activată după migrare. Dacă o programare nu este configurată pentru componentă în setările KSWS, componenta Application Control este dezactivată după migrare. Nu este posibilă configurarea unei planificări separate pentru componentă. Componenta este întotdeauna activată în timp ce Kaspersky Endpoint Security este operațional.

Instalarea KES în loc de KSWS

Puteți instala Kaspersky Endpoint Security în următoarele moduri:

- Instalarea KES după îndepărtarea KSWS (recomandat).
- Instalarea KES peste KSWS.

Eliminarea Kaspersky Security for Windows Server

Puteți elimina aplicația la distanță folosind activitatea *Uninstall application remotely* sau local, pe server. Poate fi necesar să reporniți serverul după eliminarea KSWS. Dacă doriți să instalați Kaspersky Endpoint Security fără o repornire, asigurați-vă că Kaspersky Security for Windows Server este complet eliminat. În cazul în care aplicația nu este complet eliminată, instalarea Kaspersky Endpoint Security poate cauza funcționarea defectuoasă a serverului. De asemenea, se recomandă să vă asigurați că aplicația este complet eliminată dacă ați folosit utilitarul kavremover. Utilitarul kavremover nu acceptă gestionarea KSWS.

Dacă Protecție cu parolă este activată pentru a restricționa accesul la KSWS, introduceți parola pentru dezinstalare în setările pachetului de instalare KES.

După ce ați eliminat KSWS, instalați Kaspersky Endpoint Security for Windows utilizând orice metodă disponibilă.

Instalarea Kaspersky Endpoint Security

Când instalați KES de la distanță, componentele pe care le-ați selectat în proprietățile pachetului de instalare sunt instalate pe server. Vă recomandăm să selectați componentele implicite în proprietățile pachetului de instalare. O repornire nu este necesară când instalați KES peste KSWS.

Înainte de instalarea locală, Kaspersky Endpoint Security verifică prezența pe computer a aplicațiilor Kaspersky. Dacă Kaspersky Security for Windows Server este instalat pe computer, KES detectează setul de componente KSWS care sunt instalate și selectează aceleași componente pentru instalare. O repornire nu este necesară când instalați KES peste KSWS.

Dacă instalarea KES peste KSWS nu a reușit, puteți anula instalarea. După anularea instalării, se recomandă să reporniți serverul și să încercați din nou.

Setările și activitățile KSWS nu sunt migrate când este instalat Kaspersky Endpoint Security for Windows. Pentru a migra setările și activitățile, executați Expertul de conversie în bloc a politicilor și activităților.

Puteți verifica lista componentelor instalate în secțiunea **Securitate** a interfeței aplicației, utilizând comanda `status` sau în consola Kaspersky Security Center din proprietățile computerului. Puteți modifica setul de componente după instalare utilizând opțiunea *Modificare componente ale aplicației*.

Migrarea configurării [KES+KEA] la [KES+agent încorporat]

Pentru a sprijini utilizarea Kaspersky Endpoint Security for Windows ca parte a EDR (KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox, KUMA și MDR, la aplicație a fost adăugat un agent încorporat. Nu mai aveți nevoie de aplicația Kaspersky Endpoint Agent pentru a utiliza aceste soluții.

La migrarea de la KSWS la KES, soluțiile EDR (KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox și MDR continuă să funcționeze cu agenții încorporați Kaspersky Endpoint Security. În plus, Kaspersky Endpoint Agent va fi eliminat din computer.

Migrarea configurației [KSWS+KEA] la [KES+agent încorporat] implică pașii următori:

1. **Migrarea de la KSWS la KES**

   Migrarea de la KSWS la KES implică instalarea Kaspersky Endpoint Security în locul Kaspersky Security for Windows Server.

   De obicei, administratorii activează component Protecție prin parolă pentru a restricționa accesul la KSWS și KEA. Începând cu Kaspersky Security Center Linux 15.1, puteți introduce parola de dezinstalare a aplicației în setările sarcinii *Install application remotely*. Sarcina permite introducerea unei singure parole de dezinstalare. Adică, dacă aceeași parolă este setată pentru KSWS și KEA, aplicațiile KSWS și KEA sunt eliminate cu succes. Dacă parolele sunt diferite, eliminarea uneia dintre aplicații eșuează și este afișată o eroare de acces. Pentru a finaliza migrarea, trebuie să dezactivați Protecția prin parolă pentru aplicația a cărei parolă nu ați putut-o introduce în setările sarcinii *Install application remotely*.

   Pentru a efectua migrarea, trebuie să selectați componentele necesare pentru a accepta soluțiile Detection and Response ca parte a Kaspersky Endpoint Security. După instalarea aplicației, Kaspersky Endpoint Security trece la utilizarea agentului încorporat și elimină Kaspersky Endpoint Agent.

2. **Migrarea politicii și a activităților**

Migrarea politicilor și activităților [KSWS+KEA] la [KES+agent încorporat] implică pașii următori:

1. Migrarea politicilor și activităților de la KSWS la KES utilizând Expertul de conversie în loturi a politicilor și activităților (disponibil numai în Consola de administrare (MMC)).

   Ca urmare, un profil de politică cu numele *UpgradedFromKSWS <Numele politicii Kaspersky Security for Windows Server>* este adăugat la politica KES. Sunt create și noi activități KES cu numele *<nume activitate KSWS> (convertit)*.

2. Migrarea politicilor și activităților de la KEA la KES folosind expertul pentru migrarea de la Kaspersky Endpoint Agent (disponibil numai în Web Console și Cloud Console).

   Ca rezultat, este creată o nouă politică cu numele *<Numele politicii Kaspersky Endpoint Security> &<Numele politicii Kaspersky Endpoint Agent>*. Sunt create, de asemenea, activități noi și activități KES.

3 Funcționalitatea de licențiere

Dacă folosiți o licență obișnuită Kaspersky Endpoint Detection and Response Optimum sau Kaspersky Optimum Security pentru a activa Kaspersky Endpoint Security for Windows și Kaspersky Endpoint Agent, funcționalitatea EDR Optimum va fi activată automat după efectuarea upgrade-ului aplicației la versiunea 11.7.0. Nu trebuie să faceți nimic.

Dacă folosiți o licență independentă Kaspersky Endpoint Detection and Response Optimum Add-on pentru a activa funcționalitatea EDR Optimum, trebuie să vă asigurați că cheia EDR Optimum Add-on este adăugată la depozitul Kaspersky Security Center și că funcționalitatea de distribuire automată a cheii licenței este activată. După efectuarea upgrade-ului aplicației la versiunea 11.7.0, funcționalitatea EDR Optimum este activată automat.

Dacă folosiți o licență Kaspersky Endpoint Detection and Response Optimum sau Kaspersky Optimum Security pentru a activa Kaspersky Endpoint Agent și o licență diferită pentru a activa Kaspersky Endpoint Security for Windows, trebuie să înlocuiți cheia pentru Kaspersky Endpoint Security for Windows cu o cheie Kaspersky Endpoint Detection and Response Optimum sau Kaspersky Optimum Security. Puteți înlocui cheia utilizând activitatea *Add key*.

Nu trebuie să activați funcționalitatea Kaspersky Sandbox. Funcționalitatea Kaspersky Sandbox va fi disponibilă imediat după efectuarea upgrade-ului și activarea Kaspersky Endpoint Security for Windows.

Numai licența Kaspersky Anti Targeted Attack Platform poate fi utilizată pentru a activa Kaspersky Endpoint Security ca parte a soluției Kaspersky Anti Targeted Attack Platform. După efectuarea upgrade-ului aplicației la versiunea 12.1, funcționalitatea EDR (KATA) este activată automat. Nu trebuie să faceți nimic.

4 Verificarea stării componentelor Kaspersky Endpoint Detection and Response Optimum și Kaspersky Sandbox

Dacă după upgrade componenta are starea *Critical* în consola Kaspersky Security Center:

- asigurați-vă că Agentul de rețea versiunea 13.2 sau o versiune ulterioară este instalată pe computer.
- Verificați starea de funcționare a agentului încorporat, vizualizând *Report on status of application components*. Dacă o componentă are starea *Not installed*, instalați componenta, utilizând activitatea *Change application components*.
- Asigurați-vă că acceptați Declarația Kaspersky Security Network în noua politică a Kaspersky Endpoint Security for Windows.

Asigurați-vă că funcționalitatea EDR Optimum este activată utilizând *Report on status of application components*. Dacă o componentă are starea *Nu este acoperită de licență*, asigurați-vă că funcționalitatea de distribuire automată a cheii de licență a componentei EDR Optimum este activată.

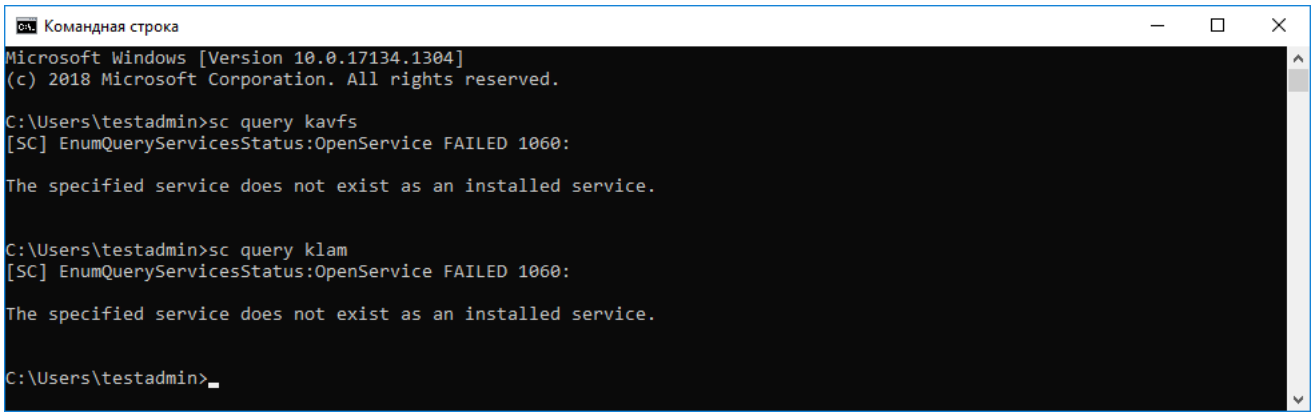
Asigurați-vă că Kaspersky Security for Windows Server a fost eliminat cu succes

Asigurați-vă că Kaspersky Security for Windows Server este complet eliminat:

- Directorul `%ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\` nu există.
- Următoarele servicii nu sunt prezente:
  - Kaspersky Security Service (KAVFS)
  - Serviciul Kaspersky Security Management (KAVFSGT)
  - Serviciul Kaspersky Security Exploit Prevention (KAVFSSLP)
  - Serviciul Kaspersky Security Script Checker (KAVFSSCS)

  Puteți verifica serviciile care rulează în Managerul de activități sau prin lansarea comenzii `sc query` (a se vedea figura de mai jos).
- Nu sunt prezente următoarele drivere:
  - klam.sys
  - klflt.sys
  - klramdisk.sys
  - klelaml.sys
  - klfltdev.sys
  - klips.sys
  - klids.sys
  - klwtpee

Puteți verifica driverele instalate în folderul `C:\Windows\System32\drivers` sau prin emiterea comenzii `sc query`. Dacă lipsește un serviciu sau un driver, veți primi următorul răspuns:



Asigurați-vă că serviciile și driverele Kaspersky Security for Windows Server au fost eliminate cu succes

În cazul în care pe server rămân fișiere de aplicații sau de drivere, ștergeți manual fișierele respective. Dacă serviciile Kaspersky Security for Windows Server încă mai rulează pe server, opriți (`sc stop`) și ștergeți (`sc delete`) serviciile manual. Pentru a opri driverul klam.sys, utilizați comanda `fltmc unload klam`.

Activarea KES cu o cheie KSWS

După instalarea aplicației, puteți activa Kaspersky Endpoint Security for Windows (KES) folosind o cheie de licență Kaspersky Security for Windows Server (KSWS). Procesul de activare după migrare depinde de metoda de activare KSWS (consultați tabelul de mai jos).

Kaspersky Endpoint Security nu acceptă *licența Kaspersky Security for Storage*. Pentru a lucra cu această licență, trebuie să utilizați Kaspersky Security for Windows Server.

Pentru a activa KES cu cheia KSWS poți folosi doar codul de activare. Dacă folosești un fișier cheie pentru a activa aplicația, trebuie să contactezi Suportul tehnic pentru un fișier cheie Kaspersky Endpoint Security.

Activarea Kaspersky Endpoint Security for Windows cu o cheie Kaspersky Security for Windows Server

Metoda de activare a Kaspersky Security for Windows Server	Migrarea cheii la Kaspersky Endpoint Security for Windows.
Distribuirea automată a cheii de licență KSWS către computere.	Dacă distribuirea automată a cheilor este activată în proprietățile cheii de licență KSWS, KES este activat automat cu cheia KSWS.
Cheia KSWS este adăugată de o activitate.	Dacă KSWS este activat utilizând activitatea, cheia de licență KSWS este ștearsă în timpul migrării de la KSWS. Trebuie să activați din nou aplicația. De exemplu, puteți adăuga o cheie de licență la pachetul de instalare Kaspersky Endpoint Security for Windows.
Cheia KSWS este adăugată local în interfața aplicației.	Dacă KSWS este activat local utilizând Expertul de activare a aplicației, cheia de licență KSWS este ștearsă în timpul migrării de la KSWS. Trebuie să activați din nou aplicația. De exemplu, puteți adăuga o cheie de licență la pachetul de instalare Kaspersky Endpoint Security for Windows.
Cheia KSWS este adăugată la pachetul de instalare.	Dacă KSWS este activat local utilizând cheia din pachetul de instalare, cheia de licență KSWS este ștearsă în timpul migrării de la KSWS. Trebuie să activați din nou aplicația. De exemplu, puteți adăuga o cheie de licență la pachetul de instalare Kaspersky Endpoint Security for Windows.
Imagine de mașină virtuală plătită (Amazon Machine Image – AMI) în Amazon Web Services (AWS).	Dacă ați achiziționat Kaspersky Security Center ca imagine de mașină virtuală plătită (Amazon Machine Image – AMI) în Amazon Web Services (AWS), nu este necesară activarea KES. În acest caz, Kaspersky Security Center utilizează abonamentul AWS care este deja adăugată în aplicație.
Imaginea Kaspersky Security Center gata pregătită și gratuită cu propria dvs. licență (modelul Bring Your Own License – BYOL).	Dacă folosiți o imagine Kaspersky Security Center gratuită și gata de utilizare cu propria licență într-un mediu cloud (modelul Bring Your Own License – BYOL), trebuie să activați aplicația prin orice metodă disponibilă. Veți avea nevoie de o licență Kaspersky Hybrid Cloud Security.

Considerații speciale pentru migrarea serverelor cu încărcare mare

În cazul serverelor cu încărcare mare, este important să se monitorizeze performanța și să se evite defecțiunile. După migrarea la Kaspersky Endpoint Security for Windows, vă recomandăm să dezactivați temporar componentele aplicației care utilizează resurse substanțiale ale serverului în comparație cu alte componente. După ce vă asigurați că serverul funcționează în mod normal, puteți activa din nou componentele aplicației.

Vă recomandăm să migrați serverele cu încărcare mare după cum urmează:

1. Creați o politică Kaspersky Endpoint Security cu setările implicite.

   Setările implicite sunt considerate optime. Aceste setări sunt recomandate de experții Kaspersky. Setările implicite oferă nivelul de protecție recomandat și utilizarea optimă a resurselor.

2. În setările de politică, dezactivați următoarele componente: Network Threat Protection, Behavior Detection, Exploit Prevention, Remediation Engine, Application Control.

   Dacă organizația dvs. are implementată soluția Kaspersky Managed Detection and Response (MDR), încărcați fișierul de configurare BLOB în politica Kaspersky Endpoint Security.

3. Eliminați Kaspersky Security for Windows Server de pe server.

4. Instalați Kaspersky Endpoint Security for Windows cu setul implicit de componente.

   Dacă organizația dvs. are implementate soluții Detection and Response, selectați componentele relevante în proprietățile pachetului de instalare.

5. Verificați setările aplicației:

   - Aplicația este activată cu ajutorul cheii de licență KSWS.
   - Se aplică noua politică. Componentele selectate anterior sunt dezactivate.

6. Asigurați-vă că serverul funcționează. Asigurați-vă că Kaspersky Endpoint Security for Windows nu utilizează mai mult de 1% din resursele serverului.

7. Dacă este necesar, creați excluderi de scanare, adăugați aplicații de încredere, creați o listă de adrese web de încredere.

8. Activați componentele Behavior Detection, Exploit Prevention, Remediation Engine. Asigurați-vă că Kaspersky Endpoint Security for Windows nu utilizează mai mult de 1% din resursele serverului.

9. Activați componenta Network Threat Protection. Asigurați-vă că Kaspersky Endpoint Security for Windows nu utilizează mai mult de 2% din resursele serverului.

10. Activați componenta Application Control în modul de testare a regulilor.

11. Asigurați-vă că Application Control funcționează. Dacă este necesar, adăugați noi reguli Application Control și dezactivați modul de testare a regulilor după ce confirmați că Application Control funcționează.

După migrarea de la KSWS la KES, asigurați-vă că aplicația funcționează corect. Verificați starea serverului în consolă (ar trebui să fie *OK*). Asigurați-vă că nu sunt raportate erori pentru aplicație, verificați, de asemenea, ora ultimei conexiuni la serverul de administrare, ora ultimei actualizări a bazei de date și starea de protecție a serverului.

Gestionarea aplicației pe un server în modul Server Core

Un server în modul Server Core nu are o interfață grafică. Prin urmare, poți gestiona aplicația de la distanță doar folosind consola Kaspersky Security Center sau local, din linia de comandă.

Gestionarea aplicației folosind consola Kaspersky Security Center

Instalarea aplicației folosind consola Kaspersky Security Center nu este diferită de instalarea acesteia în mod normal. Când creezi un pachet de instalare, poți adăuga o cheie de licență pentru a activa aplicația. Poți utiliza o cheie Kaspersky Endpoint Security for Windows sau o cheie Kaspersky Security for Windows Server.

Pe un server în modul Server Core, următoarele componente ale aplicației nu sunt disponibile: Web Threat Protection, Mail Threat Protection, Control Web, BadUSB Attack Prevention, File Level Encryption (FLE), Kaspersky Disk Encryption (FDE).

Repornirea nu este necesară atunci când instalezi Kaspersky Endpoint Security. Repornirea este necesară numai dacă trebuie să elimini aplicații incompatibile înainte de instalare. Repornirea poate fi necesară și atunci când actualizezi versiunea aplicației. Aplicația nu poate afișa o fereastră pentru a solicita utilizatorului să repornească serverul. Poți afla despre necesitatea repornirii serverului din rapoartele din consola Kaspersky Security Center.

Gestionarea aplicației pe un server în modul Server Core nu este diferită de gestionarea unui computer. Poți utiliza politici și activități pentru a configura aplicația.

Gestionarea aplicației pe un server în modul Server Core implică următoarele considerații speciale:

- Serverul în modul Server Core nu are o interfață grafică, prin urmare Kaspersky Endpoint Security nu afișează un avertisment care să îi spună utilizatorului că este necesară Dezinfectarea avansată. Pentru a neutraliza o amenințare, este necesar să activați tehnologia Dezinfectare avansată în setările aplicației și să activați imediat Dezinfectarea avansată din proprietățile activității *Scanare malware*. Apoi, este necesar să porniți activitatea *Scanare malware*.

- BitLocker Drive Encryption este disponibilă numai cu un Trusted Platform Module (TPM). Un PIN/o parolă nu poate fi utilizat(ă) pentru criptare, deoarece aplicația nu poate afișa fereastra de solicitare a parolei pentru autentificarea prepornire. Dacă sistemul de operare are modul de compatibilitate Standarde federale de procesare a informațiilor (FIPS) activat, conectați o unitate amovibilă pentru salvarea cheii de criptare înainte de a începe criptarea unității.

Gestionarea aplicației din linia de comandă

Când nu poți utiliza o interfață grafică, poți gestionați Kaspersky Endpoint Security din linia de comandă.

Pentru a instala aplicația pe un server în modul Server Core, executați următoarea comandă:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /s
```

Pentru a activa aplicația, execută următoarea comandă:

```
avp.com license /add <activation code or key file>
```

Pentru a verifica stările profilului aplicației, execută următoarea comandă:

```
avp.com status
```

Pentru a vizualiza lista comenzilor de administrare a aplicațiilor, execută următoarea comandă:

```
avp.com help
```

Migrarea de la [KSWS+KEA] la [KES+agent încorporat]

Atunci când migrați de la Kaspersky Security for Windows Server (KSWS) la Kaspersky Endpoint Security (KES), puteți utiliza următoarele recomandări pentru a configura protecția serverului și pentru a optimiza performanța. Aici vom analiza un exemplu de migrare pentru o singură organizație.

Infrastructura organizației

Compania are instalate următoarele echipamente:

- Kaspersky Security Center 14.2

  Administratorul gestionează soluțiile Kaspersky cu ajutorul Consolei de administrare (MMC). Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) este de asemenea implementat

  În Kaspersky Security Center, sunt create trei grupuri de administrare, care conțin serverele organizației: două grupuri de administrare pentru serverele SQL și un grup de administrare pentru serverele Microsoft Exchange. Fiecare grup de administrare este gestionat de propria politică. Activitățile *Database Update* și *On-demand scan* sunt create pentru toate serverele din organizație.

  Cheia de activare KSWS este adăugată la Kaspersky Security Center. Distribuirea automată a cheilor este activată.

- Servere SQL cu Kaspersky Security for Windows Server 11.0.1 și Kaspersky Endpoint Agent 3.11 instalate. Serverele SQL sunt combinate în două clustere.

  KSWS este administrat de politicile *SQL_Policy(1)* și *SQL_Policy(2)*. Sunt create și activitățile *Database Update*, *On-demand scan*.

- Un server Microsoft Exchange cu Kaspersky Security for Windows Server 11.0.1 și Kaspersky Endpoint Agent 3.11 instalat.

  KSWS este gestionat de politica *Exchange_Policy*. Sunt create și activitățile *Database Update*, *On-demand scan*.

Planificarea migrării

Migrarea implică următoarele etape:

1. Migrarea activităților și a politicilor KSWS cu ajutorul Expertului de conversie în bloc a politicilor și activităților.
2. Migrarea politicii Kaspersky Endpoint Agent cu ajutorul Expertului de conversie în bloc a politicilor și activităților.
3. Utilizarea etichetelor pentru a activa profilurile de politici în proprietățile noii politici.
4. Instalarea KES în loc de KSWS.
5. Activarea EDR Optimum.
6. Confirmarea faptului că KES funcționează.

Scenariul de migrare se realizează inițial pe unul dintre serverele SQL din cluster. Apoi, scenariul de migrare se realizează pe celălalt cluster de servere SQL. Apoi, scenariul de migrare se realizează pe Microsoft Exchange.

Migrarea activităților și a politicilor KSWS cu ajutorul Expertului de conversie în bloc a politicilor și activităților

Pentru a migra activitățile KSWS, puteți utiliza Expertul de conversie în bloc a politicilor și activităților (expertul de migrare). Ca urmare, în locul politicilor *SQL_Policy(1)*, *SQL_Policy(2)* și *Exchange_Policy*, veți obține o singură politică cu trei profiluri pentru serverele SQL și, respectiv, Microsoft Exchange. Noul profil de politici cu setări KSWS va fi numit *UpgradedFromKSWS <Numele politicii Kaspersky Security for Windows Server>*. În proprietățile profilului, asistentul de migrare selectează automat eticheta dispozitivului `UpgradedFromKSWS` ca și criteriu de declanșare. Astfel, setările din profilul de politică sunt aplicate automat serverelor.

Migrarea politicii Kaspersky Endpoint Agent cu ajutorul Expertului de conversie în bloc a politicilor și activităților

Pentru a migra politicile Kaspersky Endpoint Agent, puteți utiliza Expertul de conversie în bloc a politicilor și activităților. Expertul de migrare a politicilor și activităților pentru Kaspersky Endpoint Agent este disponibil numai în Consola web.

Utilizarea etichetelor pentru a activa profilurile de politici în proprietățile noii politici

Selectați eticheta dispozitivului pe care ați atribuit-o anterior ca și condiție de activare a profilului. Deschideți proprietățile politicii și selectați *General rules for policy profile activation* ca condiție de activare a profilului.

Instalarea KES în loc de KSWS

Înainte de a instala KES, trebuie să dezactivați Protecția prin parolă în proprietățile politicii KSWS.

Instalarea KES presupune următorii pași:

1. Pregătiți pachetul de instalare. În proprietățile pachetului de instalare, selectați kitul de distribuire Kaspersky Endpoint Security for Windows 12.0 și selectați setul implicit de componente.
2. Creați o activitate *Install application remotely* pentru unul dintre grupurile de administrare a serverului SQL.
3. În proprietățile activității, selectați pachetul de instalare și fișierul cu cheia de licență.
4. Așteptați până când activitatea se finalizează cu succes.
5. Repetați instalarea KES pentru celelalte grupuri de administrare.

Kaspersky Security Center adaugă automat eticheta `UpgradedFromKSWS` la numele computerelor din consolă după finalizarea instalării KES.

Pentru a verifica instalarea KES, puteți utiliza *Report on protection deployment*. De asemenea, puteți verifica starea dispozitivului. Pentru a confirma activarea aplicației, puteți utiliza *Report on usage of license keys*.

Activarea EDR Optimum

Puteți activa funcționalitatea EDR Optimum utilizând o licență Kaspersky Endpoint Detection and Response Optimum Add-on autonomă. Trebuie să confirmați că cheia EDR Optimum este adăugată în depozitul Kaspersky Security Center și că este activată funcționalitatea de distribuire automată a cheilor de licență.

Pentru a verifica activarea componentei EDR Optimum, puteți utiliza *Report on status of application components*.

Confirmarea faptului că KES funcționează

Pentru a confirma că KES funcționează, puteți verifica dacă nu sunt raportate erori. Starea dispozitivului trebuie să fie *OK*. Activități de actualizare și scanare malware și finalizate cu succes.

Modul Light Agent pentru protejarea mașinilor virtuale

Începând cu versiunea 12.8, poți utiliza Kaspersky Endpoint Security for Windows ca parte a Kaspersky Security for Virtualization Light Agent. *Kaspersky Security for Virtualization Light Agent* este o soluție integrată care oferă protecție completă pentru mașinile virtuale împotriva diferitelor tipuri de amenințări la securitatea informațiilor, atacuri de rețea și atacuri de tip phishing. Pentru a utiliza această soluție, trebuie să instalezi aplicația în modul Light Agent.

Instalarea Kaspersky Endpoint Security în modul Light Agent pe mașinile virtuale bazate pe arhitectura ARM nu este acceptată.

Poți utiliza Kaspersky Endpoint Security în modul Light Agent ca parte a Kaspersky Security for Virtualization Light Agent începând cu versiunea 6.2.

Când pornești Light Agent, acesta stabilește și menține o conexiune la SVM-ul mașinii virtuale (Secure Virtual Machine). Un Server de protecție este implementat pe SVM. *Serverul de protecție* este componenta soluției Kaspersky Security for Virtualization Light Agent care scanează fișierele pentru viruși și alte programe malware, actualizează bazele de date antivirus și gestionează cheile de licență. Light Agent trimite fișiere sau fragmente ale acestora care necesită scanare către SVM. Rezultatele scanării sunt disponibile pentru toate mașinile virtuale pe care este instalat Light Agent (tehnologia SharedCache). Această tehnologie sporește eficiența soluției și asigură un răspuns mai rapid la amenințări.

Infrastructura organizației poate conține multe mașini virtuale cu Light Agent instalat și multe SVM-uri. Serverul de integrare gestionează interacțiunea dintre mașinile virtuale și SVM-urile. *Serverul de integrare* este o componentă a soluției Kaspersky Security for Virtualization Light Agent care generează o listă de SVM-uri disponibile și transferă aceste date către Light Agents, participă la descoperirea SVM-urilor de către Light Agents, protejează conexiunea dintre Light Agents și SVM-uri și îndeplinește alte funcții.

Considerații speciale pentru modul Light Agent

Poți gestiona Kaspersky Endpoint Security în modul Standard și în modul Light Agent, utilizând politicile și activitățile Kaspersky Endpoint Security. În modul Light Agent, unele componente și caracteristici ale aplicației nu sunt disponibile.

Actualizarea bazelor de date și modulelor aplicației

Kaspersky Endpoint Security în modul Light Agent utilizează baze de date cu programe malware speciale de care are nevoie aplicația atunci când lucrează ca parte a soluției Kaspersky Security for Virtualization Light Agent. Kaspersky Endpoint Security primește baze de date și actualizări ale modulelor aplicațiilor de la Serverul de protecție.

Bazele de date și modulele de pe mașinile virtuale protejate sunt actualizate cu ajutorul unei activități speciale *Actualizarea modulelor bazelor de date și ale aplicațiilor*, în care un director de pe SVM este specificat ca sursă de actualizare. Light Agent execută automat activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor*. Nu poți selecta o sursă de actualizare diferită, nu poți configura programarea activităților sau eliminarea activității.

O derulare înapoi a celei mai recente actualizări a bazei de date malware este gestionată și pe partea Serverului de protecție. După o derulare înapoi a bazelor de date și a modulelor aplicației de pe SVM, o activitate locală specială *Actualizarea modulelor bazelor de date și ale aplicațiilor* este pornită pe mașina virtuală protejată. Această activitate face ca Light Agent să revină la utilizarea setului anterior de baze de date cu programe malware.

Kaspersky Endpoint Security în modul Light Agent nu acceptă activitatea *Derulare înapoi actualizare*.

Activarea Light Agent

Pentru a activa aplicația, trebuie să adaugi o cheie de licență la SVM-ul la care este conectat Light Agent. Nu este nevoie să activezi aplicația separat.

Alte considerații speciale pentru modul Light Agent

- Când creezi o politică pentru aplicație, îți recomandăm să selectezi modul Light Agent. În acest mod, Expertul pentru o politică nouă îți solicită să configurezi conexiunea SVM. Aceste setări sunt necesare pentru ca aplicația să funcționeze în modul Light Agent.
- Nu poți instala componentele Data Encryption și Control adaptiv al anomaliilor în modul Light Agent. Setul de componente depinde și de tipul sistemului de operare invitat: stație de lucru sau server.
- Light Agent nu acceptă integrarea cu soluțiile Kaspersky Endpoint Detection and Response Expert și Kaspersky Endpoint Detection and Response Expert (cloud).
- Poți gestiona Light Agent în Consola de administrare (MMC) și Kaspersky Security Center Web Console. Nu este posibil să gestionați Light Agent în Kaspersky Security Center Cloud Console.
- Modificarea setului de componente ale aplicației pe mașinile virtuale VDI nu este acceptată.
- Kaspersky Endpoint Security comunică cu serverele KSN printr-un server proxy KSN. Comunicarea directă cu KSN nu este acceptată.
- Modul Cloud al Kaspersky Security Network nu este acceptat.
- Utilizarea serverului proxy al aplicației la conectarea la Serverul de integrare (VIIS), la Serverul de protecție (SVM) și la serverele KSN nu este acceptată.

Configurarea preliminară a mașinii virtuale

Poți instala Kaspersky Endpoint Security pe o mașină virtuală care utilizează tehnologia platformei virtuale. Kaspersky Endpoint Security acceptă platformele virtuale VMware, Microsoft Hyper-V, Citrix. Înainte de instalare, trebuie să efectuezi configurarea preliminară a mașinilor virtuale.

Compatibilitatea cu tehnologia Citrix App Layering

Dacă intenționezi să utilizezi Full User Layer pentru a salva starea mașinilor virtuale temporare, trebuie să parcurgi următoarele etape înainte de a instala pe șablon mașinii virtuale:

1. Creează fișierul C:\Program Files\Unidesk\Uniservice\UserExclusions\KESLA.txt și adaugă în el următoarele excluderi:

   - `C:\ProgramData\KasperskyLab\`
   - `C:\ProgramData\Kaspersky Lab\`
   - `C:\Program Files (x86)\Kaspersky Lab\`

2. În registry-ul sistemului de operare în cheia HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Unifltr, creează o nouă valoare DWORD numită MiniFilterBypass și seteaz-o la 1.

3. În registry-ul sistemului de operare în cheia HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Unirsd, creează o nouă valoare MULTI_SZ numită ExcludeKey și seteaz-o la \Registry\Machine\SOFTWARE\WOW6432Node\KasperskyLab.

4. Repornește mașina virtuală.

Pentru instalarea pe mașini virtuale într-o infrastructură care utilizează Citrix App Layering, trebuie să faci următoarele:

1. Instalează Kaspersky Security Center Administration Agent și Kaspersky Endpoint Security for Windows pe șablonul mașinii virtuale din Application Layer.

2. Creează o imagine de mașină virtuală constând din mai multe straturi.

3. Implementează imaginea creată pe hipervizoarele care acceptă soluția Citrix App Layering.

4. Configurează crearea de mașini virtuale temporare din imaginea creată.

Pentru detalii despre instalarea software-ului antivirus împreună cu Citrix App Layering, consultă Documentația Citrix App Layering.

Compatibilitatea cu tehnologia Citrix Provisioning (Citrix Provisioning Services)

Pentru a te asigura că aplicația este compatibilă cu tehnologia Citrix Provisioning (Citrix Provisioning Services):

- Dacă software-ul Citrix Provisioning Target Device este instalat pe mașina virtuală, trebuie să îl elimini înainte de a instala aplicația Kaspersky Endpoint Security (pentru detalii, accesează pagina Site-ul web de asistență tehnică Citrix). După instalarea aplicației, trebuie să instalezi Citrix Provisioning Target Device.

- La instalarea aplicației utilizând Expertul de configurare sau de la distanță, folosind Kaspersky Security Center, trebuie să bifezi caseta de selectare **Asigură compatibilitatea cu Citrix PVS**.

Compatibilitatea cu tehnologia Omnissa App Volumes

Înainte de a instala pe șablon mașinii virtuale, trebuie să creezi fișierul %SVAgent%\Config\Custom\snapvol.cfg fișier și să adaugi în el următoarele excluderi:

- `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`

Pentru detalii, consultați documentația Omnissa.

Instalarea Light Agent

Instalarea Kaspersky Endpoint Security în modul Light Agent pe mașinile virtuale bazate pe arhitectura ARM nu este acceptată.

Instalarea aplicației în modul Light Agent este aceeași ca și în modul Standard. Înainte de a instala Light Agent pe o mașină virtuală, trebuie să te asiguri că Kaspersky Security Center Network Agent este instalat. Componenta *Agent de rețea* facilitează interacțiunea dintre Serverul de administrare și o mașină virtuală.

Light Agent poate fi instalat pe o mașină virtuală în unul dintre următoarele moduri:

- De la distanță, folosind Kaspersky Security Center.
- Local, folosind Expertul de configurare.
- Local, din linia de comandă.

Pentru a instala Light Agent, trebuie să selectați configurația corespunzătoare în setările pachetului de instalare sau în Expertul de configurare.

Atunci când se instalează Light Agent pe un server, componentele de protecție avansată (Behavior Detection, Exploit prevention, Remediation Engine) sunt excluse din configurația implicită a aplicației. Setările implicite ale aplicației oferă nivelul de protecție recomandat și utilizarea optimă a resurselor serverului. Atunci când se instalează Light Agent pe o stație de lucru, componentele de protecție avansată sunt incluse în configurația implicită a aplicației.

Când instalezi Light Agent, recomandăm selectarea excluderi lor predefinite și a aplicațiilor de încredere pentru mediul virtual relevant. Excluderile de scanare predefinite și aplicațiile de încredere te ajută să configurezi rapid aplicația și să eviți problemele de compatibilitate cu mediul virtual. De asemenea, poți configura excluderile de scanare predefinite și aplicațiile de încredere dupa instalare, în politică.

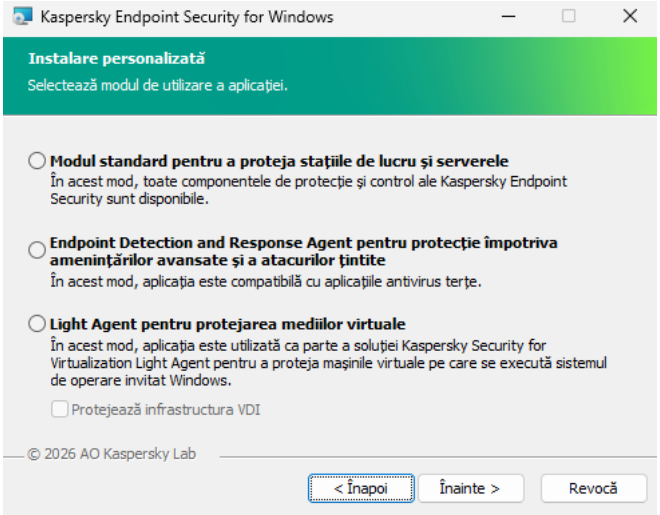
Când instalezi Light Agent pe mașini virtuale persistente, poate fi necesar să modifici algoritmul de generare Sensor ID. Sensor ID este utilizat în soluția Kaspersky Anti Targeted Attack Platform pentru a identifica computerele care trimit telemetrie către server. Pentru a crea un Sensor ID unic, setează `EnableUniqueSensorID=1` când instalezi aplicația din linia de comandă.

Cum se instalează Light Agent utilizând Expertul de configurare

1. Copiază directorul cu kitul de distribuție pe o mașină virtuală.
2. Rulați setup_kes.exe.

   Expertul de instalare pornește.

Configurarea Kaspersky Endpoint Security



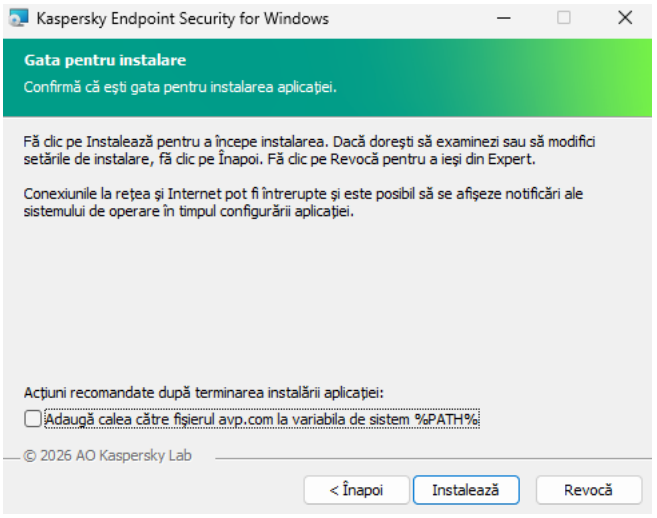
Alegerea configurației aplicației

Selectați configurația **Light Agent pentru protejarea mediilor virtuale**. Această configurație este destinată aplicației care este utilizată ca parte a soluției Kaspersky Security for Virtualization Light Agent. Light Agent trebuie instalat pe fiecare mașină virtuală care trebuie protejată folosind soluția. În această configurație, nu puteți utiliza componentele Data Encryption sau Control adaptiv al anomaliilor. Dacă instalezi Light Agent pe un șablon de mașină virtuală care va fi folosit pentru a crea *mașini virtuale non-persistente*, bifează caseta de selectare **Protejează infrastructura VDI** (VDI înseamnă Virtual Desktop Infrastructure). Modul de protecție VDI ajută la optimizarea performanței Kaspersky Endpoint Security pe mașinile virtuale non-persistente. În acest mod, Light Agent refuză actualizările aplicației care necesită repornirea mașinii virtuale. Când se primesc actualizări ale aplicației care necesită o repornire, Light Agent generează un eveniment despre necesitatea actualizării șablonului mașinilor virtuale protejate.

Componentele Kaspersky Endpoint Security

Selectați componentele pe care doriți să le instalați (consultați figura de mai jos). Puteți schimba componentele disponibile ale aplicației după instalarea aplicației. Pentru a face acest lucru, trebuie să executați din nou Expertul de configurare și să alegeți să schimbați componentele disponibile.

Setări avansate



Setări avansate pentru instalarea aplicației

Protejează procesul de instalare a aplicației. Protejarea instalării include protecția împotriva înlocuirii pachetului de distribuție cu aplicații rău intenționate, blocarea accesului la directorul de instalare al aplicației Kaspersky Endpoint Security și blocarea accesului la secțiunea de registre a sistemului care conține cheile aplicației. Cu toate acestea, dacă aplicația nu poate fi instalată (de exemplu, atunci când se execută o instalare la distanță cu ajutorul Windows Remote Desktop), te sfătuim să dezactivezi protecția procesului de instalare.

Asigură compatibilitatea cu Citrix PVS. Poți activa suportul pentru Citrix Provisioning Services pentru a instala aplicația Kaspersky Endpoint Security pe o mașină virtuală.

Adaugă calea către fișierul avp.com la variabila de sistem %PATH%. Poți adăuga calea de instalare la variabila %PATH% pentru utilizarea comodă a interfeței liniei de comandă.

Cum se instalează Light Agent utilizând linia de comandă

1. Executați interpretorul de linii de comandă (cmd.exe) ca administrator.
2. Deschide directorul în care se află pachetul de distribuție pentru Kaspersky Endpoint Security.
3. Execută următoare comandă:

   ```
   setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pLIGHTAGENTMODE=1 [/pVDI=1] [/s]
   ```

   sau

   ```
   msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 LIGHTAGENTMODE=1 [VDI=1] [/qn]
   ```

   Opțiunea `VDI` activează modul de protecție VDI (Virtual Desktop Infrastructure). Modul de protecție VDI ajută la optimizarea performanței Kaspersky Endpoint Security pe mașinile virtuale non-persistente. În acest mod, Light Agent refuză actualizările aplicației care necesită repornirea mașinii virtuale. Când se primesc actualizări ale aplicației care necesită o repornire, Light Agent generează un eveniment despre necesitatea actualizării șablonului mașinilor virtuale protejate. În mod implicit, modul de protecție VDI este dezactivat.

Ca rezultat, Light Agent este instalat pe mașina virtuală cu setul de componente implicit. Poți edita setul de componente și poți specifica setările avansate folosind fișierul setup.ini. De asemenea, poți specifica setările de instalare în linia de comandă.

Cum se instalează Light Agent utilizând Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele consolei, selectează directorul **Advanced** → **Remote installation** → **Installation packages**.

   Aceasta deschide o listă cu pachetele de instalare care au fost descărcate în Kaspersky Security Center.
3. Deschide proprietățile pachetului de instalare Kaspersky Endpoint Security for Windows.

   Daca este necesar, creați un nou pachet de instalare.
4. Accesează secțiunea **Settings**.
5. Selectați configurația **Light Agent pentru protejarea mediilor virtuale**. Această configurație este destinată aplicației care este utilizată ca parte a soluției Kaspersky Security for Virtualization Light Agent. Light Agent trebuie instalat pe fiecare mașină virtuală care trebuie protejată folosind soluția. În această configurație, nu puteți utiliza componentele Data Encryption sau Control adaptiv al anomaliilor. Dacă instalezi Light Agent pe un șablon de mașină virtuală care va fi folosit pentru a crea *mașini virtuale non-persistente*, bifează caseta de selectare **Protejează infrastructura VDI** (VDI înseamnă Virtual Desktop Infrastructure). Modul de protecție VDI ajută la optimizarea performanței Kaspersky Endpoint Security pe mașinile virtuale non-persistente. În acest mod, Light Agent refuză actualizările aplicației care necesită repornirea mașinii virtuale. Când se primesc actualizări ale aplicației care necesită o repornire, Light Agent generează un eveniment despre necesitatea actualizării șablonului mașinilor virtuale protejate.
6. Selectați componentele pe care doriți să le instalați.

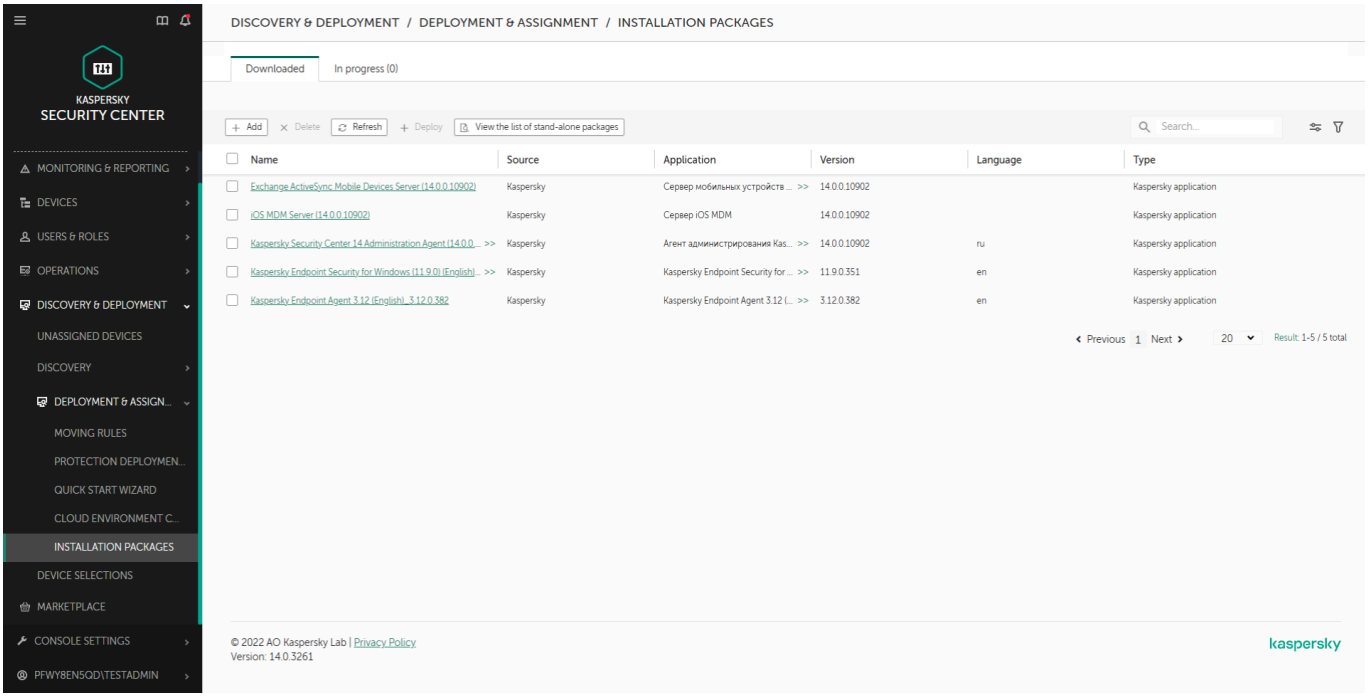
   Puteți schimba componentele disponibile ale aplicației după instalarea aplicației.
7. Configurează zona de încredere. Selectează excluderile de la scanare predefinite și aplicațiile de încredere pentru mediul virtual în care instalezi aplicația.

   Excluderile de scanare predefinite și aplicațiile de încredere te ajută să configurezi rapid aplicația și să eviți problemele de compatibilitate cu mediul virtual.
8. Salvați-vă modificările.
9. Creați unui pachet de instalare la distanță. În proprietățile activității, selectați pachetul de instalare pe care l-ați creat.

Cum se instalează Light Agent utilizând Web Console

1. În fereastra principală a componentei Web Console, selectați **Discovery & deployment** → **Deployment & assignment** → **Installation packages**.

Aceasta deschide o listă cu pachetele de instalare care au fost descărcate în Kaspersky Security Center.



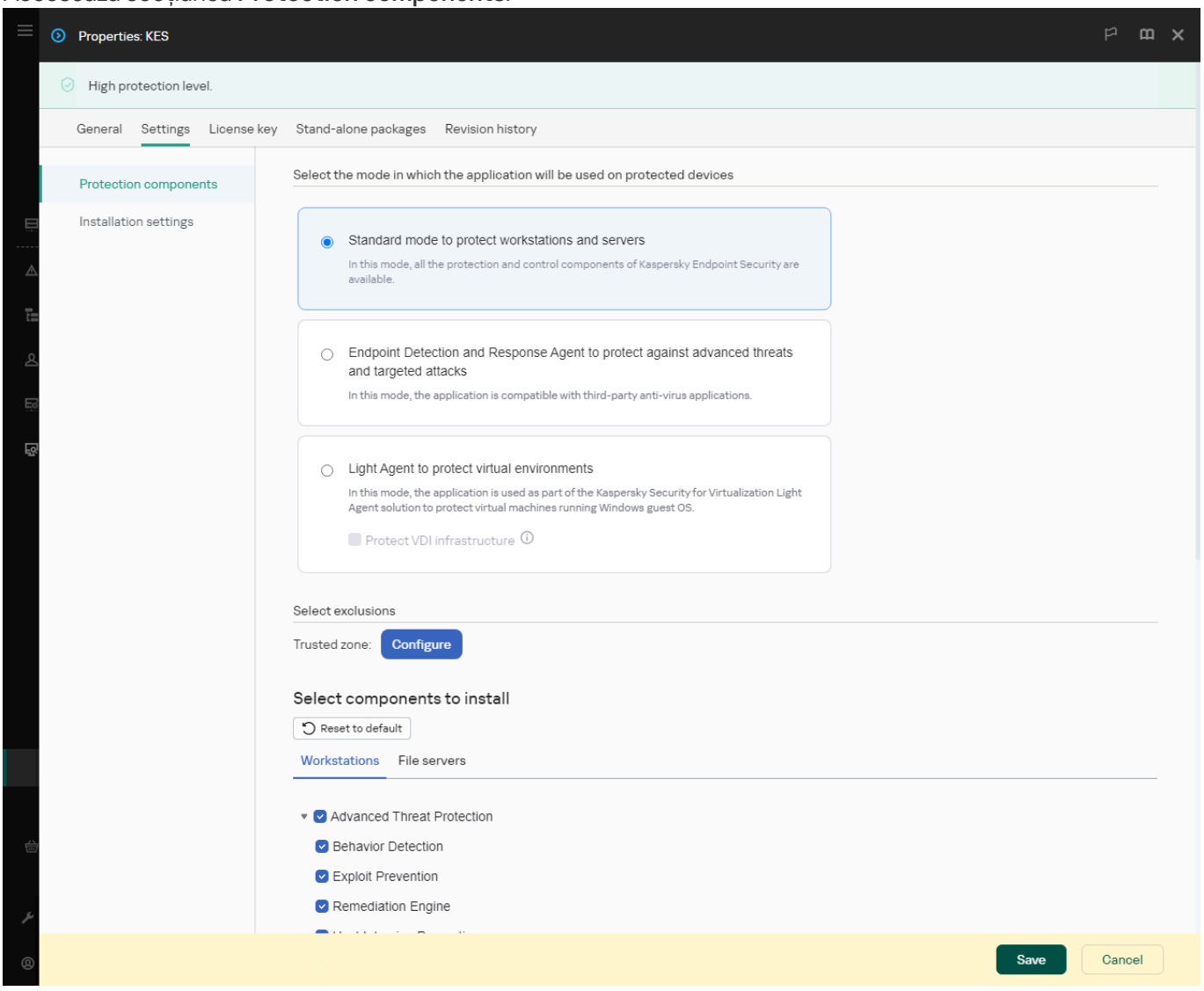
Lista pachetelor de instalare

2. Deschide proprietățile pachetului de instalare Kaspersky Endpoint Security for Windows.

   Daca este necesar, creați un nou pachet de instalare.

3. Selectați fila **Settings**.

4. Accesează secțiunea **Protection components**.



Componente incluse în pachetul de instalare

5. Selectați configurația **Light Agent to protect virtual environments**. Această configurație este destinată aplicației care este utilizată ca parte a soluției Kaspersky Security for Virtualization Light Agent. Light Agent trebuie instalat pe fiecare mașină virtuală care trebuie protejată folosind soluția. În această configurație, nu puteți utiliza componentele Data Encryption sau Control adaptiv al anomaliilor. Dacă instalezi Light Agent pe un șablon de mașină virtuală care va fi folosit pentru a crea *mașini virtuale non-persistente*, bifează caseta de selectare **Protect VDI infrastructure** (VDI înseamnă Virtual Desktop Infrastructure). Modul de protecție VDI ajută la optimizarea performanței Kaspersky Endpoint Security pe mașinile virtuale non-persistente. În acest mod, Light Agent refuză actualizările aplicației care necesită repornirea mașinii virtuale. Când se primesc actualizări ale aplicației care necesită o repornire, Light Agent generează un eveniment despre necesitatea actualizării șablonului mașinilor virtuale protejate.

6. Selectați componentele pe care doriți să le instalați.

   Puteți schimba componentele disponibile ale aplicației după instalarea aplicației.

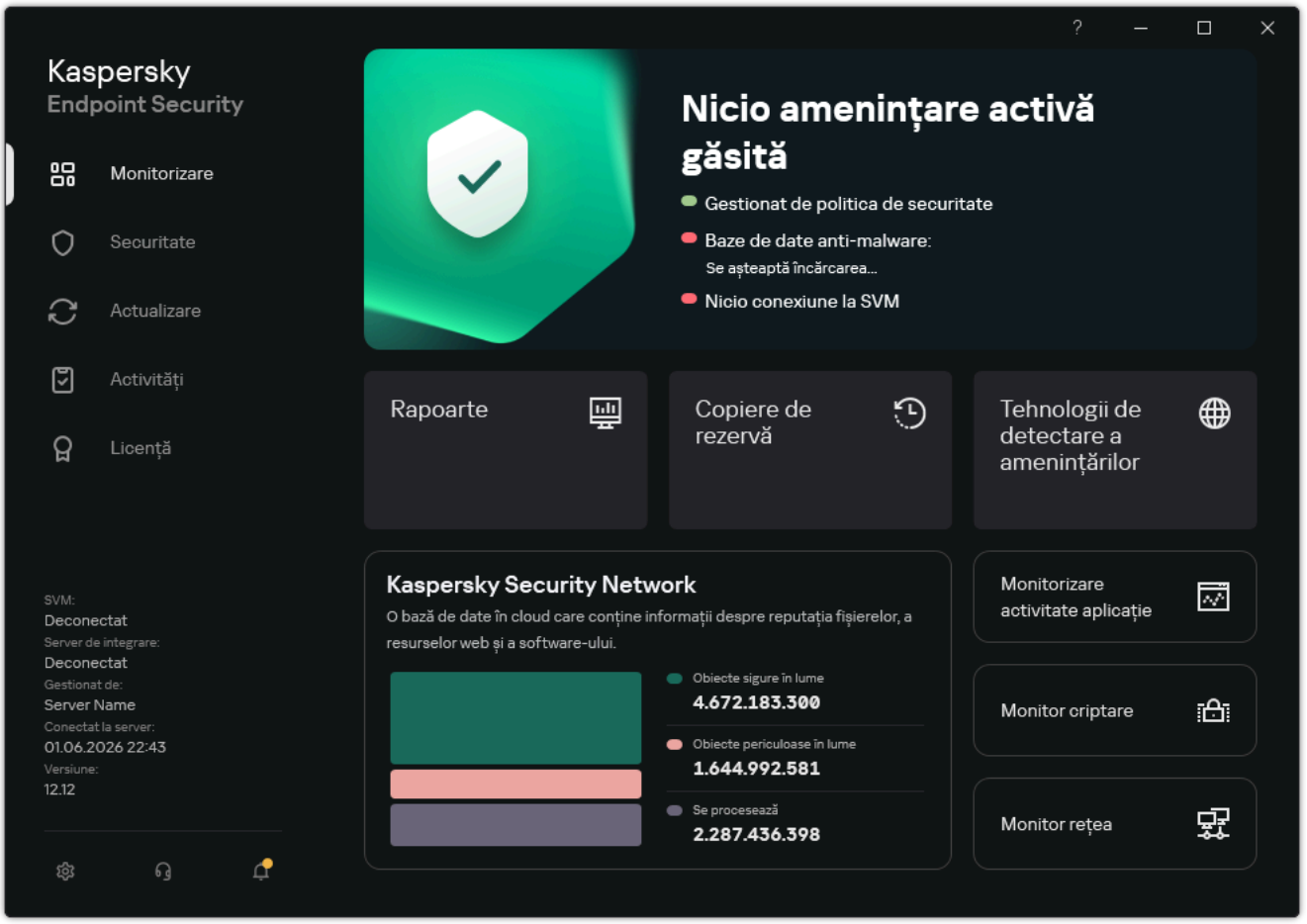
7. Configurează zona de încredere. Selectează excluderile de la scanare predefinite și aplicațiile de încredere pentru mediul virtual în care instalezi aplicația.

   Excluderile de scanare predefinite și aplicațiile de încredere te ajută să configurezi rapid aplicația și să eviți problemele de compatibilitate cu mediul virtual.

8. Salvați-vă modificările.

9. Creați unui pachet de instalare la distanță. În proprietățile activității, selectați pachetul de instalare pe care l-ați creat.

Drept rezultat, Light Agent este instalat pe mașina virtuală. Puteți utiliza interfața aplicației și o pictogramă a aplicației este afișată în zona de notificare . Acum trebuie să configurezi conecxiune Light Agent la SVM.



Fereastra principală a Light Agent

Conectarea Light Agent la SVM

Soluția Kaspersky Security for Virtualization Light Agent necesită comunicare continuă între Light Agent și SVM. Acest lucru este necesar pentru a scana fișierele trimise de Light Agent pentru viruși și alte programe malware. Fără o conexiune SVM, Light Agent nu poate trimite fișiere pentru scanare. Dacă conexiunea nu poate fi stabilită timp de peste cinci minute, scanarea se termină cu o eroare.

Conectarea unui Light Agent la un SVM implică următorii pași:

1. Light Agent primește lista SVM-urilor disponibile.

2. Light Agent determină un Server de protecție disponibil (SVM) care este optim pentru stabilirea conexiunii conform Algoritmul de selectare a SVM-urilor.

3. Light Agent verifică setări suplimentare de conectare la SVM: etichete, starea protecției conexiunii, funcționalitatea aplicației acoperită de licență.

4. Conectarea Light Agent la SVM.

Poți obține informații despre starea conexiunii Light Agent la SVM în Kaspersky Endpoint Security sau folosind comanda aplicației. Aplicația generează un eveniment ori de câte ori se pierde sau se stabilește conexiunea SVM-ului Light Agent și trimite aceste evenimente către Kaspersky Security Center. Dacă utilizați un Server de integrare pentru descoperirea SVM, poți obține informații despre starea SVM-ului și numărul de agenți Light Agents conectați în consola Serverului de integrare. Pentru detalii despre monitorizarea stării SVM-ului, consultă Ajutor Kaspersky Security for Virtualization Light Agent.

Descoperire SVM

Poți selecta una dintre metodele de descoperire a SVM-ului pentru Light Agent:

- Utilizarea serverului de integrare (VIIS).

  Serverul de integrare este componenta soluției care permite interacțiunea Kaspersky Security for Virtualization Light Agent cu infrastructura virtuală și generează o listă de SVN-uri disponibile pentru conectare. Light Agent stabilește o conexiune cu Integration Server și primește lista adreselor SVM.

  Serverul de integrare este cel mai util în infrastructurile virtuale mari, deoarece echilibrează automat sarcina între SVM-uri, obține informații despre SVM-urile disponibile, analizează aceste informații și oferă Light Agents o listă de servere de protecție (SVM) optime pentru conectare.

  Pentru ca Light Agent să poată obține o listă de SVM-uri, trebuie doar să introduci adresa Serverului de integrare.

- Utilizarea listei de adrese SVM.

  Dacă trebuie să specifici SVM-uri individuale la care dorești să se conecteze Light Agent, poți pregăti o listă manual.

  Trebuie să enumerezi adresele SVM-urilor disponibile la care se poate conecta Light Agent.

Cum se configurează descoperirea SVM-ului de către Light Agent în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Modul Light Agent → Setări descoperire SVM**.
4. Selectează o metodă de descoperire a SVM-urilor.

   - **Utilizează Serverul de integrare**. Introdu setările de conectare la Serverul de integrare. Introdu adresa IP în format IPv4 sau numele de domeniu complet calificat (FQDN) al dispozitivului pe care este instalat Serverul de integrare.

   - **Utilizează o listă personalizată de adrese SVM**. Creează o listă de SVM-uri la care Light Agent se poate conecta. Specifică adresa IP în format IPv4 sau numele de domeniu complet calificat (FQDN) al SVM-ului. Fiecare element al listei trebuie introdus pe o linie nouă sau separat de elementul anterior prin caracterul punct și virgulă (`;`).

     > În lista de adrese SVM, specifică numai nume de domeniu complete (FQDN) care sunt corelate cu o singură adresă IP. Utilizarea unui nume de domeniu complet calificat care corespunde mai multor adrese IP poate duce la erori ale soluției.

5. Salvați-vă modificările.

Cum se configurează descoperirea SVM-ului de către Light Agent în Web Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Light Agent Mode** → **SVM discovery settings**.
5. Selectează o metodă de descoperire a SVM-urilor.

   - **Use Integration Server**. Introdu setările de conectare la Serverul de integrare. Introdu adresa IP în format IPv4 sau numele de domeniu complet calificat (FQDN) al dispozitivului pe care este instalat Serverul de integrare.
   - **Use a custom list of SVM addresses**. Creează o listă de SVM-uri la care Light Agent se poate conecta. Specifică adresa IP în format IPv4 sau numele de domeniu complet calificat (FQDN) al SVM-ului. Fiecare element al listei trebuie introdus pe o linie nouă sau separat de elementul anterior prin caracterul punct și virgulă (`;`).

     În lista de adrese SVM, specifică numai nume de domeniu complete (FQDN) care sunt corelate cu o singură adresă IP. Utilizarea unui nume de domeniu complet calificat care corespunde mai multor adrese IP poate duce la erori ale soluției.
6. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se configurează descoperirea SVM-ului de către Light Agent în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul .
2. În fereastra de setări a aplicației, în **Modul Light Agent** fă clic pe opțiunea **Setări descoperire SVM**.
3. Selectează o metodă de descoperire a SVM-urilor.

   - **Utilizează Serverul de integrare**. Introdu setările de conectare la Serverul de integrare. Introdu adresa IP în format IPv4 sau numele de domeniu complet calificat (FQDN) al dispozitivului pe care este instalat Serverul de integrare.
   - **Utilizează o listă personalizată de adrese SVM**. Creează o listă de SVM-uri la care Light Agent se poate conecta. Specifică adresa IP în format IPv4 sau numele de domeniu complet calificat (FQDN) al SVM-ului. Fiecare element al listei trebuie introdus pe o linie nouă sau separat de elementul anterior prin caracterul punct și virgulă (`;`).

     În lista de adrese SVM, specifică numai nume de domeniu complete (FQDN) care sunt corelate cu o singură adresă IP. Utilizarea unui nume de domeniu complet calificat care corespunde mai multor adrese IP poate duce la erori ale soluției.
4. Salvați-vă modificările.

Configurarea algoritmului de selectare a SVM pentru Light Agent

Infrastructura organizației poate avea mai multe SVM-uri implementate la care Light Agents se pot conecta. Pentru a echilibra sarcina în rețea și resursele infrastructurii virtuale, trebuie să distribui Light Agents între SVM-uri.

Light Agents pot aplica următorii algoritmi de selectare a SVM-ului pentru conectare:

Algoritm standard (implicit)

Dacă se aplică acest algoritm, după instalare și pornire, Light Agent de pe mașina virtuală alege să se conecteze la un SVM *local* în raport cu Light Agent.

Faptul că un SVM este considerat local pentru un Light Agent depinde de tipul infrastructurii virtuale:

- Într-o infrastructură virtuală bazată pe Basis Dynamix Enterprise, SVM-ul considerat local pentru un Light Agent este SVM-ul implementat pe același nod ca mașina virtuală pe care este instalat Light Agent.
- Într-o infrastructură virtuală bazată pe Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer sau Basis Dynamix Standard, SVM-ul considerat local pentru un Light Agent este SVM-ul implementat pe același hipervizor ca și mașina virtuală pe care este instalat Light Agent.
- Într-o infrastructură virtuală care se execută pe platforma OpenStack sau VK Private Cloud, poți specifica modul de determinare a locației SVM-ului în raport cu Light Agent folosind parametrul `StandardAlgorithmSvmLocality` în secțiunea `HypervisorSpecificSettings:Openstack` din fișierul de configurare al serverului de integrare, appsettings.json. În funcție de versiunea Serverului de integrare, fișierul se află în una dintre următoarele căi:
  - /var/opt/kaspersky/viis/common/ pentru Serverul de integrare bazat pe Linux
  - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\ pentru Serverul de integrare bazat pe Windows

  Parametrul `StandardAlgorithmSvmLocality` poate lua următoarele valori:
  - `ServerGroup` – dacă este selectată această valoare, SVM-ul este considerat local pentru Light Agent dacă se află în același grup de servere ca și mașina virtuală pe care este instalat Light Agent. Această valoare este utilizată în mod implicit.
  - `Project` – dacă este selectată această valoare, SVM-ul este considerat local pentru Light Agent dacă acesta este implementat în cadrul aceluiași proiect OpenStack ca și mașina virtuală pe care este instalat Light Agent.
  - `AvailabilityZone` – dacă este selectată această valoare, SVM-ul este considerat local pentru Light Agent dacă se află în aceeași zonă de disponibilitate ca și mașina virtuală pe care este instalat Light Agent.

Dacă nu există SVM-uri locale disponibile pentru conectare, Light Agent selectează SVM-ul cu cei mai puțini Light Agents conectați, indiferent de calea SVM-ului din infrastructura virtuală.

Aplicația nu determină dacă SVM-ul este local în raport cu Light Agent dacă modul de protecție pentru infrastructură mare este activat pentru Serverul de protecție de pe SVM. În acest caz, se recomandă utilizarea algoritmului extins de selecție a SVM-ului și selectarea Serverului de integrare ca metodă de descoperire a SVM-ului.

Algoritm extins

Dacă se aplică acest algoritm, poți defini următoarele setări de selectare a SVM-ului:

- dacă să se ia în considerare sau să se ignore locația SVM-ului în infrastructură atunci când se aleg SVM-uri pentru conectare
- dacă se ia în considerare locația SVM-ului, metoda de determinare a localizării SVM-ului în raport cu Light Agent

Dacă Light Agents ignoră locația SVM-urilor în infrastructură, aceștia se vor putea conecta la orice SVM-uri disponibile pentru conectare.

Dacă Light Agents trebuie să ia în considerare locația SVM-urilor în infrastructură, trebuie să selectezi tipul de cale pentru SVM care va fi luat în considerare la determinarea locației SVM-ului în raport cu Light Agent. Faptul că un SVM este considerat local pentru Light Agent depinde de tipul infrastructurii virtuale.

Într-o infrastructură virtuală bazată pe Basis Dynamix Enterprise, un SVM poate fi considerat local pentru Light Agent în oricare dintre următoarele cazuri:

- Un SVM este implementat pe același nod ca și mașina virtuală pe care este instalat Light Agent.
- Un SVM este implementat în aceeași zonă ca și mașina virtuală pe care este instalat Light Agent.
- Un SVM este implementat în același centru de date ca și mașina virtuală pe care este instalat Light Agent.

Într-o infrastructură virtuală bazată pe Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer sau Basis Dynamix Standard, un SVM poate fi considerat local față de Light Agent în oricare dintre următoarele cazuri:

- Un SVM este implementat pe același hipervizor ca și mașina virtuală pe care este instalat Light Agent.
- Un SVM este implementat pe același cluster de hipervizori ca și mașina virtuală pe care este instalat Light Agent.
- Un SVM este implementat în același centru de date ca și mașina virtuală pe care este instalat Light Agent.

Într-o infrastructură virtuală care se execută pe platforma OpenStack sau VK Private Cloud, un SVM poate fi considerat local față de Light Agent în oricare dintre următoarele cazuri:

- Un SVM se află în același grup de servere ca și mașina virtuală pe care este instalat Light Agent.
- Un SVM este implementat în cadrul aceluiași proiect OpenStack ca și mașina virtuală pe care este instalat Light Agent.
- Un SVM se află în aceeași zonă de disponibilitate ca și mașina virtuală pe care este instalat Light Agent.

Dacă Light Agents iau în considerare locația SVM-urilor în infrastructură atunci când aleg SVM-ul la care să se conecteze, Light Agents se pot conecta doar la SVM-uri locale.

De exemplu, dacă specifici un cluster de hipervizori ca tip de cale pentru SVM, toate SVM-urile implementate pe acest cluster de hipervizori vor fi considerate locale pentru Light Agent, iar Light Agent se poate conecta doar la unul dintre aceste SVM-uri. Dacă nu există SVM-uri disponibile pentru conectare în același cluster în care se execută Light Agents, Light Agent nu se conectează la SVM.

La selectarea SVM-urilor, Light Agents iau în considerare și numărul de Light Agents conectați pentru a se asigura că aceștia sunt distribuiți uniform între SVM-urile disponibile pentru conectare.

Dacă Light Agent utilizează algoritmul extins de selectare a SVM-ului și metoda de descoperire a SVM-ului este setată la lista de adrese pentru SVM, iar modul de protecție a infrastructurii mari este activat pe SVM, atunci conectarea unui Light Agent la acest SVM este posibilă numai dacă se ignoră calea SVM-ului.

Pe lângă algoritmii de conectare SVM, poți reglementa conectareaa Light Agents la SVM-uri utilizând etichete.

Cum se configurează algoritmul de selectare a SVM-ului pentru Light Agent în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Modul Light Agent** → **Algoritm selectare SVM**.
4. Selectează algoritmul:
   - **Utilizează algoritmul standard de selectare a SVM**. Light Agent selectează SVM-urile implementate în același hipervizor.
   - **Utilizează algoritmul standard de selecție SVM**. Light Agent selectează SVM-urile implementate în tipul de cale SVM selectat (în mod implicit, **Hipervizor**).
5. Dacă este necesar, selectează locațiile SVM pentru algoritmul de selectare SVM extins:
   - **Hipervizor**. Light Agent selectează pentru conectare un SVM care corespunde unui anumit criteriu (în funcție de tipul infrastructurii virtuale):
     - SVM-urile sunt implementate în același hipervizor ca și mașina virtuală pe care este instalat Light Agent (într-o infrastructură virtuală pe Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer sau Basis Dynamix Standard).
     - SVM-ul este situat în același grup de servere ca și mașina virtuală pe care este instalat Light Agent (într-o infrastructură virtuală care rulează pe platforma OpenStack sau platforma VK Private Cloud platform).
     - SVM-ul se află pe același nod ca și mașina virtuală pe care este instalat Light Agent (într-o infrastructură virtuală Basis Dynamix Enterprise).

     Dacă nu există SVM-uri disponibile pentru conectare pe același hipervizor sau în același Grup de servere unde se află mașina virtuală p care se află Light Agent, atunci Light Agent nu se conectează la SVM.

- **Cluster**. Light Agent selectează un SVM la care să se conecteze și care îndeplinește criteriile (în funcție de tipul de infrastructură virtuală):

  - SVM-urile sunt implementate în același cluster de hipervizori ca și mașina virtuală pe care este instalat Light Agent (într-o infrastructură virtuală bazată pe Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer sau Basis Dynamix Standard).

  - SVM-urile sunt implementate în același proiect OpenStack ca și mașina virtuală pe care este instalat Light Agent (într-o infrastructură virtuală care rulează pe platforma OpenStack sau platforma VK Private Cloud).

  - SVM-ul este situat în aceeași zonă ca și mașina virtuală pe care este instalat Light Agent (într-o infrastructură virtuală Basis Dynamix Enterprise).

  Dacă nu există SVM-uri disponibile pentru conectare pe același cluster de hipervizori sau în același proiect OpenStack unde se află mașina virtuală pe care este instalat Light Agent, atunci Light Agent nu se conectează la SVM.

- **Centru de date**. Light Agent selectează un SVM la care să se conecteze și care îndeplinește criteriile (în funcție de tipul de infrastructură virtuală):

  - SVM-urile sunt implementate în același centru de date ca și mașina virtuală pe care este instalat Light Agent (într-o infrastructură virtuală bazată pe Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer sau Basis Dynamix Standard).

  - SVM-urile sunt situate în aceeași zonă de disponibilitate ca și mașina virtuală pe care este instalat Light Agent (într-o infrastructură virtuală care rulează pe platforma OpenStack sau platforma VK Private Cloud).

  - SVM-ul se află în același centru de date ca și mașina virtuală pe care este instalat Light Agent (într-o infrastructură virtuală Basis Dynamix Enterprise).

  Dacă nu există SVM-uri disponibile pentru conectare în același centru de date sau zonă de disponibilitate în care se află mașina virtuală pe care este instalat Light Agent, Light Agent nu se conectează la SVM.

- **Ignoră**. Light Agent ignoră calea SVM pentru conectarea la Serverul de protecție. Light Agents iau în considerare și alte criterii: etichete, numărul de Light Agents conectați la un SVM și așa mai departe.

6. Salvați-vă modificările.

Cum se configurează algoritmul de selectare la SVM pentru Light Agent în Web Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Application settings**.

4. Accesați **Light Agent Mode** → **SVM selection algorithm**.

5. Selectează algoritmul:

- **Use the standard SVM selection algorithm**. Light Agent selectează SVM-urile implementate în același hipervizor.

- **Use the extended SVM selection algorithm**. Light Agent selectează SVM-urile implementate în tipul de cale SVM selectat (în mod implicit, **Hypervisor**).

6. Dacă este necesar, selectează locațiile SVM pentru algoritmul de selectare SVM extins:

- **Hypervisor**. Light Agent selectează un SVM la care să se conecteze și care îndeplinește criteriile (în funcție de tipul de infrastructură virtuală):

  - SVM-urile sunt implementate în același hipervizor ca și mașina virtuală pe care este instalat Light Agent (într-o infrastructură virtuală pe Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer sau Basis Dynamix Standard).

  - SVM-ul este situat în același grup de servere ca și mașina virtuală pe care este instalat Light Agent (într-o infrastructură virtuală care rulează pe platforma OpenStack sau platforma VK Private Cloud platform).

  - SVM-ul se află pe același nod ca și mașina virtuală pe care este instalat Light Agent (într-o infrastructură virtuală Basis Dynamix Enterprise).

  Dacă nu există SVM-uri disponibile pentru conectare pe același hipervizor sau în același Grup de servere unde se află mașina virtuală p care se află Light Agent, atunci Light Agent nu se conectează la SVM.

- **Cluster**. Light Agent selectează un SVM la care să se conecteze și care îndeplinește criteriile (în funcție de tipul de infrastructură virtuală):

  - SVM-urile sunt implementate în același cluster de hipervizori ca și mașina virtuală pe care este instalat Light Agent (într-o infrastructură virtuală bazată pe Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer sau Basis Dynamix Standard).

  - SVM-urile sunt implementate în același proiect OpenStack ca și mașina virtuală pe care este instalat Light Agent (într-o infrastructură virtuală care rulează pe platforma OpenStack sau platforma VK Private Cloud).

  - SVM-ul este situat în aceeași zonă ca și mașina virtuală pe care este instalat Light Agent (într-o infrastructură virtuală Basis Dynamix Enterprise).

  Dacă nu există SVM-uri disponibile pentru conectare pe același cluster de hipervizori sau în același proiect OpenStack unde se află mașina virtuală pe care este instalat Light Agent, atunci Light Agent nu se conectează la SVM.

- **Data center**. Light Agent selectează un SVM la care să se conecteze și care îndeplinește criteriile (în funcție de tipul de infrastructură virtuală):

  - SVM-urile sunt implementate în același centru de date ca și mașina virtuală pe care este instalat Light Agent (într-o infrastructură virtuală bazată pe Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer sau Basis Dynamix Standard).

  - SVM-urile sunt situate în aceeași zonă de disponibilitate ca și mașina virtuală pe care este instalat Light Agent (într-o infrastructură virtuală care rulează pe platforma OpenStack sau platforma VK Private Cloud).

  - SVM-ul se află în același centru de date ca și mașina virtuală pe care este instalat Light Agent (într-o infrastructură virtuală Basis Dynamix Enterprise).

  Dacă nu există SVM-uri disponibile pentru conectare în același centru de date sau zonă de disponibilitate în care se află mașina virtuală pe care este instalat Light Agent, Light Agent nu se conectează la SVM.

- **Ignore**. Light Agent ignoră calea SVM pentru conectarea la Serverul de protecție. Light Agents iau în considerare și alte criterii: etichete, numărul de Light Agents conectați la un SVM și așa mai departe.

7. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se configurează algoritmul de selectare la SVM pentru Light Agent în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul .

2. În fereastra de setări a aplicației, în **Modul Light Agent** fă clic pe opțiunea **Setări descoperire SVM**.

3. Selectează algoritmul:

   - **Utilizează algoritmul standard de selectare a SVM-ului**. Light Agent selectează SVM-urile implementate în același hipervizor.

   - **Utilizează algoritmul standard de selecție SVM**. Light Agent selectează SVM-urile implementate în tipul de cale SVM selectat (în mod implicit, **Hipervizor**).

4. Dacă este necesar, selectează locațiile SVM pentru algoritmul de selectare SVM extins:

   - **Hipervizor**. Light Agent selectează un SVM la care să se conecteze și care îndeplinește criteriile (în funcție de tipul de infrastructură virtuală):

     - SVM-urile sunt implementate în același hipervizor ca și mașina virtuală pe care este instalat Light Agent (într-o infrastructură virtuală pe Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer sau Basis Dynamix Standard).

     - SVM-ul este situat în același grup de servere ca și mașina virtuală pe care este instalat Light Agent (într-o infrastructură virtuală care rulează pe platforma OpenStack sau platforma VK Private Cloud platform).

     - SVM-ul se află pe același nod ca și mașina virtuală pe care este instalat Light Agent (într-o infrastructură virtuală Basis Dynamix Enterprise).

     Dacă nu există SVM-uri disponibile pentru conectare pe același hipervizor sau în același Grup de servere unde se află mașina virtuală p care se află Light Agent, atunci Light Agent nu se conectează la SVM.

- **Cluster**. Light Agent selectează un SVM la care să se conecteze și care îndeplinește criteriile (în funcție de tipul de infrastructură virtuală):

  - SVM-urile sunt implementate în același cluster de hipervizori ca și mașina virtuală pe care este instalat Light Agent (într-o infrastructură virtuală bazată pe Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer sau Basis Dynamix Standard).

  - SVM-urile sunt implementate în același proiect OpenStack ca și mașina virtuală pe care este instalat Light Agent (într-o infrastructură virtuală care rulează pe platforma OpenStack sau platforma VK Private Cloud).

  - SVM-ul este situat în aceeași zonă ca și mașina virtuală pe care este instalat Light Agent (într-o infrastructură virtuală Basis Dynamix Enterprise).

  Dacă nu există SVM-uri disponibile pentru conectare pe același cluster de hipervizori sau în același proiect OpenStack unde se află mașina virtuală pe care este instalat Light Agent, atunci Light Agent nu se conectează la SVM.

- **Centru de date**. Light Agent selectează un SVM la care să se conecteze și care îndeplinește criteriile (în funcție de tipul de infrastructură virtuală):

  - SVM-urile sunt implementate în același centru de date ca și mașina virtuală pe care este instalat Light Agent (într-o infrastructură virtuală bazată pe Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer sau Basis Dynamix Standard).

  - SVM-urile sunt situate în aceeași zonă de disponibilitate ca și mașina virtuală pe care este instalat Light Agent (într-o infrastructură virtuală care rulează pe platforma OpenStack sau platforma VK Private Cloud).

  - SVM-ul se află în același centru de date ca și mașina virtuală pe care este instalat Light Agent (într-o infrastructură virtuală Basis Dynamix Enterprise).

  Dacă nu există SVM-uri disponibile pentru conectare în același centru de date sau zonă de disponibilitate în care se află mașina virtuală pe care este instalat Light Agent, Light Agent nu se conectează la SVM.

- **Ignoră**. Light Agent ignoră calea SVM pentru conectarea la Serverul de protecție. Light Agents iau în considerare și alte criterii: etichete, numărul de Light Agents conectați la un SVM și așa mai departe.

5. Salvați-vă modificările.

Distribuirea conexiunilor Light Agents la SVM-uri (etichete)

Mai mulți Light Agents se pot conecta la un SVM. Pentru a echilibra conexiunile Light Agent, poți specifica o listă separată de SVM-uri. Dacă utilizezi un Server de integrare pentru descoperirea SVM, poți utiliza *etichete* pentru a echilibra conexiunile Light Agent la SVM-uri. Adică, pentru un Light Agent poți aloca o listă de SVM-uri pentru conectare folosind o etichetă. Pentru aceasta, trebuie să atribui o etichetă pentru Light Agent și să specifici această etichetă în setările SVM-ului. Pentru detalii despre specificarea etichetelor în setările SVM, consultă Ajutor Kaspersky Security for Virtualization Light Agent.

Exemplu: Soluția Kaspersky Endpoint Detection and Response Optimum este implementată în infrastructura ta pentru gazdele desemnate ale mașinilor virtuale. În acest caz, poți atribui eticheta `[EDROptimum]` la Light Agent pentru a-l face să se conecteze la SVM-urile care au adăugată cheia de licență EDR Optimum (suplimentul EDR Optimum). Ca rezultat, poți utiliza funcționalitatea EDR Optimum pe mașina virtuală pe care este instalat Light Agent. Când conectezi Light Agent la un SVM fără o cheie de licență EDR Optimum, funcționalitatea Kaspersky Endpoint Detection and Response Optimum nu este disponibilă.

Cum se atribuie o etichetă de conexiune la SVM unui Light Agent în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Modul Light Agent → Etichetă conexiune SVM**.
4. Bifează caseta de selectare **Utilizează etichete pentru conectare** și introdu o etichetă de conexiune SVM.

   Pentru o etichetă, poți introduce un șir de text de până la 255 de caractere. Poți folosi orice caracter, cu excepția caracterului `;`.
5. Salvați-vă modificările.

Cum se atribuie o etichetă de conexiune la SVM unui Light Agent în Web Console

1. În fereastra principală a Web Console, selectați **Asset management → Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Light Agent Mode → SVM connection tag**.
5. Bifează caseta de selectare **Use connection tag** și introdu o etichetă de conexiune SVM.

   Pentru o etichetă, poți introduce un șir de text de până la 255 de caractere. Poți folosi orice caracter, cu excepția caracterului `;`.
6. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se atribuie o etichetă de conexiune la SVM unui Light Agent în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra de setări a aplicației, în **Modul Light Agent** fă clic pe opțiunea **Etichetă conexiune SVM**.
3. Bifează caseta de selectare **Utilizează etichete pentru conectare** și introdu o etichetă de conexiune SVM.

   Pentru o etichetă, poți introduce un șir de text de până la 255 de caractere. Poți folosi orice caracter, cu excepția caracterului `;`.
4. Salvați-vă modificările.

Protecția conexiunii dintre un Light Agent și SVM

Poți configura criptarea conexiunii dintre Light Agents și Serverul de protecție. Pentru aceasta, trebuie să activezi criptarea canalului de date dintre Light Agent și Serverul de protecție în setările Protection Server de pe SVM și în setările Light Agent.

Un Light Agent pentru care este activată protecția conexiunii se poate conecta numai la SVM-uri pentru care este activată criptarea canalului de date dintre Light Agent și Serverul de protecție. Un Light Agent pentru care protecția conexiunii este dezactivată se poate conecta numai la SVM-uri pentru care criptarea canalului este dezactivată sau este permisă o conexiune nesigură între Serverul de protecție și Light Agent.

Pentru detalii despre configurarea protecției conexiunii pe Serverul de protecție, consultă Ajutor Kaspersky Security for Virtualization Light Agent.

Protejarea conexiunii prin criptare poate reduce performanța Kaspersky Security for Virtualization Light Agent.

Cum se configurează protecția conexiunii într-un Light Agent în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Modul Light Agent** → **Protecție conexiune**.
4. Bifați caseta de selectare **Criptează canalul de date dintre Light Agent și Serverul de protecție**.
5. Salvați-vă modificările.

Cum se configurează protecția conexiunii într-un Light Agent în Web Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.
   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **Light Agent Mode** → **Connection protection**.
5. Bifați caseta de selectare **Encrypt data channel between Light Agent and the Protection Server**.
6. Pentru a aplica politica pe computere, închideți pictogramele cu lacăt și salvați modificările.

Cum se configurează protecția conexiunii într-un Light Agent în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul .
2. În fereastra de setări a aplicației, în **Modul Light Agent** fă clic pe opțiunea **Protecție conexiune**.

3. Bifați caseta de selectare **Criptează canalul de date dintre Light Agent și Serverul de protecție**.

4. Salvați-vă modificările.

Activarea Light Agent

Dacă Kaspersky Endpoint Security este utilizat în modul Light Agent pentru a proteja mediile virtuale, nu este necesar să activezi aplicația separat. Pentru a activa aplicația, trebuie să adaugi o cheie de licență la SVM. Puteți adăuga o cheie de licență la SVM folosind activitatea specială din consola Kaspersky Security Center. Nu poți gestiona cheile de licență în interfața Light Agent, cu toate acestea, poți vizualiza informații despre licență (vezi figura de mai jos). De asemenea, poți vizualiza informațiile de licențiere a Light Agent în linia de comandă (vezi instrucțiunile de mai jos). Light Agent primește aceste informații de la SVM. Pentru detalii despre activarea soluției și gestionarea cheilor de licență, consultă Ajutor Kaspersky Security for Virtualization Light Agent.

Pentru a vizualiza informațiile de licențiere pentru Light Agent:

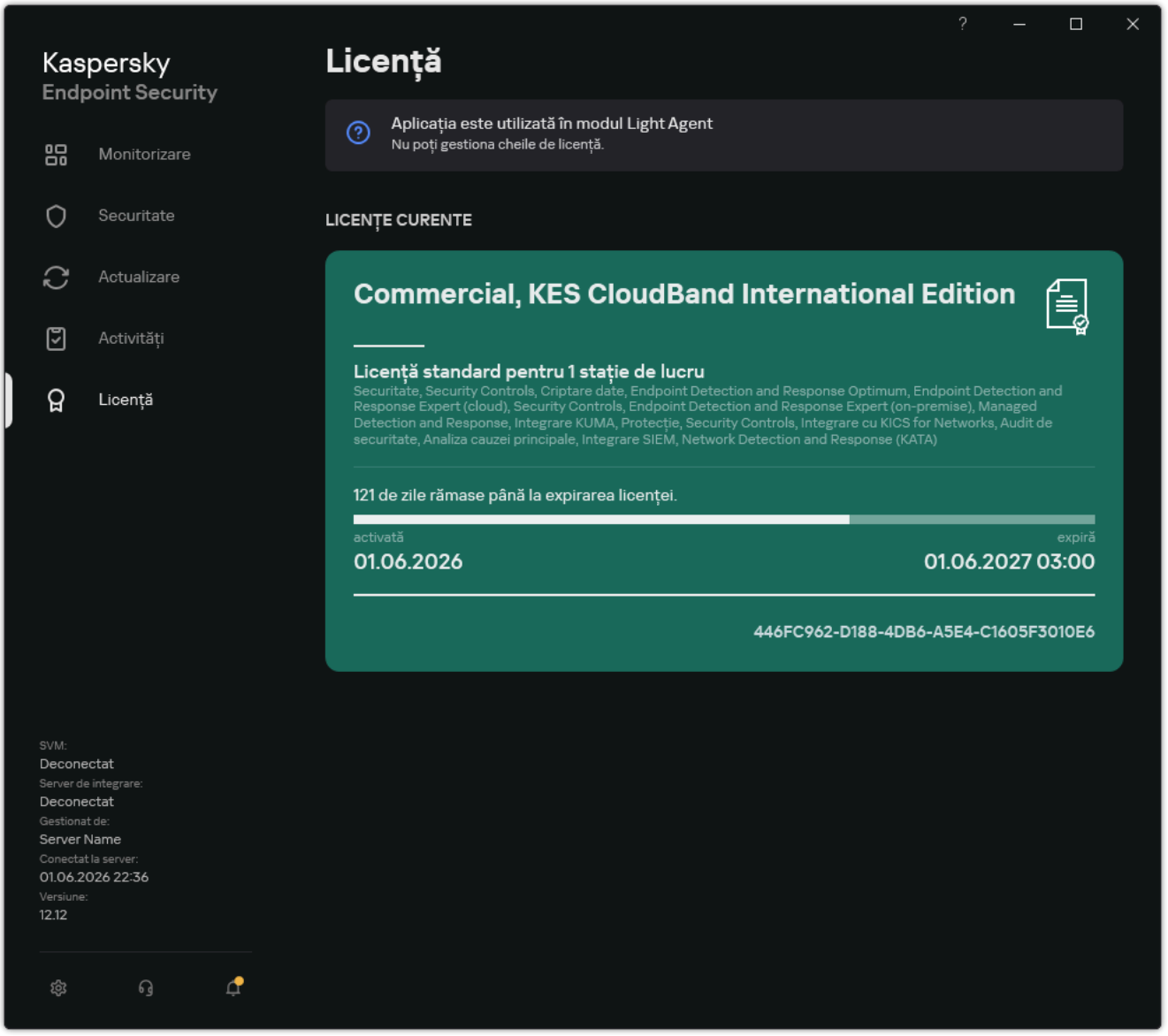
1. Execută interpretorul liniei de comandă (cmd) ca administrator.

2. Deschideți directorul în care se află fișierul executabil Kaspersky Endpoint Security.

3. Execută următoare comandă:

```
avp.com LICENSE /CHECK
```

Ca rezultat, Kaspersky Endpoint Security afișează informații despre licență: adresa SVM-ului la care este conectat Light Agent, numărul de zile până la expirarea licenței și alte informații. Dacă întâmpini probleme la activarea Light Agent, consultă Baza de cunoștințe a Suportului tehnic.



Fereastra Licențiere

Ghid de migrare de la KSVLA Light Agent la KES Light Agent

Kaspersky Security for Virtualization 5.2 Light Agent include componenta Light Agent for Windows 5.2 (denumită în continuare și „KSVLA Light Agent"). În Kaspersky Security for Virtualization Light Agent 6.2, Kaspersky Endpoint Security în modul Light Agent este utilizat ca și componentă Light Agent. Pentru a actualiza soluția la versiunea 6.2, trebuie să migrezi de la KSVLA Light Agent 5.2 la Kaspersky Endpoint Security în modul Light Agent (denumit în continuare și „KES Light Agent"). Pentru detalii despre actualizarea versiunii soluției Kaspersky Security for Virtualization Light Agent, consultă Ajutor Kaspersky Security for Virtualization Light Agent.

Cerințe software

Înainte de a începe migrarea de la KSVLA Light Agent la KES Light Agent, asigură-te că mașina ta virtuală îndeplinește cerințele hardware și software ale Kaspersky Endpoint Security for Windows. Listele cu versiunile de sisteme de operare acceptate sunt diferite pentru KES și KSWS. De exemplu, KES nu este compatibil cu serverele care rulează Windows Server 2003.

Cerințe minime de software pentru migrarea de la KSVLA Light Agent la KES Light Agent:

- Kaspersky Endpoint Security pentru Windows 12.8.
- Kaspersky Security for Virtualization Light Agent 6.2 (inclusiv componentele Server de protecție și Server de integrare).
- Kaspersky Security Center 14.2

  Dacă aveți instalată o versiune anterioară a Kaspersky Security Center, actualizați-o la 14.2 sau la o versiune ulterioară. În această versiune a Kaspersky Security Center, expertul de conversie în bloc a politicilor și sarcinilor vă permite să migrați politicile într-un profil, mai degrabă decât într-o politică. În această versiune a Kaspersky Security Center, expertul de conversie în loc a politicilor și sarcinilor vă permite, de asemenea, să migrați o gamă mai largă de setări de politici.

Etapele de migrare

Migrarea de la KSVLA Light Agent la KES Light Agent se realizează semi-automat. Acest lucru este necesar din cauza arhitecturilor diferite ale aplicațiilor.

Migrează de la KSVLA Light Agent la KES Light Agent în următoarea ordine:

1. **Migrează activitățile și politicile KSVLA Light Agent**

   Pentru a migra setările politicilor, trebuie să execuți Expertul de conversie în bloc a politicilor și activităților (expertul de migrare). După migrarea setărilor politicii, trebuie să configurezi manual setările pe care expertul de migrare nu le poate migra automat (de exemplu, setările de actualizare a bazei de date). După migrare, se recomandă, de asemenea, să verificați dacă expertul de migrare a migrat corect toate setările.

   Dacă protecția prin parolă este activată pentru a restricționa accesul la KSVLA Light Agent, înainte de a instala KES Light Agent, trebuie să dezactivezi Protecția prin parolă în politica KSVLA Light Agent. Nu poți introduce parola de dezinstalare în setările pachetului de instalare KES Light Agent. După finalizarea instalării KES Light Agent peste KSVLA Light Agent, trebuie să activezi Protecția prin parolă în politica KES.

2. **Instalează Kaspersky Endpoint Security în modul Light Agent**

   Poți instala KES Light Agent în următoarele moduri:

   - Instalarea KES Light Agent după eliminarea KSVLA Light Agent (recomandat)
   - Instalarea KES Light Agent peste KSVLA Light Agent

3 Confirmați că aplicația este în stare de funcționare după migrare

După migrarea de la KSVLA Light Agent la KES Light Agent, asigură-te că aplicația funcționează corect. Activează politica convertită. Verifică starea mașinii virtuale în Kaspersky Security Center (ar trebui să fie *OK*). Asigură-te că nu sunt raportate erori pentru aplicație, verifică și ora ultimei conectări la SVM și starea protecției mașinii virtuale. Nu trebuie să activezi Light Agent deoarece cheia de licență este adăugată la SVM.

Instalarea KES Light Agent în loc de KSVLA Light Agent

Poți instala KES Light Agent în următoarele moduri:

- Instalarea KES Light Agent după eliminarea KSVLA Light Agent (recomandat)
- Instalarea KES Light Agent peste KSVLA Light Agent

Eliminarea KSVLA Light Agent

Poți elimina aplicația la distanță, folosind activitatea *Install application remotely* local, pe mașina virtuală, sau în șablonul mașinii virtuale. După eliminarea KSVLA Light Agent, poate fi necesară repormirea mașinii virtuale.

După eliminarea KSVLA Light Agent, instalează KES Light Agent utilizând orice metodă potrivită.

Instalarea Kaspersky Endpoint Security

Dacă protecția prin parolă este activată pentru a restricționa accesul la KSVLA Light Agent, înainte de a instala KES Light Agent, trebuie să dezactivezi Protecția prin parolă în politica KSVLA Light Agent. Nu poți introduce parola de dezinstalare în setările pachetului de instalare KES Light Agent. După finalizarea instalării KES Light Agent peste KSVLA Light Agent, trebuie să activezi Protecția prin parolă în politica KES.

Când instalezi Kaspersky Endpoint Security, trebuie să selectezi modul **Light Agent pentru protejarea mediilor virtuale**. Înainte de a instala KES Light Agent pe o mașină virtuală, programul de instalare detectează KSVLA Light Agent ca software incompatibil și îl elimină. Migrarea configurației KSVLA Light Agent nu este acceptată. Adică, atunci când instalezi KES Light Agent, setul de componente ce trebuie instalat este determinat de opțiunile selectate de tine în proprietățile pachetului de instalare sau în expertul de instalare. După eliminarea KSVLA Light Agent, trebuie să repornești mașina virtuală.

Setările și activitățile KSVLA Light Agent nu sunt migrate atunci când instalezi KES Light Agent. Pentru a migra setările și activitățile, executați Expertul de conversie în bloc a politicilor și activităților.

Puteți verifica lista componentelor instalate în secțiunea **Securitate** a interfeței aplicației, utilizând comanda `status` sau în consola Kaspersky Security Center din proprietățile computerului. Puteți modifica setul de componente după instalare utilizând opțiunea *Modificare componente ale aplicației*.

Corespondența componentelor KSVLA Light Agent și KES Light Agent

Seturile de componente ale KSVLA Light Agent și KES Light Agent sunt practic aceleași. KES Light Agent are mai multe setări decât KSVLA Light Agent. După migrare, noile setări au valori implicite.

Corespondența componentelor KSVLA Light Agent și KES Light Agent

Light Agent 5.2	KES Light Agent
Scan kernel	Nucleu aplicație
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	Application Control
Web Control	Control Web
Device Control	Control dispozitive
System Watcher	În Kaspersky Endpoint Security, această componentă este împărțită în următoarele componente: • Exploit Prevention • Behavior Detection • Remediation Engine
System Integrity Monitoring	Monitorizare integritate sistem
Integration with Kaspersky Endpoint Agent	*(nu sunt acceptate)* Începând cuKaspersky Endpoint Security for Windows 11.9.0, pachetul de distribuție Kaspersky Endpoint Agent nu mai face parte din kitul de distribuție.
AMSI Protection	Protecție AMSI

Migrarea activităților și politicilor KSVLA Light Agent

Poți migra setările politicilor și activităților KSVLA Light Agent utilizând Expertul de conversie în loturi a politicilor și activităților (denumit în continuare „Asistent de migrare").

Asistentul de migrare pentru KSVLA Light Agent este disponibil numai în consola de administrare (MMC). Politica și setările activităților nu pot fi migrate în Web Console și Cloud Console.

Următoarele considerații speciale sunt implicate în migrarea politicilor și a activităților:

- O nouă politică poartă numele *<Policy> (convertit)*.
- Noua politică are starea *Inactive policy*.
- Interzicerea modificării setărilor („lacătul") nu este migrată. Expertul de migrare setează valorile implicite.
- Profilurile politicilor nu sunt migrate. Trebuie să adaugi manual profilurile politicii.

- Gestionare îmbunătățită a zonelor de încredere. În KSVLA Light Agent, poți adăuga excluderi predefinite numai la crearea unei politici. Ulterior, în proprietățile politicii, poți configura excluderi predefinite adăugate anterior sau să adaugi manual excluderi. Nu poți adăuga excluderi predefinite în proprietățile politicii. În KES Light Agent, excluderile predefinite sunt disponibile atât în timpul creării politicii, cât și în proprietățile politicii create. De asemenea, poți selecta excluderi predefinite în pachetul de instalare.

- Configurația interfeței cu utilizatorul aplicației din Kaspersky Endpoint Security a fost mutată din programul de instalare în politică. Dacă ai nevoie, de exemplu, să ascunzi interfața cu utilizatorul a aplicației, gestionează setările politicii.

- Seturile de funcționalități pentru configurarea controlului accesului bazat pe drepturi (RBAC) sunt diferite în Kaspersky Endpoint Security și KSVLA Light Agent. Trebuie să configurezi de la zero drepturile de acces ale utilizatorului la zonele funcționale.

Cum să utilizezi Expertul de conversie în bloc a politicilor și activităților pentru a migra setările politicilor KSVLA Light Agent

1. În Consola de administrare, selectați Server de administrare și faceți clic dreapta pentru a deschide meniul contextual.

2. Selectați **All tasks** → **Policies and tasks batch conversion wizard**.

Expertul de conversie în loturi a politicilor și activităților va începe. Urmează instrucțiunile din expert.

Pasul 1. Selectarea aplicației pentru care doriți să convertiți politicile și activităților

La acest pas, trebuie să selectați Kaspersky Endpoint Security for Windows. Mergeți la pasul următor.

Pasul 2. Conversia politicilor

Selectați politica Kaspersky Security for Virtualization 5.2 Light Agent for Windows pe care dorești să o convertești. Mergeți la pasul următor.

Expertul de migrare va începe apoi să efectueze conversia politicilor. În timpul conversiei, Expertul de migrare îți solicită să acceptați condițiile Declarației KSN. O nouă politică poartă numele *<Policy> (convertit)*.

Pasul 3. Conversia activităților

Expertul pentru migrare creează noi activități pentru Kaspersky Endpoint Security for Windows. În lista de activități, selectează activitățile KSVLA Light Agent pe care dorești să le creezi pentru Kaspersky Endpoint Security. Noile activități vor fi denumite *<Nume activitate> (convertită)*. Mergeți la pasul următor.

Pasul 4. Finalizarea expertului

Ieșiți din Expert.

După migrarea unei politici, trebuie să deschizi proprietățile politicii, să verifici setările acesteia și să salvezi politica. Dacă nu parcurgi acești pași, KES Light Agent poate ignora politica convertită.

Acordă o atenție deosebită migrării setărilor conexiunii SVM a Light Agent, a listelor de excludere, aplicațiilor de încredere, adreselor web de încredere, regulilor Application Control.

Migrarea configurației [KSVLA Light Agent+KEA] la configurația [KES Light Agent+agent încorporat]

Pentru a sprijini utilizarea Kaspersky Endpoint Security for Windows ca parte a EDR (KATA), EDR Optimum, Kaspersky Sandbox, la aplicație a fost adăugat un agent încorporat. Nu mai aveți nevoie de aplicația Kaspersky Endpoint Agent pentru a utiliza aceste soluții.

La migrarea de la KSVLA Light Agent la KES Light Agent, soluțiile EDR (KATA), EDR Optimum, Kaspersky Sandbox continuă să funcționeze cu agenții încorporați Kaspersky Endpoint Security. În plus, Kaspersky Endpoint Agent va fi eliminat din computer.

Înainte de a migra de la KSVLA Light Agent la KES Light Agent, trebuie să actualizezi toate componentele Kaspersky Security for Virtualization la versiunea 6.2, inclusiv componentele Server de protecție și Server de integrare. Pentru detalii despre actualizarea versiunii soluției Kaspersky Security for Virtualization Light Agent, consultă Ajutor Kaspersky Security for Virtualization Light Agent.

Migrarea configurației [KSVLA Light Agent+KEA] la [KES Light Agent+agent încorporat] implică pașii următori:

1. **Migrarea politicii și a activităților**

   Migrarea politicilor și activităților [KSVLA Light Agent+KEA] la [KES+agent încorporat] implică pașii următori:

   1. Migrarea politicilor și activităților de la KSVLA Light Agent la KES Light Agent utilizând Expertul de conversie în blocuri a politicilor și activităților (disponibil numai în Consola de administrare (MMC)).

      Ca rezultat, este creată o nouă politică cu numele *<Politică> (convertit)*. Sunt create și noi activități KES cu numele *<Nume activitate> (convertit)*.

   2. Migrarea politicilor și activităților de la KEA la KES folosind expertul pentru migrarea de la Kaspersky Endpoint Agent (disponibil numai în Web Console și Cloud Console).

      Ca rezultat, este creată o nouă politică cu numele *<Numele politicii Kaspersky Endpoint Security> &<Numele politicii Kaspersky Endpoint Agent>*. Sunt create, de asemenea, activități noi și activități KES.

2. **Migrarea de la KSVLA Light Agent la KES Light Agent**

   Migrarea de la KSVLA Light Agent la KES Light Agent implică instalarea KES Light Agent în loc de KSVLA Light Agent.

De obicei, administratorii activează component Protecție prin parolă pentru a restricționa accesul la KSVLA Light Agent și KEA. Poți introduce parola de dezinstalare KEA doar în proprietățile activității *Install application remotely*. Pentru migrare, trebuie să dezactivezi Protecție prin parolă pentru KSVLA Light Agent.

Pentru a efectua migrarea, trebuie să selectați componentele necesare pentru a accepta soluțiile Detection and Response ca parte a Kaspersky Endpoint Security. După instalarea aplicației, Kaspersky Endpoint Security trece la utilizarea agentului încorporat și elimină Kaspersky Endpoint Agent.

3. **Funcționalitatea de licențiere**

   Dacă aplicația este utilizată în modul Light Agent, nu este necesar să activezi aplicația. Pentru a activa aplicația, trebuie să adaugi o cheie de licență la SVM. De asemenea, trebuie să adaugi cheia de licență pentru activarea funcționalității suplimentare (de exemplu, EDR Optimum) la SVM. Adică, ca parte a migrării, licențierea funcționalității are loc automat.

4. **Verificarea stării componentelor Kaspersky Endpoint Detection and Response Optimum și Kaspersky Sandbox**

   Dacă după upgrade componenta are starea *Critical* în consola Kaspersky Security Center:

   - asigurați-vă că Agentul de rețea versiunea 13.2 sau o versiune ulterioară este instalată pe computer.
   - Verificați starea de funcționare a agentului încorporat, vizualizând *Report on status of application components*. Dacă o componentă are starea *Not installed*, instalați componenta, utilizând activitatea *Change application components*.
   - Asigurați-vă că acceptați Declarația Kaspersky Security Network în noua politică a Kaspersky Endpoint Security for Windows.
   - Asigurați-vă că funcționalitatea EDR Optimum este activată utilizând *Report on status of application components*. Dacă o componentă are starea *Nu este acoperită de licență*, asigurați-vă că funcționalitatea de distribuire automată a cheii de licență a componentei EDR Optimum este activată.
   - Verifică starea conexiunii mașinii virtuale la SVM. Poți obține informații despre starea conexiunii Light Agent la SVM în Kaspersky Endpoint Security sau folosind comanda aplicației.

Gestionarea aplicației din linia de comandă

Puteți gestiona Kaspersky Endpoint Security din linia de comandă. Poți vizualiza lista de comenzi pentru gestionarea aplicației executând comanda `avp.com HELP`. Pentru a citi despre sintaxa unei anumite comenzi, introduceți `avp.com HELP <command>`.

Caracterele speciale din cadrul comenzii trebuie omise. Pentru a omite caracterele `&`, `|`, `(`, `)`, `<`, `>`, `^`, folosiți caracterul `^` (de exemplu, pentru a utiliza caracterul `&`, introduceți `^&`). Pentru a omite caracterul `%`, introduceți `%%`.

Alternativele la valoare `1` sunt valorile `yes`, `on`, `enable`, `enabled` și `true`. Alternativele la valoare `0` sunt valorile `no`, `off`, `disable`, `disabled` și `false`.

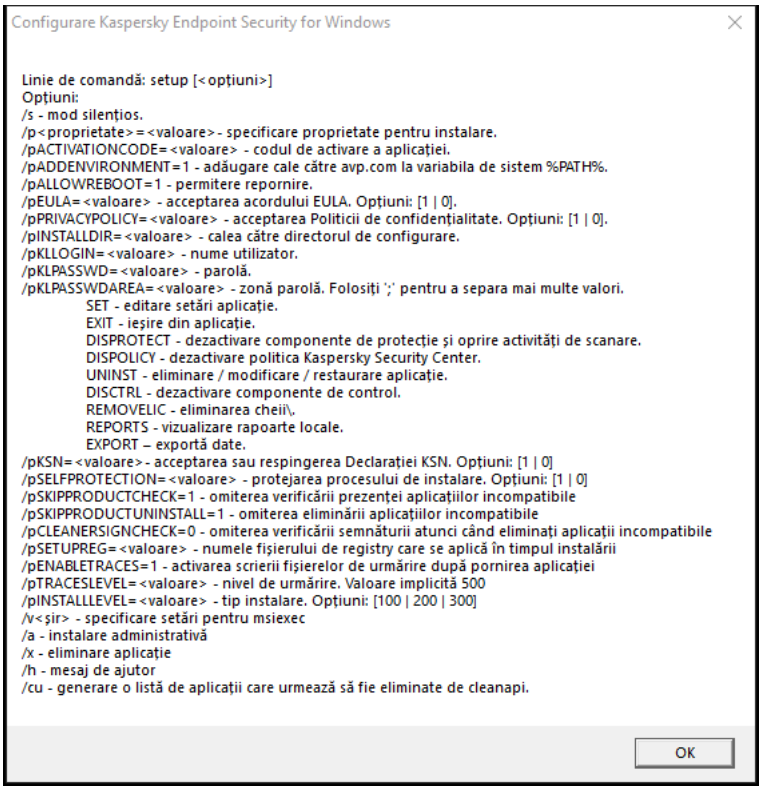
Setup. Instalarea aplicației

Aplicația Kaspersky Endpoint Security poate fi instalată din linia de comandă într-unul din următoarele moduri:

- În mod interactiv, folosind Expertul de configurare a aplicației.
- În modul silențios. După pornirea instalării în modul silențios, nu este nevoie de implicarea ta în procesul de instalare (instalare silențioasă). Pentru a instala aplicația în modul silențios, utilizați tastele `/s` și `/qn`.

  Înainte de a instala aplicația în modul silențios, vă rugăm să deschideți și să citiți Acordul de licență pentru utilizatorul final și textul Politicii de confidențialitate. Acordul de licență pentru utilizatorul final și textul Politicii de confidențialitate sunt incluse în Kit de distribuție Kaspersky Endpoint Security. Puteți continua să instalați aplicația numai dacă ați citit, ați înțeles și ați acceptat prevederile și termenii Acordului de licență pentru utilizatorul final, înțelegeți și sunteți de acord că datele dvs. vor fi prelucrate și transmise (inclusiv țărilor terțe) în conformitate cu Politica de confidențialitate și ați citit și înțeles pe deplin Politica de confidențialitate. Dacă nu acceptați prevederile și termenii Acordului final de licență pentru utilizatorul final și Politica de confidențialitate, vă rugăm să nu instalați sau să utilizați Kaspersky Endpoint Security.

Poți vizualiza lista de comenzi pentru instalarea aplicației executând comanda `/h`. Pentru a obține ajutor cu privire la sintaxa comenzii de instalare, tastați `setup_kes.exe /h`. Ca rezultat, programul de instalare afișează o fereastră cu o descriere a opțiunilor de comandă (vezi figura de mai jos).



Descrierea opțiunilor comenzii de instalare

Pentru a instala aplicația sau a face upgrade unei versiuni anterioare a aplicației:

1. Executați interpretorul de linii de comandă (cmd.exe) ca administrator.
2. Deschide directorul în care se află pachetul de distribuție pentru Kaspersky Endpoint Security.
3. Execută următoare comandă:

```
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]
```

sau

```
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]
```

Ca rezultat, aplicația este instalată pe computer. Poți confirma faptul că aplicația este instalată și să verifici setările aplicației inițiind comanda `status`.

`EULA=1`	Acceptarea termenilor Acordului de licență pentru utilizatorul final. Textul Acordului de licență este inclus în kitul de distribuire al Kaspersky Endpoint Security. Acceptarea termenilor Acordului de licență pentru utilizatorul final este necesară pentru instalarea aplicației sau pentru efectuarea unui upgrade la versiunea aplicației.
`PRIVACYPOLICY=1`	Acceptarea Politicii de confidențialitate. Textul Politicii de confidențialitate este inclus în kitul de distribuire Kaspersky Endpoint Security. Pentru a instala aplicația sau pentru a face upgrade la versiunea aplicației, trebuie să acceptați Politica de confidențialitate.
`KSN`	Acordul sau refuzul de a participa în Kaspersky Security Network (KSN). Dacă pentru acest parametru nu este setată nicio valoare, Kaspersky Endpoint Security vă va solicita să confirmați consimțământul sau refuzul de a participa la KSN la prima pornire a aplicației Kaspersky Endpoint Security. Valori disponibile: • `1` – acord de participare la KSN. • `0` – refuz de a participa la KSN (valoare implicită). Pachetul de distribuție Kaspersky Endpoint Security este optimizat pentru utilizare cu Kaspersky Security Network. Dacă ați optat să nu participați la Kaspersky Security Network, trebuie să actualizați Kaspersky Endpoint Security imediat după finalizarea instalării.
`CONFIGPATH=<path to the configuration file>`	Instalarea aplicației cu setări predefinite. Pentru aceasta, trebuie să încarci un fișier care definește setările pentru aplicația Kaspersky Endpoint Security. Poți crea un fișier de configurare în interfața locală a aplicației.
`ALLOWREBOOT=1`	Se repornește automat computerul, dacă este necesar, după instalarea sau upgrade-ul aplicației. Dacă nu este setată nicio valoare pentru acest parametru, repornirea automată a computerului este blocată. Repornirea nu este necesară atunci când instalezi Kaspersky Endpoint Security. Repornirea este necesară numai dacă trebuie să elimini aplicații incompatibile înainte de instalare. Repornirea poate fi necesară și atunci când actualizezi versiunea aplicației.
`SKIPPRODUCTCHECK=1`	Dezactivează verificarea pentru software-ul instalat. Lista programelor software care pot cauza probleme de incompatibilitate este disponibilă în fișierul incompatible.txt, care este inclus în kitul de distribuție. Dacă nu este setată nicio valoare pentru acest parametru și este detectat un software din listă, instalarea aplicației Kaspersky Endpoint Security va fi oprită.
`SKIPPRODUCTUNINSTALL=1`	Dezactivează eliminarea automată a software-ului detectat din lista incompatible.txt. Dacă nu este setată nicio valoare pentru acest parametru, Kaspersky Endpoint Security încearcă să elimine software-ul care poate cauza probleme de compatibilitate. Eliminarea automată a software-ului incompatibil nu poate fi activată când se instalează Kaspersky Endpoint Security folosind programul de instalare msiexec. Pentru a elimina automat software-ul care poate cauza probleme de compatibilitate, utilizează fișierul setup_kes.exe.
`CLEANERSIGNCHECK=0|1`	Verificarea semnăturilor digitale ale fișierelor software detectate din lista incompatible.txt. Pentru a elimina software-ul, Kaspersky Endpoint Security rulează fișierul de instalare a software-ului. Dacă fișierul de instalare nu are o semnătură digitală, Kaspersky Endpoint Security consideră că fișierul nu este de încredere și oprește eliminarea software-ului pentru a evita executarea unui cod potențial rău intenționat. Dacă aplicația nu poate verifica semnătura digitală a fișierului software-ului detectat, instalarea Kaspersky Endpoint Security este oprită cu o eroare. Valoarea implicită este diferită, în funcție de metoda de instalare a software-ului: • `0` înseamnă că verificarea semnăturii digitale este dezactivată (valoarea implicită, dacă este implementată prin Kaspersky Security Center). • `1` înseamnă că verificarea semnăturii digitale este activată (valoarea implicită, dacă aplicația este instalată local).
`STANDALONEMODE=1`	Instalarea aplicației în configurația Endpoint Detection and Response Agent (EDR Agent) pentru integrarea cu soluțiile Kaspersky Endpoint Detection and Response (KATA) sau Kaspersky Endpoint Detection and Response Expert (on-premises). Această configurație este necesară dacă o platformă Endpoint Protection Platform (EPP) terță este implementată în organizația ta împreună cu soluția de clasă Kaspersky Endpoint Detection and Response. Acest lucru face ca Kaspersky Endpoint Security în configurația Endpoint Detection and Response Agent să fie compatibil cu aplicațiile EPP terțe.
`KLLOGIN`	Setează numele de utilizator pentru accesarea caracteristicilor și setărilor aplicației Kaspersky Endpoint Security (componenta Protecție prin parolă). Numele de utilizator se setează împreună cu setările `KLPASSWD` și `KLPASSWDAREA`. În mod implicit este utilizat numele de utilizator KLAdmin.

KLPASSWD	Specifică o parolă pentru accesarea funcțiilor și setărilor Kaspersky Endpoint Security (parola este specificată împreună cu parametrii KLLOGIN și KLPASSWDAREA). Dacă ați specificat o parolă, însă nu ați specificat un nume de utilizator cu parametrul KLLOGIN, se utilizează în mod implicit numele de utilizator KLAdmin.
KLPASSWDAREA	Specifică domeniul parolei pentru accesarea aplicației Kaspersky Endpoint Security. Atunci când un utilizator încearcă să efectueze o acțiune care este inclusă în acest domeniu, Kaspersky Endpoint Security solicită acreditările contului utilizatorului (parametrii KLLOGIN și KLPASSWD). Folosiți caracterul ; pentru a specifica mai multe valori. Valori disponibile: • SET – modificare a setărilor aplicației. • EXIT – ieșire din aplicație. • DISPROTECT – dezactivare a componentelor protecției și oprire a activităților de scanare. • DISPOLICY – dezactivare a politicii Kaspersky Security Center. • UNINST – eliminare a aplicației de pe computer. • DISCTRL – dezactivare a componentelor de control. • REMOVELIC – eliminare a cheii. • REPORTS – vizualizare a rapoartelor. • EXPORT – exportarea setărilor aplicației. De exemplu, KLPASSWDAREA=SET;KLPASSWDAREA=UNINST;KLPASSWDAREA=EXIT. Contul KLAdmin are dreptul de a efectua orice acțiune care este protejată prin parolă. Prin urmare, configurarea domeniului de aplicare al parolei pentru contul KLAdmin este imposibilă. Dacă încerci să configurezi domeniul de aplicare al parolei pentru contul KLAdmin, aplicația interzice acțiunile specificate pentru grupul „Oricine”.
PROTECTOSSERVICES	Protecția funcționalității serviciilor sistemului de operare. Protecția serviciilor sistemului de operare împiedică aplicațiile terțe să interfereze cu funcționarea serviciilor sistemului de operare. Printre aceste servicii se numără, de exemplu, serviciul de pornire automată a aplicațiilor. • 1 înseamnă că protecția serviciilor sistemului de operare este activată (valoare implicită). • 0 înseamnă că protecția serviciilor sistemului de operare este dezactivată.
ENABLETRACES	Activarea sau dezactivarea urmăririi aplicațiilor. După ce pornește Kaspersky Endpoint Security, acesta salvează fișierele de urmărire în directorul %ProgramData%\Kaspersky Lab\KES.14.1\Traces. Valori disponibile: • 1 – urmărirea este activată. • 0 – urmărirea este dezactivată (valoare implicită).
TRACESLEVEL	Nivelul de detaliere a urmăririi. Valori disponibile: • 100 (critic). Numai mesaje despre erorile fatale. • 200 (ridicat). Mesaje despre toate erorile, inclusiv erorile fatale. • 300 (diagnosticare). Mesaje despre toate erorile, precum și avertismente. • 400 (important). Toate mesajele de eroare, avertismentele și informațiile suplimentare. • 500 (normal). Mesaje despre toate erorile și avertismentele, precum și informații detaliate despre funcționarea aplicației în modul normal (implicit). • 600 (scăzut). Toate mesajele.
ENABLEAZURESUPPORT	Activarea sau dezactivarea modului de compatibilitate Azure WVD. Valori disponibile: • 1 – Modul de compatibilitate Azure WVD este activat. • 0 – Modul de compatibilitate Azure WVD este dezactivat (valoare implicită). Această funcție asigură afișarea corectă a stării mașinii virtuale Azure în consola Kaspersky Anti Targeted Attack Platform. Pentru a monitoriza performanța computerului, Kaspersky Endpoint Security trimite date de telemetrie către serverele KATA. Telemetria include un ID al computerului (Sensor ID). Modul de compatibilitate Azure WVD permite alocarea unui Sensor ID unic permanent către aceste mașini virtuale. Dacă modul de compatibilitate este dezactivat, Sensor ID se poate schimba după ce computerul este repornit din cauza modului în care funcționează mașinile virtuale Azure. Acest lucru poate face ca duplicate ale mașinilor virtuale să apară pe consolă.
AMPPL	Activează sau dezactivează protecția proceselor aplicației Kaspersky Endpoint Security folosind tehnologia AM-PPL (Antimalware Protected Process Light). Pentru mai multe detalii despre tehnologia AM-PPL, vizitați site-ul web Microsoft. Tehnologia AM-PPL este disponibilă pentru Windows 10 versiunea 1703 (RS2) sau ulterioară și pentru sistemele de operare Windows Server 2019. Valori disponibile: • 1 – protecția proceselor aplicației Kaspersky Endpoint Security folosindu-se tehnologia AM-PPL este activată. • 0 – protecția proceselor aplicației Kaspersky Endpoint Security folosindu-se tehnologia AM-PPL este dezactivată.

UPGRADEMODE	Mod upgrade aplicație: • Seamless înseamnă efectuarea upgrade-ului aplicației cu repornirea computerului (valoare implicită) • Force înseamnă efectuarea upgrade-ului aplicației fără repornire. Poți efectua upgrade-ul aplicației fără repornire începând cu versiunea 11.10.0. Pentru a efectua upgrade-ul unei versiuni anterioare a aplicației, trebuie să repornești computerul. De asemenea, poți instala corecții fără repornire începând cu versiunea 11.11.0. Repornirea nu este necesară atunci când instalezi Kaspersky Endpoint Security. Așadar, modul de actualizare a aplicației va fi specificat în setările aplicației. Poți modifica acest parametru în setările aplicației sau în politică. Când upgrade-ul a instalat deja aplicația, prioritatea parametrului liniei de comandă este mai mică decât cea a parametrului specificat în setările aplicației sau în fișierul setup.ini. De exemplu, dacă modul de upgrade Force este specificat în linia de comandă și modul Seamless este specificat în setările aplicației, upgrade-ul va fi instalat prin repornirea computerului (Seamless).
RESTAPI	Gestionarea aplicației prin API REST. Pentru a gestiona aplicația prin API REST, trebuie să specificați numele de utilizator (parametrul RESTAPI_User). Valori disponibile: • 1 - gestionarea prin API REST este permisă. • 0 - gestionarea prin API REST este blocată (valoarea implicită). Pentru a gestiona aplicația prin API REST, trebuie să fie permisă gestionarea folosind sisteme administrative. Pentru a face acest lucru, setați parametrul AdminKitConnector=1. Dacă gestionați aplicația prin API REST, este imposibil să gestionați aplicația folosind sistemele de administrare ale Kaspersky.
RESTAPI_User	Numele de utilizator al contului domeniului Windows utilizat pentru gestionarea aplicației prin API REST. Gestionarea aplicației prin API REST este disponibilă numai pentru acest utilizator. Introduceți numele de utilizator în formatul <DOMAIN>\<UserName> (de exemplu, RESTAPI_User=COMPANY\Administrator). Puteți selecta un singur utilizator pentru a lucra cu API REST. Adăugarea unui nume de utilizator este o condiție necesară pentru gestionarea aplicației prin API REST.
RESTAPI_Port	Port utilizat pentru gestionarea aplicației prin API REST. Portul 6782 este folosit în mod implicit. Asigurați-vă că portul este liber.
RESTAPI_Certificate	Certificat pentru identificarea solicitărilor (de exemplu, RESTAPI_Certificate=C:\cert.pem). Interacțiunea sigură a Kaspersky Endpoint Security cu clientul REST necesită configurarea identificării solicitării. Pentru aceasta, trebuie să instalați un certificat și ulterior să semnați sarcina fiecărei solicitări.
ADMINKITCONNECTOR	Gestionarea aplicațiilor folosind sisteme de administrare. Sistemele de administrare includ, de exemplu, Kaspersky Security Center. Pe lângă sistemele de administrare Kaspersky, puteți utiliza soluții terțe. Kaspersky Endpoint Security oferă o API în acest scop. Valori disponibile: • 1 - gestionarea aplicațiilor cu ajutorul sistemelor de administrare este permisă (valoare implicită). • 0 - gestionarea aplicațiilor este permisă doar prin interfața locală.
EnableUniqueSensorID	Crearea unui identificator unic de computer (Sensor ID) în timpul instalării sau actualizării aplicației. Sensor ID este utilizat în soluția Kaspersky Anti Targeted Attack Platform pentru a identifica computerele care trimit telemetrie către server. La crearea unui Sensor ID, aplicația folosește un algoritm care ține cont de configurația computerului, cum ar fi numărul de serie al plăcii de bază. În unele cazuri, de exemplu, când se utilizează aplicația într-un mediu virtual, Sensor ID poate fi duplicat. Ca urmare, Kaspersky Anti Targeted Attack Platform nu poate identifica computerul de pe care este trimisă telemetria. Pentru a crea un Sensor ID unic, trebuie să setezi parametrul EnableUniqueSensorID=1. Ca urmare, aplicația va folosi un alt algoritm pentru a crea Sensor ID, care ia în considerare și alte date despre computer. Acest lucru asigură un identificator Sensor ID unic. În mod implicit, parametrul nu este setat. Aplicația moștenește identificatorul Sensor ID în următoarele cazuri: • actualizarea versiunii aplicației; • migrarea configurării [KES+KEA] la [KES+built-in agent]. Ca parte a procesului de reparare a aplicației, programul de instalare încearcă să moștenească Sensor ID. Dacă Sensor ID nu poate fi restaurat, aplicația creează un nou Sensor ID.
SKIPKB5007186CHECK=1	Dezactivarea verificării pentru actualizarea sistemului de operare instalat KB5007186. Înainte de a instala aplicația, programul de instalare verifică actualizările sistemului de operare instalat. Actualizarea KB5007186 se află pe lista actualizărilor sistemului de operare care pot cauza probleme aplicației. Pentru informații detaliate, consultați Baza de cunoștințe pentru suport tehnic. Prin urmare, programul de instalare anulează instalarea dacă această actualizare este descoperită. Pentru a continua instalarea, setează SKIPKB5007186CHECK=1.

Exemplu

```
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
```

După instalarea Kaspersky Endpoint Security, licența de încercare este activată dacă nu ați furnizat un cod de activare în fișierul setup.ini. O licență trial are, de obicei, un termen scurt. După expirarea licenței trial, toate caracteristicile aplicației Kaspersky Endpoint Security sunt dezactivate. Pentru a continua să utilizați aplicația, trebuie să activați aplicația cu o licență comercială utilizând funcția Expert de activare a aplicației sau o comandă specială.

Atunci când instalați aplicația sau efectuați upgrade-ul versiunii aplicației în modul silențios, este acceptată folosirea următoarelor fișiere:

- setup.ini – setări generale ale instalării aplicației.

  Pentru a aplica setări din fișierul setup.ini, plasează acest fișier în directorul care conține pachetul de distribuție Kaspersky Endpoint Security.

- install.cfg – setări legate de funcționarea Kaspersky Endpoint Security

  Pentru a aplica setările din fișierul de configurare install.cfg, trebuie să specifici calea către fișier în următoarea comandă de instalare a aplicației: `CONFIGPATH=<path to the configuration file>`.

- setup.reg – chei de registry.

  Cheile de registru din fișierul setup.reg se scriu în registru numai dacă valoarea `setup.reg` este setată pentru parametrul `SetupReg` în fișierul setup.ini. Fișierul setup.reg este generat de experții de la Kaspersky. Nu este recomandabilă modificarea conținutului acestui fișier. Pentru a aplica setări din fișierul setup.reg, plasează acest fișier în directorul care conține pachetul de distribuție Kaspersky Endpoint Security. De asemenea, puteți pune fișierul setup.reg într-un alt folder. Dacă faceți acest lucru, trebuie să specificați calea către fișier în următoarea comandă de instalare a aplicației: `SETUPREG=<path to the setup.reg file>`.

Setup /x. Eliminarea aplicației

Aplicația Kaspersky Endpoint Security poate fi dezinstalată din linia de comandă într-unul din următoarele moduri:

- În mod interactiv, folosind Expertul de configurare a aplicației.
- În modul silențios. După pornirea dezinstalării în modul silențios, nu este nevoie de implicarea ta în procesul de eliminare (dezinstalare silențioasă). Pentru a dezinstala aplicația în modul silențios, utilizați comutatoarele `/s` și `/qn`.

Pentru a dezinstala aplicația în modul silențios:

1. Executați interpretorul de linii de comandă (cmd.exe) ca administrator.
2. Deschide directorul în care se află pachetul de distribuție pentru Kaspersky Endpoint Security.

3. Execută următoare comandă:

- Dacă procesul de eliminare nu este protejat cu parolă:

  ```
  setup_kes.exe /s /x
  ```

  sau

  ```
  msiexec.exe /x <GUID> /qn
  ```

  `<GUID>` este ID-ul unic al aplicației. Puteți afla codul GUID al aplicației în Baza de cunoștințe pentru suport tehnic sau folosind următoarea comandă:

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

- Dacă procesul de eliminare este protejat cu parolă:

  ```
  setup_kes.exe /pKLLOGIN=<user name> /pKLPASSWD=<password> /s /x
  ```

  sau

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

De asemenea, puteți utiliza parametrul `SAVEQB` pentru a salva fișierele scanate de aplicație și plasate în Copie de rezervă. Copiile de rezervă ale fișierelor sunt stocate în directorul `C:\ProgramData\Kaspersky Lab\KES.14.1\QB`. În mod implicit, salvarea fișierelor în Copie de rezervă este dezactivată (`SAVEQB=0`).

Exemplu

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

msiexec /i. Recuperarea aplicației

La recuperare, aplicația verifică și restabilește integritatea tuturor modulelor aplicației deteriorate și a cheilor de registry de sistem create ca parte a procesului de instalare a aplicației.

Aplicația Kaspersky Endpoint Security poate fi recuperată din linia de comandă într-unul din următoarele moduri:

- În mod interactiv, folosind Expertul de configurare a aplicației.
- În modul silențios. După începerea recuperării în modul silențios, nu este necesară implicarea ta în procesul de recuperare.

Dacă programul de instalare Kaspersky Endpoint Security rulează în modul de recuperare și aplicația nu are nevoie de recuperare, programul de instalare nu face modificări.

Dacă programul de instalare Kaspersky Endpoint Security rulează în modul de recuperare și aplicația nu este instalată, programul de instalare începe procesul de instalare.

Pentru a recupera aplicația în modul silențios:

1. Executați interpretorul de linii de comandă (cmd.exe) ca administrator.
2. Deschide directorul în care se află pachetul de distribuție pentru Kaspersky Endpoint Security.
3. Execută următoare comandă:
   - Dacă procesul de recuperare nu este protejat prin parolă:

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL /qn
     ```

     `<GUID>` este ID-ul unic al aplicației. Puteți afla codul GUID al aplicației în Baza de cunoștințe pentru suport tehnic sau folosind următoarea comandă:

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

   - Dacă procesul de recuperare este protejat prin parolă:

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL KLLOGIN=<user name> KLPASSWD=<password> /qn
     ```

Exemplu

```
msiexec.exe /i {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} REINSTALL=ALL KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

Comenzi AVP

Pentru a gestiona Kaspersky Endpoint Security din linia de comandă:

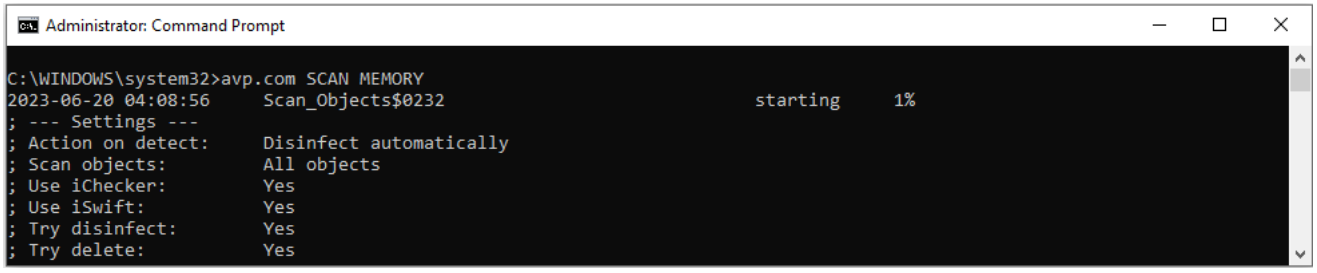
1. Executați interpretorul de linii de comandă (cmd.exe) ca administrator.
2. Deschideți directorul în care se află fișierul executabil Kaspersky Endpoint Security.

   Puteți adăuga calea către fișierul executabil la variabila de sistem %PATH% în timpul instalării aplicației.

3. Utilizează următorul șablon pentru a executa comanda:

```
avp.com <command> [options]
```

Drept urmare, Kaspersky Endpoint Security va executa comanda (a se vedea figura de mai jos).



Gestionarea aplicației din linia de comandă

SCAN. Scanare malware

Executarea activității *Scanare malware*.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Sintaxa de comandă

```
avp.com SCAN [<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>] [/C:<file with scan settings>]
```

Domeniu de scanare	
`<files to scan>`	O listă separată de spațiu de fișiere și directoare. Căile lungi trebuie să fie incluse între ghilimele. Căile scurte (format MS-DOS) nu trebuie să fie incluse între ghilimele. De exemplu: • `"C:\Program Files (x86)\Example Folder"` – cale lungă. • `C:\PROGRA~2\EXAMPL~1` – cale scurtă.
`/ALL`	Executați activitatea *Scanare malware* Kaspersky Endpoint Security scanează următoarele obiecte: • memoria kernel • Obiectele încărcate la pornirea sistemului de operare • sectoarele de boot • Crearea unei copii de rezervă a sistemului de operare • Toate unitățile de disc și amovibile În Kaspersky Endpoint Security for Windows 12.12 e-mailul este exclus din domeniul de scanare al aplicației. Scanarea mesajelor de e-mail primite și trimise este efectuată de componenta Mail Threat Protection. Dacă utilizezi o versiune anterioară a plug-in-ului de administrare, aplicația exclude e-mailurile din domeniul de scanare, chiar dacă politica le include.
`/MEMORY`	Scanați memoria kernel
`/STARTUP`	Scanați obiectele încărcate la pornirea sistemului de operare

`/REMDRIVES`	Scanați unitățile amovibile.
`/FIXDRIVES`	Scanați unitățile de hard disk.
`/NETDRIVES`	Scanați unitățile de rețea.
`/QUARANTINE`	Scanați fișierele din Copia de rezervă a aplicației Kaspersky Endpoint Security.
`/@:<file list.lst>`	Scanați fișierele și directoarele dintr-o listă. Fiecare fișier din listă trebuie să fie pe o linie nouă. Căile lungi trebuie să fie incluse între ghilimele. Căile scurte (format MS-DOS) nu trebuie să fie incluse între ghilimele. De exemplu: • `"C:\Program Files (x86)\Example Folder"` – cale lungă. • `C:\PROGRA~2\EXAMPL~1` – cale scurtă.

Acțiune la detectarea amenințării	
`/i0`	**Informează**. Dacă este selectată această opțiune, Kaspersky Endpoint Security adaugă informațiile despre fișierele infectate în lista de amenințări active la detectarea acestor fișiere.
`/i1`	**Dezinfectează; informează dacă dezinfectarea nu reușește**. Dacă selectați această opțiune, Kaspersky Endpoint Security încearcă automat să dezinfecteze toate fișierele infectate care sunt detectate. Dacă dezinfectarea eșuează, Kaspersky Endpoint Security adaugă informațiile despre fișierele infectate detectate în lista de amenințări active.
`/i2`	**Dezinfectează; șterge dacă dezinfectarea nu reușește**. Dacă selectezi această opțiune, aplicația încearcă automat să dezinfecteze fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, aplicația șterge fișierul. Această acțiune este selectată în mod implicit.
`/i3`	**Șterge dacă dezinfectarea nu reușește**. Ștergeți și fișierele compuse (de exemplu, arhivele) dacă fișierul infectat nu poate fi dezinfectat sau șters.
`/i4`	**Șterge**. Ștergeți și fișierele compuse (de exemplu, arhivele) dacă fișierul infectat nu poate fi șters.

Tipuri de fișiere	
`/fe`	**Fișiere scanate după extensie**. Dacă se activează această setare, aplicația scanează numai fișierele infectabile. Formatul fișierului se determină în funcție de extensia sa.
`/fi`	**Fișiere scanate după format**. Dacă se activează această setare, aplicația scanează numai fișierele infectabile. Înainte de scanarea unui fișier pentru detectarea de cod rău intenționat, se analizează antetul intern al fișierului pentru a se determina formatul fișierului (de exemplu, .txt, .doc sau .exe). De asemenea, scanarea caută fișiere cu anumite extensii de fișiere.
`/fa`	**Toate fișierele**. Dacă se activează această setare, aplicația verifică toate fișierele, fără excepție (toate formatele și toate extensiile). Aceasta este setarea implicită.

Excluderi de la scanare	
`-e:a`	Arhivele RAR, ARJ, ZIP, CAB, LHA, JAR și ICE sunt excluse din domeniul de scanare.
`-e:<file mask>`	Fișierele care se potrivesc cu masca de fișier sunt excluse din domeniul de scanare. De exemplu: • Masca `*.exe` va include toate căile către fișierele care au extensia exe. • Masca `example*` va include toate căile către fișierele denumite EXAMPLE.
`-e:<seconds>`	Fișierele a căror scanare durează mai mult decât limita de timp specificată (în secunde) sunt excluse din domeniul de scanare.
`-es:<megabytes>`	Fișierele care sunt mai mari decât dimensiunea maximă specificată (în megabyți) sunt excluse din domeniul de scanare.

Salvarea evenimentelor într-un mod de fișier raport (numai pentru profilurile Scanare, Program de actualizare și Derulare înapoi)	
`/R:<report file>`	Salvați numai evenimente critice în fișierul raport.
`/RA:<report file>`	Salvați toate evenimentele într-un fișier raport.

Tehnologii de scanare	
`/iChecker=on|off`	Această tehnologie permite creșterea vitezei de scanare excluzând de la scanare anumite fișiere. Fișierele sunt excluse de la scanări utilizând un algoritm special care ia în considerare data lansării bazelor de date Kaspersky Endpoint Security, data celei mai recente scanări a fișierului și orice modificare adusă setărilor scanării. Există limitări ale tehnologiei iChecker: aceasta nu funcționează în cazul fișierelor mari și se aplică numai la fișierele cu o structură pe care aplicația o recunoaște (de exemplu, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP și RAR).
`/iSwift=on|off`	Această tehnologie permite creșterea vitezei de scanare excluzând de la scanare anumite fișiere. Fișierele sunt excluse de la scanări utilizând un algoritm special care ia în considerare data lansării bazelor de date Kaspersky Endpoint Security, data celei mai recente scanări a fișierului și orice modificare adusă setărilor scanării. Tehnologia iSwift reprezintă o versiune îmbunătățită a tehnologiei iChecker și este destinată sistemului de fișiere NTFS.

Setări avansate	
`/C:<file with scan settings>`	Fișier cu setările activității *Scanare malware*. Fișierul trebuie creat manual și salvat în format TXT. Fișierul poate avea următorul conținut: `[<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>]`.

Exemplu

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

UPDATE. Actualizarea bazelor de date și modulelor aplicației

Executarea activității *Actualizarea modulelor bazelor de date și ale aplicațiilor*.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Această comandă nu poate fi executată dacă aplicația este instalată în modul Light Agent.

Sintaxa de comandă

```
avp.com UPDATE [local] ["<update source>"] [/R[A]:<report file>] [/C:<file with update settings>]
```

Setări activitate de actualizare	
`local`	Începerea activității de *Actualizarea modulelor bazelor de date și ale aplicațiilor* care a fost creată automat după ce aplicația a fost instalată. Puteți modifica setările activității de *Actualizarea modulelor bazelor de date și ale aplicațiilor* în interfața aplicației locale sau în consola Kaspersky Security Center. Dacă această setare nu este configurată, Kaspersky Endpoint Security pornește activitatea de *Actualizarea modulelor bazelor de date și ale aplicațiilor* cu setările implicite sau cu setările specificate în comandă. Puteți configura setările activității *Actualizarea modulelor bazelor de date și ale aplicațiilor* după cum urmează: • `UPDATE` pornește activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* cu setările implicite: sursa de actualizare o reprezintă serverele de actualizare, contul este Sistem și alte setări implicite. • `UPDATE local` pornește activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* care a fost creată automat după instalare (activitate predefinită). • `UPDATE <update settings>` pornește activitatea *Actualizarea modulelor bazelor de date și ale aplicațiilor* setările stabilite manual (a se vedea mai jos).

Sursă actualizare	
`"<update source>"`	Adresa unui server HTTP sau FTP sau a unui director partajat cu pachetul de actualizare. Puteți specifica o singură sursă de actualizare. Dacă sursa de actualizare nu este specificată, Kaspersky Endpoint Security utilizează sursa implicită: Serverele de actualizare ale Kaspersky.

Salvarea evenimentelor într-un mod de fișier raport (numai pentru profilurile Scanare, Program de actualizare și Derulare înapoi)	
`/R:<report file>`	Salvați numai evenimente critice în fișierul raport.
`/RA:<report file>`	Salvați toate evenimentele într-un fișier raport.

Setări avansate	
`/C:<file with update settings>`	Fișier cu setările activității *Actualizarea modulelor bazelor de date și ale aplicațiilor*. Fișierul trebuie creat manual și salvat în format TXT. Fișierul poate avea următorul conținut: `["<update source>"] [/R[A]:<report file>]`.

Exemplu

```
avp.com UPDATE local
```

```
avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

ROLLBACK. Derulare înapoi ultima actualizare

Derularea înapoi a ultimei actualizări a bazei de date antivirus. Acest lucru vă permite să derulați înapoi bazele de date și modulele de aplicații la versiunile lor anterioare, atunci când este necesar, de exemplu când noua versiune a bazei de date conține o semnătură nevalidă care face ca aplicația Kaspersky Endpoint Security să blocheze o aplicație sigură.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Această comandă nu poate fi executată dacă aplicația este instalată în modul Light Agent.

Sintaxa de comandă

```
avp.com ROLLBACK [/R[A]:<report file>]
```

Salvarea evenimentelor într-un mod de fișier raport (numai pentru profilurile Scanare, Program de actualizare și Derulare înapoi)	
`/R:<report file>`	Salvați numai evenimente critice în fișierul raport.
`/RA:<report file>`	Salvați toate evenimentele într-un fișier raport.

Exemplu

```
avp.com ROLLBACK /RA:rollback.txt
```

TRACES. Urmărirea

Fișierele de urmărire sunt stocate pe computer cât timp aplicația este în uz și sunt permanent șterse atunci când aplicația este eliminată. Fișierele de urmărire, cu excepția fișierelor de urmărire ale Agentului de Autentificare, sunt stocate în directorul `%ProgramData%\Kaspersky Lab\KES.14.1\Traces`. În mod implicit, urmărirea este dezactivată.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Sintaxa de comandă

```
avp.com TRACES on|off [<tracing level>] [<advanced settings>]
```

Nivel urmărire	
`<tracing level>`	Nivelul de detaliere a urmăririi. Valori disponibile: • `100` (critic). Numai mesaje despre erorile fatale. • `200` (ridicat). Mesaje despre toate erorile, inclusiv erorile fatale. • `300` (diagnosticare). Mesaje despre toate erorile, precum și avertismente. • `400` (important). Toate mesajele de eroare, avertismentele și informațiile suplimentare. • `500` (normal). Mesaje despre toate erorile și avertismentele, precum și informații detaliate despre funcționarea aplicației în modul normal (implicit). • `600` (scăzut). Toate mesajele.

Setări avansate	
`all`	Execută o comandă cu parametrii `file` și `mem`.
`file`	Salvați un fișier de urmărire (fără limită de dimensiune).
`rot`	Salvați urmărirea la un număr limitat de seturi de fișiere cu dimensiune limitată și suprascrieți fișierele mai vechi atunci când este atinsă dimensiunea maximă.
`mem`	Salvați urmărirea în fișierele dump.

Exemplu

```
avp.com TRACES on 500
```

```
avp.com TRACES off
```

```
avp.com TRACES on 500 mem
```

```
avp.com TRACES off file
```

START. Pornirea unui profil

Pornirea unui profil (de exemplu, pornirea unei actualizări a bazei de date sau activarea unei componente de protecție).

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Sintaxa de comandă

```
avp.com START <profile> [/R[A]:<report file>]
```

Profil	
`<profile>`	Numele profilului. Un *Profil* este o componentă, o activitate sau o caracteristică a aplicației Kaspersky Endpoint Security. Puteți vizualiza lista de profiluri disponibile rulând comanda `HELP START`.

Salvarea evenimentelor într-un mod de fișier raport (numai pentru profilurile Scanare, Program de actualizare și Derulare înapoi)	
`/R:<report file>`	Salvați numai evenimente critice în fișierul raport.
`/RA:<report file>`	Salvați toate evenimentele într-un fișier raport.

Exemplu

```
avp.com START Scan_Objects
```

STOP. Oprirea unui profil

Oprirea executării profilului (de exemplu, oprirea unei Scanări a unităților amovibile sau dezactivarea unei componente de protecție).

> Pentru a executa această comandă, funcția Protecție prin parolă trebuie activată. Utilizatorul trebuie să aibă permisiuni **Dezactivează componentele de protecție** și **Dezactivează componentele de control**.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Sintaxa de comandă

```
avp.com STOP <profile> /login=<user name> /password=<password>
```

Profil	
`<profile>`	Numele profilului. Un *Profil* este o componentă, o activitate sau o caracteristică a aplicației Kaspersky Endpoint Security. Puteți vizualiza lista de profiluri disponibile rulând comanda `HELP STOP`.

Autentificare	
`/login=<user name> /password=<password>`	Acreditări de cont de utilizator cu permisiunile necesare de protecție prin parolă.

STATUS. Starea profilului

Afișarea informațiilor despre stare pentru profilurile aplicației (de exemplu, `running` sau `completed`). Puteți vizualiza lista de profiluri disponibile rulând comanda `HELP STATUS`.

Kaspersky Endpoint Security afișează, de asemenea, informații despre starea profilurilor de serviciu. Informații despre starea profilurilor de serviciu pot fi solicitate atunci când contactați serviciul de Asistență tehnică Kaspersky.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Sintaxa de comandă

```
avp.com STATUS [<profile>]
```

Dacă introduceți comanda fără un profil, Kaspersky Endpoint Security afișează starea pentru toate profilurile aplicației.

STATISTICS. Statistici de funcționare a profilului

Afișarea statisticilor despre un profil al aplicației (de exemplu, durata scanării sau numărul de amenințări detectate.) Puteți vizualiza lista de profiluri disponibile rulând comanda `HELP STATISTICS`.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Sintaxa de comandă

```
avp.com STATISTICS <profile>
```

RESTORE. Restaurarea fișierelor din Copie de rezervă

Restaurarea unui fișier din Copie de rezervă în directorul său original. Dacă la calea specificată există deja un fișier cu același nume, aplicația va solicita confirmarea pentru a înlocui fișierul. Fișierul care este restaurat este copiat păstrându-i-se numele inițial.

Pentru a executa această comandă, funcția Protecție prin parolă trebuie activată. Utilizatorul trebuie să aibă permisiunea **Restaurează din Copii de rezervă**.

Opțiunea *Copiere de rezervă* stochează copii de rezervă ale fișierelor care au fost șterse sau modificate în timpul dezinfectării. O *copie de rezervă* este copia unui fișier creată înainte ca fișierul să fie dezinfectat sau șters. Copiile de rezervă ale fișierelor sunt stocate într-un format special și nu reprezintă o amenințare.

Copiile de rezervă ale fișierelor sunt stocate în directorul `C:\ProgramData\Kaspersky Lab\KES.14.1\QB`.

Utilizatorii din grupul Administratori au permisiuni complete de a accesa acest director. Utilizatorul al cărui cont a fost utilizat pentru a instala Kaspersky Endpoint Security primește drepturi de acces limitate la acest director.

Kaspersky Endpoint Security nu permite configurarea permisiunilor de acces al utilizatorului la copiile de rezervă ale fișierelor.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Sintaxa de comandă

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Setări avansate	
`/REPLACE`	Suprascrieți un fișier existent.
`<file name>`	Numele fișierului care va fi restaurat.

Autentificare	
`/login=<user name> /password=<password>`	Acreditări de cont de utilizator cu permisiunile necesare de protecție prin parolă.

Exemplu

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

EXPORT. Exportarea setărilor aplicației

Exportați setările Kaspersky Endpoint Security într-un fișier. Dacă comanda conține doar numele fișierului în care doriți să exportați setările, aplicația plasează fișierul după cum urmează:

- În cazul în care calea către avp.com este adăugată la variabila de sistem %PATH%, aplicația plasează fișierul în directorul `C:\Windows\SysWOW64`.
- Dacă executați comanda din directorul de instalare a aplicației, exportul va eșua deoarece funcția de autoprotecție a aplicației blochează crearea unui fișier nou în directorul aplicației. Pentru a exporta setările aplicației într-un fișier, introduceți calea fișierului.

Pentru a executa această comandă, funcția Protecție prin parolă trebuie activată. Utilizatorul trebuie să aibă permisiunea **Exportă setările**.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Sintaxa de comandă

```
avp.com EXPORT <profile> <file name> /login=<user name> /password=<password>
```

Profil	
`<profile>`	Numele profilului. Un *Profil* este o componentă, o activitate sau o caracteristică a aplicației Kaspersky Endpoint Security. Puteți vizualiza lista de profiluri disponibile rulând comanda `HELP EXPORT`.

Fișier de exportat	
`<file name>`	Numele fișierului în care vor fi exportate setările aplicației. De asemenea, puteți introduce calea fișierului. Puteți exporta setările Kaspersky Endpoint Security într-un fișier de configurare DAT sau CFG, într-un fișier text TXT sau într-un document XML.

Autentificare	
`/login=<user name> /password=<password>`	Acreditări de cont de utilizator cu permisiunile necesare de protecție prin parolă.

Exemplu

```
avp.com EXPORT ids ids_C:\Users\Fred123\Documents\config.dat
```

```
avp.com EXPORT fm fm_config.txt
```

IMPORT. Importarea setărilor aplicației

Importul setărilor pentru Kaspersky Endpoint Security dintr-un fișier creat cu ajutorul comenzii `EXPORT`.

Pentru a executa această comandă, funcția Protecție prin parolă trebuie activată. Utilizatorul trebuie să aibă permisiunea **Configurează setările aplicației**.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Sintaxa de comandă

```
avp.com IMPORT <file name> /login=<user name> /password=<password>
```

Fișier de importat	
`<file name>`	Numele fișierului din care vor fi importate setările aplicației. Puteți importa setările Kaspersky Endpoint Security dintr-un fișier de configurare DAT sau CFG, un fișier text TXT sau un document XML.

Autentificare	
`/login=<user name> /password=<password>`	Acreditări de cont de utilizator cu permisiunile necesare de protecție prin parolă.

Exemplu

```
avp.com IMPORT config.dat /login=KLAdmin /password=samplePassword
```

ADDKEY. Aplicarea unui fișier cheie

Activarea componentei Kaspersky Endpoint Security folosind un fișier cheie. Dacă aplicația este deja activată, cheia va fi adăugată drept cheie de rezervă.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Această comandă nu poate fi executată dacă aplicația este instalată în modul Light Agent.

Sintaxa de comandă

```
avp.com ADDKEY <file name> [/login=<user name> /password=<password>]
```

Fișier cheie	
`<file name>`	Numele fișierului cheie.

Autentificare	
`/login=<user name> /password=<password>`	Acreditările contului de utilizator. Aceste acreditări trebuie introduse numai dacă funcția Protecție prin parolă este activată.

Exemplu

```
avp.com ADDKEY file.key
```

LICENSE. Licențiere

Gestionarea cheilor de licență ale Kaspersky Endpoint Security, EDR Optimum sau EDR Expert (Suplimentul Kaspersky Endpoint Detection and Response).

Pentru a executa această comandă și a elimina o cheie de licență, funcția Protecție prin parolă trebuie să fie activată. Utilizatorul trebuie să aibă permisiunea **Elimină cheia**.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Această comandă nu poate fi executată dacă aplicația este instalată în modul Light Agent.

Sintaxa de comandă

```
avp.com LICENSE <operation> [/login=<user name> /password=<password>]
```

Funcționare	
`/ADD <file name>`	Activarea componentei Kaspersky Endpoint Security folosind un fișier cheie. Dacă aplicația este deja activată, cheia va fi adăugată drept cheie de rezervă.
`/ADD <activation code>`	Activați Kaspersky Endpoint Security folosind un cod de activare. Dacă aplicația este deja activată, cheia va fi adăugată drept cheie de rezervă.
`/REFRESH`	Actualizați starea licenței Kaspersky Endpoint Security. Drept urmare, aplicația primește informații actualizate despre starea licenței de la serverele de activare Kaspersky.
`/REFRESH <license ID>`	Actualizează starea licențelor utilizând ID-ul licenței. Folosind această comandă, poți actualiza starea suplimentului EDR, a suplimentului MDR, a suplimentului KUMA sau a altor licențe. Poți obține ID-ul licenței din certificatul de licență. Drept urmare, aplicația primește informații actualizate despre starea licenței de la serverele de activare Kaspersky.
`/CHECK`	Obține informații despre licență. Kaspersky Endpoint Security afișează informații despre toate cheile de licență adăugate, inclusiv cheile de rezervă, suplimentul EDR, suplimentul MDR, cheile pentru suplimentul KUMA și alte chei. Kaspersky Endpoint Security afișează următoarele informații despre licență: • denumirea licenței; • identificatorul licenței; • adresa Serverului de protecție (SVM) la care este conectată mașina virtuală pe care este instalată aplicația în modul Light Agent; • tipul de licență: trial, comercială, beta, abonament; • data și ora activării aplicației; • data și ora expirării licenței; • numărul de zile până la expirarea licenței.
`/CHECK <license ID>`	Obține informații despre licență după ID. Poți folosi această comandă pentru a obține informații despre licență. Poți obține ID-ul licenței din certificatul de licență.
`/DEL /login=<user name> /password=<password>`	Eliminați cheia de licență a aplicației. Cheia de rezervă va fi, de asemenea, eliminată.
`/DEL <license ID> /login=<user name> /password=<password>`	Șterge cheia folosind ID-ul licenței. Folosind această comandă, poți șterge o cheie din suplimentul EDR, suplimentul MDR, suplimentul KUMA sau alte licențe. Poți obține ID-ul licenței din certificatul de licență.

Autentificare	
`/login=<user name> /password=<password>`	Acreditări de cont de utilizator cu permisiunile necesare de protecție prin parolă.

Exemplu

```
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
```

Exemplu

```
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. Achiziționarea unei licențe

Deschiderea site-ului web Kaspersky pentru achiziția sau reînnoirea licenței.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Această comandă nu poate fi executată dacă aplicația este instalată în modul Light Agent.

PBATESTRESET. Resetarea rezultatele verificării discului înainte de criptarea discului

Resetarea rezultatele verificării compatibilității pentru Full Disk Encryption (FDE), incluzând atât tehnologia Kaspersky Disk Encryption, cât și tehnologia BitLocker Drive Encryption.

Înainte de a executa aplicația Full Disk Encryption, aplicația efectuează o serie de verificări pentru a verifica dacă se poate cripta computerul. În cazul în care computerul nu acceptă aplicația Full Disk Encryption, Kaspersky Endpoint Security înregistrează în jurnal informații despre incompatibilitate. Data viitoare când încercați să criptați, aplicația nu efectuează această verificare și vă avertizează că nu este posibilă criptarea. În cazul în care configurația hardware a computerului s-a modificat, rezultatele verificării compatibilității înregistrate în jurnal anterior de aplicație trebuie resetate pentru a verifica din nou unitatea de hard disk a sistemului pentru compatibilitatea cu tehnologiile Kaspersky Disk Encryption sau BitLocker de criptare a unităților.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

EXIT. Părăsirea aplicației

Părăsirea componentei Kaspersky Endpoint Security. Aplicația va fi descărcată din memoria RAM a computerului.

Pentru a executa această comandă, funcția Protecție prin parolă trebuie activată. Utilizatorul trebuie să aibă permisiunea **Părăsește aplicația**.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Sintaxa de comandă

```
avp.com EXIT /login=<user name> /password=<password>
```

EXITPOLICY. Dezactivarea politicii

Dezactivarea politicii Kaspersky Security Center pe computer. Toate setările Kaspersky Endpoint Security sunt disponibile pentru configurare, inclusiv setările care au lacăt închis în politică ( ).

Pentru a executa această comandă, funcția Protecție prin parolă trebuie activată. Utilizatorul trebuie să aibă permisiunea **Dezactivează politica Kaspersky Security Center**.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Sintaxa de comandă

```
avp.com EXITPOLICY /login=<user name> /password=<password>
```

STARTPOLICY. Activarea politicii

Activarea politicii Kaspersky Security Center pe computer. Setările aplicației vor fi configurate în conformitate cu politica.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

DISABLE. Dezactivarea protecției

Dezactivarea aplicației File Threat Protection pe un computer cu o licență Kaspersky Endpoint Security expirată. Nu este posibil să executați această comandă pe un computer care are aplicația neactivată sau are o licență validă.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

SPYWARE. Detectarea programelor spyware

Gestionarea detectării programelor spyware. Componenta pentru detectarea programelor spyware este activată în mod implicit.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Sintaxa de comandă

```
avp.com SPYWARE on|off
```

KSN. Comutarea între KSN / KPSN

Selectarea unei soluții Kaspersky pentru determinarea reputației fișierelor sau a site-urilor web. Kaspersky Endpoint Security acceptă următoarele soluții de infrastructură pentru lucrul cu bazele de date Kaspersky privind reputația:

- *Kaspersky Security Network (KSN)* este soluția folosită de majoritatea aplicațiilor Kaspersky. Participanții KSN primesc informații de la Kaspersky Security Network și trimit către Kaspersky informații despre obiecte detectate pe computerul utilizatorului, pentru a fi analizate suplimentar de analiștii Kaspersky și pentru a fi incluse în bazele de date privind reputația și în cele statistice.

- *Kaspersky Private Security Network (KPSN)* este o soluție care permite utilizatorilor de computere care găzduiesc Kaspersky Endpoint Security sau alte aplicații Kaspersky să obțină acces la bazele de date privind reputația ale Kaspersky și la alte date statistice, fără a trimite date către Kaspersky de la propriile lor computere. KPSN este conceput pentru clienții corporativi care nu pot participa la Kaspersky Security Network din oricare dintre următoarele motive:

  - Stațiile de lucru locale nu sunt conectate la Internet.

  - Transmiterea oricăror date în afara țării sau în afara rețelei locale corporative este interzisă prin lege sau restricționată de politicile de securitate corporativă.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Această comandă nu poate fi executată dacă aplicația este instalată în modul Light Agent.

Sintaxa de comandă

```
avp.com KSN /global | /private <file name>
```

Fișier de configurare Kaspersky Security Network	
`<file name>`	Numele fișierului de configurare care conține setările Kaspersky Private Security Network. Acest fișier are extensia PKCS7 sau PEM.

Exemplu

```
avp.com KSN /global
avp.com KSN /private C:\ksn_config.pkcs7
```

Exemplu

```
avp.com KSN /global
```

```
avp.com KSN /private C:\ksn_config.pkcs7
```

SERVERBINDINGDISABLE. Dezactivarea protecției conexiunii la server

Executarea activității *Protecție conexiune Server de administrare* care elimină parola de conectare a computerului la Serverul de administrare. Astfel, activitatea dezactivează protecția conexiunii la Serverul de administrare.

Pentru a executa această comandă, funcția Protecție prin parolă trebuie activată.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Sintaxa de comandă

```
avp.com SERVERBINDINGDISABLE [/password=<password>]
```

Password	
`/password=<password>`	Parola contului de utilizator KLAdmin sau parola din activitatea *Protecție conexiune Server de administrare*. Dacă parametrul nu este specificat, Kaspersky Endpoint Security îți solicită să introduci o parolă pe linia următoare.

Comenzi KESCLI

Comenzile KESCLI vă permit să primiți informații despre starea protecției computerului, utilizând componenta OPSWAT, și vă permit să efectuați activități standard precum *Scanare malware* și *Actualizarea modulelor bazelor de date și ale aplicațiilor*.

Puteți vizualiza lista comenzilor KESCLI utilizând comanda `kescli --help` sau comanda abreviată `kescli -h`.

Pentru a gestiona Kaspersky Endpoint Security din linia de comandă:

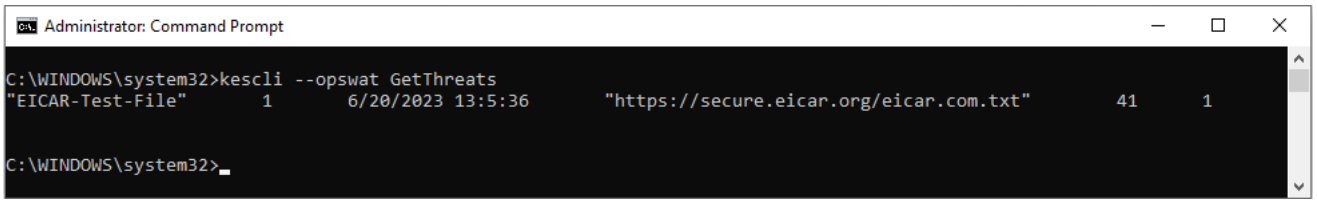
1. Executați interpretorul de linii de comandă (cmd.exe) ca administrator.
2. Deschideți directorul în care se află fișierul executabil Kaspersky Endpoint Security.

   Puteți adăuga calea către fișierul executabil la variabila de sistem %PATH% în timpul instalării aplicației.

3. Utilizează următorul șablon pentru a executa comanda:

```
kescli <comandă> [opțiuni]
```

Drept urmare, Kaspersky Endpoint Security va executa comanda (a se vedea figura de mai jos).



Gestionarea aplicației din linia de comandă

Scan. Scanare malware

Executarea activității *Scanare malware* (Scanare completă).

Pentru a executa activitatea, administratorul trebuie să Permite utilizarea activităților locale în politică.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security.

Sintaxa de comandă

```
kescli --opswat Scan "<scan scope>" <action on threat detection>
```

Puteți verifica starea finalizării activității *Scanare malware* utilizând comanda `GetScanState` și puteți vizualiza data și ora când a fost finalizată ultima dată scanarea, utilizând comanda `GetLastScanTime`.

Domeniu de scanare	
`<scan scope>`	`;`-listă separată de fișiere și directoare. De exemplu, `"C:\Program Files (x86)\Example Folder"`.

Acțiune la detectarea amenințării	
`0`	**Informează**. Dacă este selectată această opțiune, Kaspersky Endpoint Security adaugă informațiile despre fișierele infectate în lista de amenințări active la detectarea acestor fișiere.
`1`	**Dezinfectează; șterge dacă dezinfectarea nu reușește**. Dacă selectezi această opțiune, aplicația încearcă automat să dezinfecteze fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, aplicația șterge fișierul. Această acțiune este selectată în mod implicit.

Exemplu

```
kescli --opswat Scan "C:\Documents and Settings\All Users\My Documents;C:\Program Files" 1
```

GetScanState. Starea finalizării scanării

Afișarea informațiilor despre starea finalizării activității *Scanare malware* (*Scanare completă*):

- `1` – scanarea este în curs.
- `0` – scanarea nu se execută.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security.

Sintaxa de comandă

```
kescli --opswat GetScanState
```

GetLastScanTime. Determinarea orei finalizării scanării

Afișarea informațiilor despre data și ora finalizării ultimei activități *Scanare malware* (*Scanare completă*).

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security.

Sintaxa de comandă

```
kescli --opswat GetLastScanTime
```

GetThreats. Obținerea datelor despe amenințările detectate

Afișarea unei liste cu amenințările detectate (*Report on threats*). Acest raport conține informații despre amenințări și activitatea virușilor din ultimele 30 de zile anterior creării raportului.

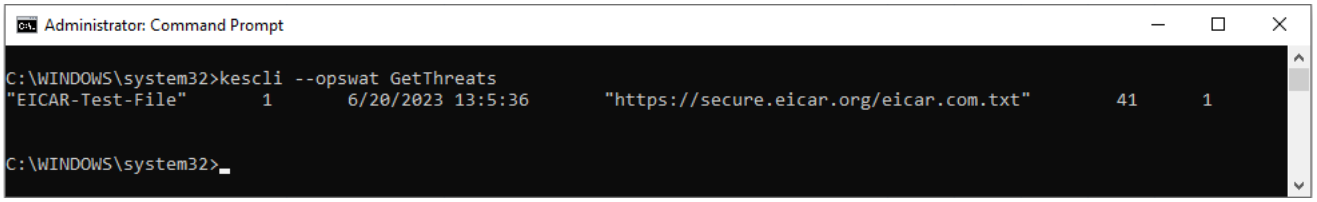
Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security.

Sintaxa de comandă

```
kescli --opswat GetThreats
```

Când este executată această comandă, Kaspersky Endpoint Security va trimite un răspuns în formatul următor:

```
<name of detected object> <type of object> <detection date and time> <path to file>
<action on threat detection> <threat danger level>
```



Gestionarea aplicației din linia de comandă

Tip obiect	
0	Nu este cunoscut (Unknown).
1	Viruși (Virware)
2	Programe de tip troian (Trojware).
3	Programe periculoase (Malware).
4	Advertisement programs (Adware).
5	Programe de apelare automată (Pornware).
6	Aplicații care pot fi utilizate de un infractor cibernetic ca să deterioreze computerul și datele utilizatorului (Riskware).
7	Obiecte arhivate ale căror metodă de arhivare poate fi utilizată pentru protejarea codurilor periculoase (Packed).
20	Obiecte necunoscute (Xfiles).
21	Aplicații cunoscute (Software).
22	Fișiere mascate (Hidden).
23	Aplicații care necesită atenție (Pupware).
24	Comportament anormal (Anomaly).
30	Nedeterminat (Undetect).
40	Bannere publicitare (Banner).
50	Atac rețea (Attack).
51	Acces registry (Registry).
52	Activitate suspectă (Suspicion).
60	Vulnerabilități (Vulnerability).
70	Phishing (Phishing).
80	Atașare e-mail nedorită (Attachment).
90	Malware detectat de Kaspersky Security Network (Urgent).
100	Link necunoscut (Suspic URL).
110	Alt malware (Behavioral).

Acțiune la detectarea amenințării	
0	Nu este cunoscut (unknown).
1	Amenințarea a fost remediată (ok).
2	Obiectul a fost infectat și nu a fost dezinfectat (infected).
5	Obiectul este într-o arhivăși nu a fost dezinfectat (archive).
9	Obiectul a fost dezinfectat (disinfected).
10	Obiectul nu a fost dezinfectat (not disinfected).
11	Obiectul a fost șters (deleted).
13	A fost creată o copie de rezervă a obiectului (backupped).
15	Obiectul a fost mutat în Copie de rezervă (quarantined).
23	Obiectul a fost șters la repornirea computerului (delete on reboot).
25	Obiectul a fost dezinfectat la repornirea computerului (disinfect on reboot).
29	Obiectul a fost mutat în Copie de rezervă de către un utilizator (added by user).
30	Obiectul a fost adăugat la excluderi (added to exclude).
31	Obiectul a fost mutat În Copie de rezervă la repornirea computerului (quarantine on reboot).

`36`	Fals pozitiv (`false alarm`).
`38`	Procesul a fost terminat (`terminated`).
`40`	Obiectul nu a fost detectat (`not found`).
`41`	Nu se poate soluționa amenințarea (`untreatable`).
`42`	Obiectul a fost restaurat (`rolled back`).
`43`	Obiectul a fost creat ca rezultat al activității amenințării (`produced by threat`).
`44`	Obiectul a fost restaurat la repornirea computerului (`roll back on reboot`).
`0xffffffff`	Obiectul nu a fost procesat (`discarded`).

Nivel de pericol amenințare	
`0`	Necunoscut
`1`	Ridicat
`2`	Scanare medie
`4`	Redus
`8`	Info (mai mic decât *Redus*)

UpdateDefinitions. Actualizarea bazelor de date și modulelor aplicației

Executarea activității *Actualizarea modulelor bazelor de date și ale aplicațiilor*. Kaspersky Endpoint Security utilizează sursa implicită: Serverele de actualizare ale Kaspersky.

Pentru a executa activitatea, administratorul trebuie să Permite utilizarea activităților locale în politică.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security.

Această comandă nu poate fi executată dacă aplicația este instalată în modul Light Agent.

Sintaxa de comandă

```
kescli --opswat UpdateDefinitions
```

Poți vizualiza data și ora lansării bazelor de date antivirus actuale utilizând comanda `GetDefinitionsetState`.

GetDefinitionState. Determinarea datei și orei ultimei actualizări a bazelor de date

Afișarea informațiilor despre data și ora ultimei actualizări a bazelor de date antivirus utilizate.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security.

Sintaxa de comandă

```
kescli --opswat GetDefinitionState
```

EnableRTP. Activarea protecției

Activarea componentelor de protecție Kaspersky Endpoint Security pe computer: File Threat Protection, Web Threat Protection, Mail Threat Protection, Network Threat Protection, Host Intrusion Prevention.

Pentru a activa componentele de protecție, administratorul trebuie să se asigure că setările relevante ale politicii pot fi modificate (atributele sunt deschise).

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security.

Sintaxa de comandă

```
kescli --opswat EnableRTP
```

Ca urmare, componentele de protecție sunt activate chiar dacă ai interzis modificarea setărilor aplicației cu Protecție prin parolă.

Puteți verifica starea de funcționare a componentei File Threat Protection utilizând comanda `GetRealTimeProtectionState`.

GetRealTimeProtectionState. Starea File Threat Protection

Afișarea informațiilor despre starea componentei File Threat Protection:

- `1` – componenta este activată.
- `0` – componenta este dezactivată.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security.

Sintaxa de comandă

```
kescli --opswat GetRealTimeProtectionState
```

GetEncryptionState. Starea criptării discului

Afișarea informațiilor despre starea criptării discului:

- `1` înseamnă că unitatea de disc este protejată de tehnologia de criptare a discului Kaspersky sau BitLocker.
- `0` înseamnă că unitatea de disc nu este criptată.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security.

Sintaxa de comandă

```
kescli --opswat GetEncryptionState
```

Version. Identificarea versiunii aplicației

Afișarea versiunii Kaspersky Endpoint Security for Windows.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security.

Sintaxa de comandă

```
kescli --Version
```

Puteți utiliza, de asemenea, comanda abreviată `-v`.

Comenzi de gestionare Detection and Response

Puteți utiliza linia de comandă pentru a gestiona funcționalitatea încorporată a soluțiilor Detection and Response (de exemplu, Kaspersky Sandbox sau Kaspersky Endpoint Detection and Response Optimum). Puteți gestiona soluțiile Detection and Response dacă gestionarea utilizând consola Kaspersky Security Center nu este posibilă. Poți vizualiza lista de comenzi pentru gestionarea aplicației executând comanda `HELP`. Pentru a citi despre sintaxa unei anumite comenzi, introduceți `HELP <command>`.

Pentru a gestiona funcțiile încorporate ale soluțiilor Detection and Response folosind linia de comandă:

1. Executați interpretorul de linii de comandă (cmd.exe) ca administrator.
2. Deschideți directorul în care se află fișierul executabil Kaspersky Endpoint Security.
3. Utilizează următorul șablon pentru a executa comanda:

   ```
   avp.com <command> [options]
   ```

   Drept urmare, Kaspersky Endpoint Security va executa comanda.

SANDBOX. Gestionarea Sandbox

Comenzi pentru gestionarea componentei Sandbox:

- Activarea sau dezactivarea componentei Sandbox.

  Componentele Sandbox asigură interacțiunea cu soluția Kaspersky Sandbox și componenta KATA Sandbox, care face parte din Kaspersky Anti Targeted Attack Platform.

- Configurarea componentei Kaspersky Sandbox:
  - Conectarea computerului la serverele Sandbox.

    Serverele utilizează imagini virtuale implementate ale sistemelor de operare Microsoft Windows pentru a executa obiectele care trebuie scanate. Puteți introduce o adresă IP (IPv4 sau IPv6) sau un nume de domeniu complet calificat. Pentru detalii despre implementarea imaginilor virtuale și configurarea serverelor Sandbox, consultați Ajutor Kaspersky Sandbox și Ajutor Kaspersky Anti Targeted Attack Platform.
  - Configurarea timpul de expirare a conexiunii pentru server.

    Expirare conexiune pentru serverul Sandbox (pentru Kaspersky Sandbox) sau serverul Central Node (pentru KATA). După expirarea perioadei de expirare configurată, Kaspersky Endpoint Security trimite o solicitare către următorul server. Poți crește perioada de expirare a conexiunii pentru server dacă viteza conexiunii este mică sau dacă conexiunea este instabilă. Perioada de expirare a solicitării recomandată este de 0.5 secunde sau mai puțin.
  - Configurarea unei conexiuni de încredere între computer și servere.

    Pentru a configura o conexiune de încredere cu serverul Sandbox (pentru Kaspersky Sandbox) sau serverul Central Node (pentru KATA), trebuie să pregătești un certificat TLS. Apoi, trebuie să adaugi certificatul pe computer, folosind o politică. De asemenea, trebuie să adaugi certificatul la serverul Sandbox (pentru Kaspersky Sandbox) sau la serverul Central Node (pentru KATA).
  - Configurarea modului de integrare.

    Trebuie să selectați o soluție care include componenta Sandbox, adică Kaspersky Sandbox sau KATA Sandbox. *Kaspersky Sandbox* este o soluție autonomă Detection and Response de la Kaspersky. *KATA Sandbox* este o componentă a soluției Kaspersky Anti Targeted Attack Platform. Atunci când este integrată cu KATA Sandbox, componenta poate funcționa în următoarele moduri:
    - **Manually**. Utilizatorul trimite manual fișierul pentru scanare din meniul contextual (**Trimite către Sandbox**).
    - **Automatically**. Aplicația detectează automat obiectele și le trimite către Sandbox pentru scanare.
    - **Combined**.
- Afișarea setările curente ale componentei.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Sintaxa de comandă

```
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>]
```

Funcționare	
stop	Dezctivați componenta Sandbox.

`start`	Activați componenta Sandbox.

`set`	Configurați componenta Sandbox. Puteți modifica următoarele setări:
	• Adăugați serverele Sandbox (`--servers`)
	• Adaugă un certificat TLS (`--pinned-certificate`)
	• Adăugați unui cripto-container (`--client-certificate`)
	• Stabiliți o parolă pentru containerul crypto (`--client-certificate-password`);
	• Setează timpul de expirare a conexiunii la server (`--timeout`)
	• Selectați un mod de integrare (`--mode`):
	  • `KSB` – integrare cu Kaspersky Sandbox;
	  • `KATAManual` – integrare manuală cu KATA Sandbox;
	  • `KATAAuto` – integrare automată cu KATA Sandbox;
	  • `KATAFull` – integrare combinată cu KATA Sandbox.

`show`	Afișați setările curente ale componentei. Veți primi următorul răspuns:
	`sandbox.timeout=<Sandbox server connection timeout (ms)>`
	`sandbox.servers=<list of Sandbox servers>`
	`sanbox.mode=<integration mode>`
	`sandbox.tls=<trusted connection status>`

Autentificare	
`/login=<user name> /password=<password>`	Acreditări de cont de utilizator cu permisiunile necesare de protecție prin parolă.

Exemplu

```
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. Gestionarea prevenirii executării

Dezactivarea componentei Prevenirea executării sau afișarea setărilor curente ale componentei, inclusiv lista regulilor de prevenire a executării.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Sintaxa de comandă

```
avp.com prevention disable
```

```
avp.com prevention /show
```

După executarea comenzii `prevention /show`, veți primi răspunsul următor:

```
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`

Valori returnate de comandă:

- `-1` înseamnă că comanda nu este acceptată de versiunea aplicației instalată pe computer;
- `0` înseamnă că comanda a fost executată cu succes;
- `1` înseamnă că un argument obligatoriu nu a fost transmis comenzii;
- `2` înseamnă că a apărut o eroare generală;
- `4` înseamnă că a apărut o eroare de sintaxă;
- `9` - operație greșită (de exemplu, o încercare de a dezactiva componenta atunci când aceasta este deja dezactivată).

ISOLATION. Gestionarea Izolării rețelei

Dezactivarea componentei Izolare rețea pe computer sau afișarea setările curente ale componentei. Setările componentei includ, de asemenea, o listă cu conexiunile la rețea adăugate la excluderi.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Sintaxa de comandă

```
avp.com isolation /OFF /login=<user name> /password=<password>
```

```
avp.com isolation /STAT
```

Ca urmare a executării comenzii `stat`, primiți următorul răspuns: `Network isolation on|off`.

RESTORE. Restaurarea fișierelor din Carantină

Restaurarea unui fișier din Carantină în directorul său original. *Carantină* este un spațiu de stocare locală special de pe computer. Utilizatorul poate pune în carantină fișierele pe care le consideră periculoase pentru computer. Fișierele introduse în carantină sunt stocate într-o stare criptată și nu amenință securitatea dispozitivului. Kaspersky Endpoint Security utilizează Carantina numai atunci când este integrată cu soluțiile Kaspersky Detection and Response. În alte cazuri, Kaspersky Endpoint Security plasează fișierul relevant în Copie de rezervă. Pentru detalii privind gestionarea funcției Carantină ca parte a soluțiilor, consultă Kaspersky Sandbox Help, Kaspersky Endpoint Detection and Response Optimum Help, Kaspersky Endpoint Detection and Response Expert Help, Kaspersky Anti Targeted Attack Platform Help, and Kaspersky Endpoint Detection and Response Expert (on-premises) Help.

Pentru a executa această comandă, funcția Protecție prin parolă trebuie activată. Utilizatorul trebuie să aibă permisiunea **Restaurează din Copii de rezervă**.

Obiectul este carantinat în contul de sistem (SYSTEM).

Restaurarea fișierelor din Carantină implică următoarele considerații speciale:

- Dacă directorul de destinație a fost șters sau utilizatorul nu are drepturi de acces la acel director, aplicația plasează fișierul în directorul `%DataRoot%\QB\Restored`. Apoi, trebuie să mutați manual fișierul în folderul destinație.
- Aplicația tratează numele fișierului restaurat ca fiind sensibil la majuscule și litere mici. Dacă nu țineți cont de majuscule și litere mici când introduceți numele fișierului, aplicația nu restaurează fișierul.
- Dacă directorul de destinație conține deja un fișier cu același nume, aplicația anulează restaurarea fișierului.
- Dacă utilizezi soluția KATA (EDR), aplicația salvează o copie a fișierului în Carantină, după restabilirea acestuia. Puteți să goliți directorul Carantină manual. Pentru soluțiile EDR Optimum și EDR Expert, aplicația șterge fișierul după restaurare.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Sintaxa de comandă

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Setări avansate	
`/REPLACE`	Suprascrieți un fișier existent.
`<file name>`	Numele fișierului care va fi restaurat.

Autentificare	
`/login=<user name> /password=<password>`	Acreditări de cont de utilizator cu permisiunile necesare de protecție prin parolă.

Exemplu

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

Valori returnate de comandă:

- `-1` înseamnă că comanda nu este acceptată de versiunea aplicației instalată pe computer;
- `0` înseamnă că comanda a fost executată cu succes;
- `1` înseamnă că un argument obligatoriu nu a fost transmis comenzii;
- `2` înseamnă că a apărut o eroare generală;
- `4` înseamnă că a apărut o eroare de sintaxă;

IOCSCAN. Scanare pentru descoperirea indicatorilor de compromitere (IOC)

Executarea activității *IOC Scan*. Un *Indicator de compromitere (IOC)* este un set de date despre un obiect sau o activitate care indică accesul neautorizat la computer (compromiterea datelor). De exemplu, multe încercări nereușite de conectare la sistem pot constitui un Indicator de compromitere. Activitatea *IOC Scan* permite găsirea Indicatorilor de compromitere pe computer și luarea măsurilor de răspuns la amenințări.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

O scanare IOC este anulată după 128 de potriviri cu indicatorii de compromitere descriși în fișierele IOC. Acest lucru este necesar pentru a limita numărul de intrări în raportul activității Scanare IOC, pentru a facilita analiza și pentru a proteja raportul împotriva debordării din cauza indicatorilor de compromitere formulați imprecis, care pot genera un număr mare de potriviri.

Sintaxa de comandă

```
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>]
```

Fișiere IOC	
`<full path to the IOC file>`	Calea completă către fișierul IOC pe care doriți să îl utilizați pentru scanare. Puteți specifica mai multe fișiere IOC separate prin spații. Calea completă către fișierul IOC trebuie introdusă fără argumentul `/path`. De exemplu, `C:\Users\Admin\Desktop\IOC\file1.ioc`
`/path=<path to the folder with IOC files>`	Calea către directorul cu fișiere IOC pe care doriți să le utilizați pentru scanare. *Fișierele IOC* sunt fișiere care conțin seturile de indicatori pe care aplicația încearcă să le potrivească pentru a contoriza o detectare. Fișierele IOC trebuie să fie conforme cu standardul OpenIOC. De exemplu, `C:\Users\Admin\Desktop\IOC`

Tipul de date pentru scanarea IOC	
`/process=on|off`	Analizați datele procesului atunci când efectuați scanarea IOC (termen ProcessItem). Dacă valoarea argumentului este `off`, Kaspersky Endpoint Security nu analizează procesele care se execută pe computer la efectuarea scanării. În cazul în care fișierul IOC conține termenii IOC ai documentului IOC ProcessItem, aceștia sunt ignorați (detectați ca nicio potrivire). Dacă argumentul nu este specificat, Kaspersky Endpoint Security analizează datele procesului numai dacă documentul IOC ProcessItem este descris în fișierul IOC care este furnizat pentru scanare.
`/hint=<full path to the executable file of the process|full path to the file>`	Analizează datele fișierului atunci când este efectuată scanarea IOC (termenii ProcessItem și FileItem). Poți selecta un fișier într-unul din următoarele moduri: • termenul `<full path to the executable file of the process>` – ProcessItem; • termenul `<full path to the file>` – FileItem.
`/registry=on|off`	Analizați datele registry-ului Windows atunci când efectuați o scanare IOC (termen RegistryItem). Dacă valoarea argumentului este `off`, Kaspersky Endpoint Security nu scanează registry-ul Windows. Dacă fișierul IOC conține termeni ai documentului IOC RegistryItem, aceștia sunt ignorați (detectați ca nepotriviți). Dacă argumentul nu este specificat, Kaspersky Endpoint Security analizează registy-ul Windows numai dacă documentul IOC RegistryItem este descris în fișierul IOC care este furnizat pentru scanare. Pentru tipul de date RegistryItem, Kaspersky Endpoint Security scanează un set de chei de registry.
`/dnsentry=on|off`	Analizați datele despre înregistrările din memoria cache DNS locală atunci când efectuați scanarea IOC (termen DnsEntryItem). Dacă valoarea argumentului este `off`, Kaspersky Endpoint Security nu scanează memoria cache DNS locală. Dacă fișierul IOC conține termeni ai documentului IOC DnsEntryItem, aceștia sunt ignorați (detectați ca nepotriviți). Dacă argumentul nu este specificat, Kaspersky Endpoint Security analizează memoria cache DNS locală numai dacă documentul IOC DnsEntryItem este descris în fișierul IOC care este furnizat pentru scanare.
`/arpentry=on|off`	Analizați datele despre înregistrările din tabelul ARP atunci când efectuați scanarea IOC (termen ArpEntryItem). Dacă valoarea argumentului este `off`, Kaspersky Endpoint Security nu scanează tabelul ARP. Dacă fișierul IOC conține termeni ai documentului IOC ArpEntryItem, aceștia sunt ignorați (detectați ca nepotriviți). Dacă argumentul nu este specificat, Kaspersky Endpoint Security analizează tabelul ARP numai dacă documentul IOC ArpEntryItem este descris în fișierul IOC care este furnizat pentru scanare.
`/ports=on|off`	Analizați datele despre porturile deschise pentru ascultare atunci când efectuați scanarea IOC (termen PortItem). Dacă valoarea argumentului este `off`, Kaspersky Endpoint Security nu scanează tabelul conexiunilor active pe dispozitiv. Dacă fișierul IOC conține termeni ai documentului IOC PortItem, aceștia sunt ignorați (detectați ca nepotriviți). Dacă argumentul nu este specificat, Kaspersky Endpoint Security analizează tabelul conexiunilor active numai dacă documentul IOC PortItem este descris în fișierul IOC care este furnizat pentru scanare.
`/services=on|off`	Analizați datele despre serviciile instalate pe dispozitiv atunci când efectuați scanarea IOC (termen ServiceItem). Dacă valoarea argumentului este `off`, Kaspersky Endpoint Security nu scanează datele despre serviciile instalate pe dispozitiv. Dacă fișierul IOC conține termeni ai documentului IOC ServiceItem, aceștia sunt ignorați (detectați ca nepotriviți). Dacă argumentul nu este specificat, Kaspersky Endpoint Security analizează datele despre servicii numai dacă documentul IOC ServiceItem este descris în fișierul IOC care este furnizat pentru scanare.
`/system=on|off`	Analizați datele despre mediu atunci când efectuați scanarea IOC (termen SystemInfoItem). Dacă valoarea argumentului este `off`, Kaspersky Endpoint Security nu analizează datele despre mediu. Dacă fișierul IOC conține termeni ai documentului IOC SystemInfoItem, aceștia sunt ignorați (detectați ca nepotriviți). Dacă argumentul nu este specificat, Kaspersky Endpoint Security analizează datele despre mediu numai dacă documentul IOC SystemInfoItem este descris în fișierul IOC care este furnizat pentru scanare.

`/users=on|off`	Analizați datele despre utilizatori atunci când efectuați scanarea IOC (termen UserItem). Dacă valoarea argumentului este `off`, Kaspersky Endpoint Security nu analizează datele despre utilizatorii creați în sistem. Dacă fișierul IOC conține termeni ai documentului IOC UserItem, aceștia sunt ignorați (detectați ca nepotriviți). Dacă argumentul nu este specificat, Kaspersky Endpoint Security analizează datele despre utilizatorii creați în sistem numai dacă documentul IOC UserItem este descris în fișierul IOC care este furnizat pentru scanare.
`/volumes=on|off`	Analizați datele despre volume atunci când efectuați scanarea IOC (termen VolumeItem). Dacă valoarea argumentului este `off`, Kaspersky Endpoint Security nu scanează datele despre volumele de pe dispozitiv. Dacă fișierul IOC conține termeni ai documentului IOC VolumeItem, aceștia sunt ignorați (detectați ca nepotriviți). Dacă argumentul nu este specificat, Kaspersky Endpoint Security analizează datele despre volume numai dacă documentul IOC VolumeItem este descris în fișierul IOC care este furnizat pentru scanare.
`/eventlog=on|off`	Analizați datele despre înregistrările din jurnalul de evenimente Windows atunci când efectuați scanarea IOC (termen EventLogItem). Dacă valoarea argumentului este `off`, Kaspersky Endpoint Security nu scanează înregistrările din jurnalul de evenimente Windows. Dacă fișierul IOC conține termeni ai documentului IOC EventLogItem, aceștia sunt ignorați (detectați ca nepotriviți). Dacă argumentul nu este specificat, Kaspersky Endpoint Security analizează jurnalul de evenimente Windows numai dacă documentul IOC EventLogItem este descris în fișierul IOC care este furnizat pentru scanare.
`/datetime=<event publication date>`	Luați în considerare data la care evenimentul a fost publicat în jurnalul de evenimente Windows atunci când determinați domeniul de scanare IOC pentru documentul IOC corespunzător. Când efectuați o scanare IOC, IOC Kaspersky Endpoint Security scanează intrările din jurnalul de evenimente Windows publicate în perioada cuprinsă între data și ora specificate și momentul la care se execută activitatea. Kaspersky Endpoint Security permite specificarea datei publicării evenimentului ca valoare a argumentului. Scanarea se efectuează numai pentru evenimentele publicate în jurnalul de evenimente Windows după data specificată și înainte de executarea scanării. Dacă argumentul nu este specificat, Kaspersky Endpoint Security scanează evenimentele cu orice dată de publicare. Setarea `TaskSettings::BaseSettings::EventLogItem::datetime` nu poate fi editată. Setarea este utilizată numai dacă documentul IOC EventLogItem este descris în fișierul IOC furnizat pentru scanare.
`/channel=<list of channels>`	Lista numelor canalelor (înregistrate în jurnal) pentru care doriți să efectuați o scanare IOC. Dacă argumentul este specificat, Kaspersky Endpoint Security scanează înregistrările publicate în jurnalele specificate. Documentul IOC trebuie să aibă termenul EventLogItem descris. Numele jurnalului este specificat ca un șir în conformitate cu numele (canalului) jurnalului specificat în proprietățile jurnalului (parametrul Full Name) sau în proprietățile evenimentului (parametrul `<Channel></Channel>` din schema xml a evenimentului). Puteți specifica mai multe canale separate prin spații. Dacă argumentul nu este specificat, Kaspersky Endpoint Security scanează înregistrările pentru canalele `Application`, `System`, `Security`.
`/files=on|off`	Analizați datele fișierului atunci când efectuați scanarea IOC (termen FileItem). Dacă valoarea argumentului este `off`, Kaspersky Endpoint Security nu analizează datele despre fișier. Dacă fișierul IOC conține termeni ai documentului IOC FileItem, aceștia sunt ignorați (detectați ca nepotriviți). Dacă argumentul nu este specificat, Kaspersky Endpoint Security analizează datele fișierului numai dacă documentul IOC FileItem este descris în fișierul IOC care este furnizat pentru scanare.
`/drives=<all|system|critical|custom>`	Setați domeniul de scanare IOC atunci când analizați datele pentru documentul IOC FileItem. Puteți seta următoarele valori pentru domeniul de scanare: • `<all>` pentru toate domeniile de fișiere disponibile, • `<system>` pentru fișierele din directoarele în care este instalat sistemul de operare, • `<critical>` pentru fișierele temporare din directoarele utilizator și sistem, • `<custom>` pentru fișierele din domenii definite de utilizator (`/scope=<list of folders to scan>`). Dacă argumentul nu este specificat, scanarea se efectuează pentru zonele critice.
`/excludes=<list of exclusions>`	Setați domeniul de excludere atunci când analizați datele pentru documentul IOC FileItem. Puteți specifica mai multe căi separate prin spații.
`/scope=<list of folders to scan>`	Domeniul de scanare IOC definit de utilizator atunci când se analizează datele pentru documentul IOC FileItem (`/drives=custom`). Puteți specifica mai multe căi separate prin spații.

`/retro /<number of days>`	*Scanare IOC retrospectivă* este un mod al activității *IOC Scan* în care Kaspersky Endpoint Security scanează pentru a descoperi indicatorii de compromitere utilizând datele pentru o anumită perioadă de timp. Acest mod este destinat căutării indicatorilor de compromitere pe baza datelor de telemetrie ale computerului protejat, cum ar fi activitatea de rețea, procesele, fișierele și alte date de telemetrie. Poți seta o perioadă de timp de la 1 la 14 zile. În mod implicit, aplicația scanează pentru depistarea indicatorilor de compromitere timp de o zi.
`/network=on|off`	Analiza datelor de rețea (termenul NetworkItem).
`/url=on|off`	Analiza datelor din jurnalele browserului (termenul UrlHistoryItem). Scanarea IOC retrospectivă analizează jurnalele următoarelor browsere: Google Chrome, Mozilla Firefox, Microsoft Edge (versiunea 79 sau o versiune ulterioară).
`/email`	Analiza obiectelor de e-mail (termenul EmailItem).
`/route`	Analiza tabelelor de rutare și redirecționare (termenul RouteEntryItem).

Valori returnate de comandă:

- `-1` înseamnă că comanda nu este acceptată de versiunea aplicației instalată pe computer;
- `0` înseamnă că comanda a fost executată cu succes;
- `1` înseamnă că un argument obligatoriu nu a fost transmis comenzii;
- `2` înseamnă că a apărut o eroare generală;
- `4` înseamnă că a apărut o eroare de sintaxă;

Dacă comanda a fost executată cu succes (valoare returnată `0`) și indicatori de compromitere au fost detectați pe parcurs, Kaspersky Endpoint Security exportă următoarele informații despre rezultatul activității în linia de comandă:

`Uuid`	ID-ul fișierului IOC din antetul structurii fișierului IOC (eticheta `<ioc id="">`)
`Name`	Descrierea fișierului IOC din antetul structurii fișierului IOC (eticheta `<description></description>`)
`Matched Indicator Items`	Lista ID-urilor tuturor indicatorilor care se potrivesc.
`Matched objects`	Date pentru fiecare document IOC pentru care a existat o potrivire.

MDRLICENSE. Activare MDR

Adăugarea fișierul de configurare BLOB pentru a activa componenta Managed Detection and Response. Fișierul BLOB conține Id-ul clientului și informații despre licența pentru componenta Kaspersky Managed Detection and Response. Fișierul BLOB se află în arhiva ZIP a fișierului de configurare MDR. Puteți obține arhiva ZIP în Consola Kaspersky Managed Detection and Response. Pentru informații detaliate despre un fișier BLOB, consultați Ajutorul Kaspersky Managed Detection and Response.

Sunt necesare privilegii de administrator pentru a efectua operații cu un fișier BLOB. Setările componentei Managed Detection and Response din politică trebuie să fie, de asemenea, disponibile pentru editare ( ).

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Sintaxa de comandă

```
avp.com MDRLICENSE <operation> [/login=<user name> /password=<password>]
```

Funcționare	
`/ADD <file name>`	Aplicați fișierul de configurare BLOB pentru integrarea cu Kaspersky Managed Detection and Response (format fișier P7). Puteți aplica doar un singur fișier BLOB. Dacă un fișier BLOB a fost deja adăugat în computer, acesta va fi înlocuit.
`/DEL`	Ștergeți fișierul de configurare BLOB.

Autentificare	
`/login=<user name> /password=<password>`	Acreditări de cont de utilizator cu permisiunile necesare de protecție prin parolă.

Exemplu

```
avp.com MDRLICENSE /ADD file.key
avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword
```

Exemplu

```
avp.com MDRLICENSE /ADD file.key
```

```
avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword
```

EDRKATA. Integrarea cu EDR (KATA)

Comenzi pentru gestionarea componentei Endpoint Detection and Response (KATA):

- Activarea sau dezactivarea componentei EDR (KATA).

  Componenta EDR (KATA) oferă interoperabilitate cu soluția Kaspersky Anti Targeted Attack Platform.

- Configurarea conexiunii la serverele Kaspersky Anti Targeted Attack Platform.

- Afișarea setările curente ale componentei.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Sintaxa de comandă

```
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
```

Funcționare	
stop	Dezactivați componenta EDR (KATA).
start	Activați componenta EDR (KATA).
set	Configurați componenta EDR (KATA). Puteți modifica următoarele setări: • Adăugați servere Central Node (`servers=<server address>:<port>`) • Adaugă un certificat TLS (`server-certificate=<path to the TLS certificate>`) • Setează timpul de expirare a conexiunii la serverul Central Node (`/timeout=<Central Node server connection timeout (s)>`) • Setează perioada pentru sincronizarea cu serverul Central Node (`/sync-period=<Central Node server synchronization period (min)>`)
show	Afișați setările curente ale componentei.

KUMA. Integrare cu KUMA

Comenzi pentru gestionarea agentului KUMA încorporat:

- Activarea sau dezactivarea integrării KUMA.

  Agentul KUMA integrat asigură interoperabilitatea cu soluția Kaspersky Unified Monitoring and Analysis Platform.

- Configurarea conexiunii la serverele Kaspersky Unified Monitoring and Analysis Platform.

- Afișarea setările curente ale componentei.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Sintaxa de comandă

```
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
```

Funcționare	
stop	Dezactivează integrarea KUMA.
start	Activează integrarea KUMA.

`set`	Configurează agentul KUMA încorporat. Puteți modifica următoarele setări: • Adăugați serverele KUMA (`/servers=<protocol>://<server address>:<port>`) Aplicația acceptă următoarele protocoale de conectare la server: `tcp`, `udp`, `http`, `https`. • Adaugă un certificat TLS (`/server-certificate=<path to the TLS certificate>`) • Setează timpul de expirare a conexiunii la server (`/timeout=<KUMA server connection timeout (s)>`) • Adăugați unui cripto-container (`/client-certificate=<path to the crypto-container> /client-certificate-password=<password>`) • Configurează întârzierea transmiterii evenimentului (`/maximum-data-transfer-time=<maximum events transmission delay (sec)>`)
`show`	Afișați setările curente ale componentei.

Autentificare	
`/login=<user name> /password=<password>`	Acreditări de cont de utilizator cu permisiunile necesare de protecție prin parolă.

Exemplu

```
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. Se execută Scanarea YARA

Executarea activității *Execută scanarea YARA*. Aplicația scanează fișierele și obiectele pentru depistarea indicatorilor atacurilor țintite asupra infrastructurii IT corporative, folosind bazele de date cu regulile YARA. *Regulile YARA* sunt descrieri ale semnăturilor atacurilor țintite și ale intruziunilor în infrastructura IT a companiei, pe care Kaspersky Endpoint Security le utilizează pentru a scana obiectele.

Pentru a executa o scanare YARA, trebuie să pregătești fișierele YARA care descriu regulile. Când creezi fișiere YARA, ține cont de următoarele cerințe:

- Kaspersky Endpoint Security acceptă fișiere YARA cu extensiile .YARA și .YAR care respectă standardul deschis YARA 4.2.3 pentru descrierea indicatorilor de compromitere.
- Numai fișierele cu reguli YARA poate fi specificat pentru activitate. Activitatea *Execută scanarea YARA* nu acceptă alte tipuri de reguli.
- Dacă ai adăugat fișiere YARA pe care Kaspersky Endpoint Security nu le acceptă sau dacă regulile conțin erori de sintaxă, activitatea este anulată cu mesajul de eroare corespunzător.
- Identificatorii tuturor fișierelor YARA utilizate într-o activitate unică trebuie să fie unici. Dacă există fișiere YARA cu același identificator, acest lucru ar putea afecta rezultatele executării activității.
- O scanare YARA este anulată după 128 de potriviri cu indicatorii descriși în regulile YARA. Acest lucru este necesar pentru a limita numărul de intrări în raportul de scanare YARA pentru a facilita analiza și pentru a proteja raportul împotriva debordării din cauza regulilor YARA formulate imprecis, care pot genera un număr mare de potriviri.

Kaspersky recomandă crearea unei reguli pentru fiecare fișier YARA. Acest lucru face rezultatele scanării mai lizibile.

O scanare YARA poate dura mult timp. În funcție de dimensiunea unității, setările activităților și numărul de obiecte de pe disc, o scanare YARA poate dura de la câteva minute până la câteva ore. Aplicația nu afișează un indicator de progres. Nu este posibilă oprirea sau revocarea unei scanări YARA. Se recomandă să așteptați până când sunt disponibile rezultatele unei scanări YARA.

Sintaxa de comandă

```
avp.com YARA <full path to the YARA file>|/path=<path to the folder with YARA files> [<advanced settings>]
```

Fișiere YARA	
`<full path to the YARA file>`	Calea completă către fișierul YARA pe care doriți să îl utilizați pentru scanare. Puteți specifica căi către mai multe fișiere YARA separate prin spații. Argument obligatoriu dacă valoarea `/path=<path to the folder with YARA files>` nu este specificată. Exemplu: `C:\Users\Admin\Desktop\YARA\file1.yar C:\Users\Admin\Desktop\YARA\file2.yar`
`/path=<path to the folder with YARA files>`	Calea completă către un director cu fișiere YARA pe care doriți să le utilizați pentru scanare. Argument obligatoriu dacă valoarea `<full path to the YARA file>` nu este specificată. Exemplu: `/path=C:\Users\Admin\Desktop\YARA`

Setări avansate	
`/fastScan=<on|off>`	Scanare YARA rapidă. Pentru fiecare obiect, aplicația înregistrează în jurnal o apariție a indicatorului detectat. Aplicația ascunde, de asemenea, duplicatele indicatorilor detectați în jurnal. Funcția Scanare YARA rapidă permite scanarea mai rapidă a fișierelor mari. Dacă această setare nu este specificată, aplicația efectuează o scanare YARA standard. În acest mod, aplicația înregistrează duplicate ale indicatorilor detectați.
`/maxRules=<maximum number of scan rules>`	Limita numărului de reguli unice declanșate care determină aplicația să oprească scanarea YARA atunci când este atinsă. Dacă valoarea acestei setări nu este specificată sau dacă este specificat `0`, aplicația efectuează scanarea YARA fără limitări.
`/timeOut=<stop scan after the specified time in seconds>`	Cât timp poate dura o scanare YARA, în secunde. Când expiră acest timp, aplicația oprește scanarea YARA. Dacă valoarea acestei setări nu este specificată sau dacă este specificat `0`, aplicația efectuează scanarea YARA fără limitări.
`/recursive=<on|off>`	Acest argument inițiază o scanare recursivă a subdirectoarelor din Scanarea personalizată a `/scanFolders`.
`/scanFolders=<list of folders to be scanned>`	Acest argument inițiază o scanare YARA a fișierelor din lista de directoare specificată. Poți specifica mai multe valori separate prin spații. Kaspersky Endpoint Security acceptă caracterele `*` și `?` la introducerea unei măști a căii către un director. Dacă această setare nu este specificată, aplicația efectuează o scanare YARA a tuturor discurilor locale, cu excepția partajărilor în rețea, a unităților cloud și a suporturilor amovibile.
`/scanMemory=<on|off>`	Scanează memoria tuturor proceselor care se execută.
`/scanProcess=<process name>`	Scanează memoria numai pentru procesele specificate. Specificați căile complete, separate prin spațiu, către fișierele executabile ale proceselor. De asemenea, puteți folosi caracterele `*` și `?` pentru a introduce o mască.
`/maxSize=<file size in bytes>`	Limitează dimensiunea fișierului pentru scanarea YARA. Aplicația omite fișierele mai mari.

`/includes=<list of objects to be scanned>>`	Editarea domeniului de scanare. Poți specifica mai multe valori separate prin spații. Sunt disponibile următoarele valori: • Nume fișier • Extensia fișierului Domeniul de scanare trebuie specificat cu parametrul `/scanFolders`. Exemplu: `/scanFolders C:\*.* /includes=*.exe *.dll` – aplicația scanează toate fișierele cu extensiile EXE și DLL de pe discul C.
`/excludes=<list of objects to be scanned>`	Excluderea fișierelor din scanarea YARA. Poți specifica mai multe valori separate prin spații. Sunt disponibile următoarele valori: • Cale fișier • Masca căii fișierului Excluderile trebuie specificate cu parametrul `/scanFolders`. Exemplu: `/scanFolders C:\*.* /excludes readme.txt C:\trusted\*.* *.xml` – aplicația omite fișierul readme.txt, toate fișierele din directorul C:\trusted și toate fișierele cu extensia .XML din directorul rădăcină de pe discul C.
`/scanAutoruns=<on|off>`	Scanare YARA a obiectelor din punctele de execuție automată.
`/excludeAutoruns=<list of autorun point areas to skip>`	Excluderea obiectelor din punctele de execuție automată din domeniul de scanare. Specificați căile complete, separate prin spațiu, către fișierele executabile ale proceselor. De asemenea, puteți folosi caracterele `*` și `?` pentru a introduce o mască.
`/logFolder=<path to the folder for saving the scan results in a TXT file>`	Dacă specificați o cale către un director, aplicația salvează rezultatele scanării urmând calea indicată, într-un fișier numit yara_<numele computerului>_<ora finalizării scanării>.txt. Dacă specificați calea către un anumit fișier TXT, aplicația salvează rezultatele scanării în acel fișier. De exemplu: `/logFolder=C:\test` sau `/logFolder=C:\test\abc.txt`. Rezultatele scanării sunt afișate în linia de comandă, indiferent dacă opțiunea `/logFolder` este specificată.

Valori returnate de comandă:

- `-1` înseamnă că comanda nu este acceptată de versiunea aplicației instalată pe computer;
- `0` înseamnă că comanda a fost executată cu succes;
- `1` înseamnă că un argument obligatoriu nu a fost transmis comenzii;
- `2` înseamnă că a apărut o eroare generală;
- `4` înseamnă că a apărut o eroare de sintaxă;
- `5` înseamnă că unul sau mai multe fișiere cu reguli YARA specificate în parametru nu au fost găsite.

Dacă comanda a fost executată cu succes (valoare returnată `0`) și indicatori de compromitere au fost detectați pe parcurs, Kaspersky Endpoint Security exportă următoarele informații despre rezultatul activității în linia de comandă:

`Started at <time>` `Finished at <time>`	Ora de începere și ora de finalizare a unei scanări.
`Host name: <computer name>`	Numele computerului pe care a fost detectat obiectul.
`Result: <error>`	Codul de eroare corespunzător erorii apărute în timpul executării activității. Dacă nu există erori, aplicația afișează `0x00000000`.
`Comment: <comment text>`	Descrierea erorii care a apărut în timpul executării activității. De exemplu, `Operation timeout`.
`Object Name:` sau `Process:` (în timpul scanării memoriei de proces)	Numele obiectului sau al procesului pentru care s-a declanșat regula YARA.

`Md5: <md5 hash>` `Sha256: <sha256 hash>`	Hash-urile obiectului care a declanșat regula YARA.
`Rule Name`	Numele regulii YARA declanșate.

`Meta:`
`Author: <author>`
`Date: <date>`
`Description: <description>`
	Metadatele specificate în regula YARA.

`Detects:`
`Offset : String name : String data`
`<offset> : <string name> : <string data>`
	S-au găsit potriviri în cadrul obiectului care îndeplinesc condițiile regulii YARA:
	• Compensare în memoria de proces sau în fișierul în care s-a detectat o potrivire (`Offset`).
	• Numele șirului care corespunde în regula YARA (`String name`).
	• Șirul corespunzător din memoria procesului sau din fișier (`String data`).

TELEMETRYFILTERS. Filtrarea evenimentelor care urmează să fie trimise către KUMA

În mod implicit, trimiterea evenimentelor către serverul KUMA este dezactivată. Pentru a vă asigura că KUMA funcționează corect, trebuie să activați transmiterea datelor de telemetrie. Puteți selecta o sursă a evenimentului dintre jurnalele standard: *Application*, *Security* sau *System*. Pentru a îmbunătăți performanța și a optimiza transmiterea datelor către serverul KUMA, poți adăuga sau exclude manual evenimente individuale din telemetrie. De exemplu, poți exclude evenimentele Sysmon.

Poți exporta lista de excluderi într-un fișier JSON din linia de comandă.

Dacă comanda conține doar numele fișierului în care doriți să exportați setările, aplicația plasează fișierul după cum urmează:

- În cazul în care calea către avp.com este adăugată la variabila de sistem %PATH%, aplicația plasează fișierul în directorul `C:\Windows\SysWOW64`.

- Dacă executați comanda din directorul de instalare a aplicației, exportul va eșua deoarece funcția de autoprotecție a aplicației blochează crearea unui fișier nou în directorul aplicației. Pentru a exporta setările aplicației într-un fișier, introduceți calea fișierului.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Sintaxa de comandă

```
avp.com TELEMETRYFILTERS /export <file name>
```

```
avp.com TELEMETRYFILTERS /import <file name>
```

Funcționare	
`export`	Exportul filtrelor pentru evenimente care urmează să fie trimise către KUMA.
`import`	Importul filtrelor pentru evenimente care urmează să fie trimise către KUMA. Dacă există deja reguli de filtrare a evenimentelor pe computer, Kaspersky Endpoint Security le înlocuiește în momentul importului.

Fișier pentru export sau import	
`<file name>`	Numele fișierului cu filtre pentru evenimente care urmează să fie trimis către KUMA. De asemenea, puteți introduce calea fișierului. Poți exporta filtrele într-un fișier JSON pentru a le trimite către KUMA.

Comenzi de gestionare a Light Agent

Poți gestiona aplicația în modul Light Agent pentru a proteja mediile virtuale în linia de comandă. Poți gestiona aplicația în modul Light Agent dacă gestionarea utilizând consola Kaspersky Security Center nu este posibilă. Poți vizualiza lista de comenzi pentru gestionarea aplicației executând comanda `HELP`. Pentru a citi despre sintaxa unei anumite comenzi, introduceți `HELP <command>`.

Pentru a gestiona aplicația în modul Light Agent din linia de comandă:

1. Executați interpretorul de linii de comandă (cmd.exe) ca administrator.
2. Deschideți directorul în care se află fișierul executabil Kaspersky Endpoint Security.
3. Utilizează următorul șablon pentru a executa comanda:

   ```
   avp.com <command> [options]
   ```

   Drept urmare, Kaspersky Endpoint Security va executa comanda.

Aplicația instalată în modul Light Agent acceptă aproape toate comenzi AVP ale aplicației instalate în modul Standard. În modul Light Agent, activitățile de actualizare a bazei de date antivirus și activitățile de gestionare a cheii de licență sunt limitate.

KSVLAINFO. Determinarea modului Light Agent

Determinarea modului Light Agent.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Sintaxa de comandă

```
avp.com KSVLAINFO
```

Comanda trimite următoarele informații către consolă:

- Modul Light Agent pentru protejarea mediilor virtuale: activată sau dezactivată.

  Dacă modul Light Agent este activat, aplicația este utilizată ca parte a soluției Kaspersky Security for Virtualization Light Agent.

- Mod de protecție VDI: activat sau dezactivat.

  Modul de protecție VDI ajută la optimizarea performanței Kaspersky Endpoint Security pe mașinile virtuale non-persistente. Dacă modul de protecție VDI este activat, actualizările care necesită repornirea mașinii virtuale protejate nu sunt instalate pe mașinile virtuale non-persistente. Când primește actualizări care necesită o repornire, Light Agent instalat pe o mașină virtuală non-persistentă trimite un mesaj către Kaspersky Security Center informându-l că șablonul mașinii virtuale protejate trebuie actualizat.

- Tipul mașinii virtuale protejate: persistent sau non-persistent.

- Rolul mașinii virtuale protejate în infrastructura virtuală: server sau stație de lucru.

- Identificator: UUID.

VIISINFO. Starea conexiunii Light Agent la Serverul de integrare

Vizualizarea informațiilor despre conectarea Light Agent la Serverul de integrare.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Sintaxa de comandă

```
avp.com VIISINFO
```

Comanda trimite următoarele informații către consolă:

- Adresa și portul Serverului de integrare la care este conectat Light Agent;

- starea conexiunii la Serverul de integrare;

- data și ora ultimei conectări a Light Agent la Serverul de integrare.

SVMINFO. Starea conexiunii Light Agent la Serverul de protecție

Vizualizarea informațiilor despre conectarea Light Agent la Serverul de protecție.

Pentru a executa comanda, accesați directorul în care se află fișierul executabil Kaspersky Endpoint Security. De asemenea, puteți adăuga calea fișierului executabil la variabila de sistem %PATH% și puteți executa comanda fără a naviga la directorul aplicației.

Sintaxa de comandă

```
avp.com SVMINFO
```

Comanda trimite următoarele informații către consolă:

- Adresa SVM-ului la care este conectat Light Agent și locația SVM-ului în infrastructura virtuală în raport cu Light Agent: locală sau non-locală.
- Metoda de descoperire SVM pe care o folosește Light Agent: folosind un Server de integrare sau o listă personalizată de adrese SVM.
- Lista de adrese SVM dacă lista de adrese SVM este selectată ca metodă de descoperire SVM.
- Etichetă pentru conectarea Light Agent la SVM.
- Algoritmul de selectare a SVM-ului: standard sau extins. Dacă se utilizează algoritmul de selectare SVM extins, este afișat și tipul de cale SVM în infrastructura virtuală.
- Starea de protecție a conexiunii dintre Light Agent și Serverul de protecție.

Coduri de eroare

Pot apărea erori atunci când lucrați cu aplicația prin linia de comandă. Când apar erori, Kaspersky Endpoint Security afișează un mesaj de eroare, de exemplu, `Error: Cannot start task 'EntAppControl'`. Kaspersky Endpoint Security poate afișa, de asemenea, informații suplimentare sub formă de cod, de exemplu, `error=8947906D` (consultați tabelul de mai jos).

Coduri de eroare

Cod eroare	Descriere
`09479001`	Această cheie este deja în uz
`0947901D`	Licența a expirat. Actualizările bazei de date sunt indisponibile
`89479002`	Cheie negăsită
`89479003`	Semnătura digitală lipsește sau este alterată
`89479004`	Datele sunt alterate
`89479005`	Fișierul cheie este alterat
`89479006`	Licența a expirat
`89479007`	Fișierul cheie nu este specificat
`89479008`	Fișier cheie nevalid
`89479009`	Salvarea datelor nu a reușit
`8947900A`	Citirea datelor nu a reușit
`8947900B`	Eroare I/O
`8947900C`	Nu au fost găsite baze de date
`8947900E`	Biblioteca de licențiere nu este încărcată
`8947900F`	Baze de date deteriorate sau actualizate manual
`89479010`	Bazele de date sunt deteriorate
`89479011`	Nu se poate utiliza fișierul cheie nevalid pentru adăugarea unei chei de rezervă
`89479012`	Eroare de sistem
`89479013`	Lista de chei respinse este alterată

Cod eroare	Descriere
89479014	Semnătura fișierului nu corespunde semnăturii digitale a Kaspersky
89479015	Nu se poate utiliza o cheie pentru licența trial drept cheie pentru licența comercială
89479016	Licența de versiune beta este necesară pentru utilizarea versiunii de beta a aplicației
89479017	Fișierul cheie nu este compatibil cu această aplicație. Este imposibilă activarea Kaspersky Endpoint Security for Windows cu un fișier cheie pentru altă aplicație. Verifică aplicația instalată
89479018	Cheia de licență a fost blocată de Kaspersky
89479019	Aplicația a fost deja utilizată sub o licență trial. Nu se poate adăuga din nou o cheie pentru licență trial
8947901A	Fișierul cheie este alterat
8947901B	Semnătura digitală lipsește, este alterată sau nu se potrivește cu semnătura digitală Kaspersky
8947901C	Nu se poate adăuga o cheie dacă licența necomercială corespunzătoare a expirat
8947901E	Data la care a fost creat sau utilizat fișierul cheie este nevalidă. Verificați data sistemului
8947901F	Nu se poate adăuga o cheie pentru licența trial: este deja activă altă cheie pentru versiunea trial
89479020	Lista de chei respinse este alterată sau lipsește
89479021	Descrierea actualizării lipsește sau este deteriorată
89479022	Cheia nu este adecvată pentru această aplicație
89479023	Nu se poate utiliza fișierul cheie nevalid pentru adăugarea unei chei de rezervă
89479025	Eroare la trimiterea solicitării către serverul de activare. Motive posibile: eroare de conexiune la Internet sau probleme temporare la serverul de activare. Încercați să activați aplicația mai târziu (peste 1 sau 2 ore) folosind codul de activare. Dacă această eroare survine din nou, contactați furnizorul de Internet
89479026	Solicitarea conține un cod de activare incorect
89479027	Nu se poate obține starea răspunsului
89479028	A survenit o eroare la salvarea fișierului temporar
89479029	A fost introdus un cod de activare incorect sau data sistemului setată pe computer este incorectă. Verificați data sistemului pe computer
8947902A	Cheia nu este compatibilă cu această aplicație sau licența a expirat
8947902B	Recepționarea unui fișier cheie nu a reușit. A fost introdus un cod de activare incorect
8947902C	Serverul de activare a returnat eroarea 400
8947902D	Serverul de activare a returnat eroarea 401
8947902E	Serverul de activare a returnat eroarea 403
8947902F	Resursă necesară indisponibilă pe serverul de activare. Serverul de activare a returnat eroarea 404. Verifică setările conexiunii la Internet
89479030	Serverul de activare a returnat eroarea 405
89479031	Serverul de activare a returnat eroarea 406
89479032	Este necesară autentificarea proxy. Verifică setările rețelei tale
89479033	Solicitarea a expirat
89479034	Serverul de activare a returnat eroarea 409
89479035	Resursă necesară indisponibilă pe serverul de activare. Serverul de activare a returnat eroarea 410. Verifică setările conexiunii la Internet
89479036	Serverul de activare a returnat eroarea 411
89479037	Serverul de activare a returnat eroarea 412
89479038	Serverul de activare a returnat eroarea 413
89479039	Serverul de activare a returnat eroarea 414

Cod eroare	Descriere
8947903A	Serverul de activare a returnat eroarea 415
8947903C	Eroare internă server
8947903D	Funcționalitatea nu este suportată
8947903E	Răspuns gateway nevalid. Verifică setările de rețea
8947903F	Resursa este temporar indisponibilă
89479040	Intervalul de timp pentru răspunsul de la gateway a expirat. Verifică setările rețelei tale
89479041	Protocolul nu este acceptat de server
89479043	Eroare HTTP necunoscută
89479044	ID resursă nevalid
89479046	URL nevalid
89479047	Director destinație nevalid
89479048	Eroare de alocare memorie
89479049	A survenit o eroare la convertirea parametrilor în șir ANSI (adresă URL, director, agent)
8947904A	A survenit o eroare la crearea firului de execuție
8947904B	Firul de execuție este executat deja
8947904C	Firul de execuție nu se află în execuție
8947904D	Fișierul cheie nu se găsește pe serverul de activare
8947904E	Cheia este blocată
8947904F	Eroare internă la serverul de activare
89479050	Date insuficiente în solicitarea de activare
89479053	Licența care corespunde cheii adăugate a expirat deja
89479054	Pe computer este setată o dată de sistem nevalidă. Verificați valoarea pentru data sistemului
89479055	Licența versiunii trial a expirat
89479056	Perioada de activare a aplicației a expirat
89479057	Limita de activări ale aplicației a fost depășită pentru codul specificat
89479058	Procedura de activare s-a finalizat cu eroare de sistem
89479059	Nu se poate utiliza o cheie pentru licența trial drept cheie pentru licența comercială
8947905C	Codul de activare este necesar
89479062	Nu se poate realiza conectarea la serverul de activare
89479064	Serverul de activare este indisponibil. Verificați setările conexiunii la Internet și încercați din nou activarea
89479065	Licența a expirat
89479066	Nu se poate înlocui cheia activă cu o cheie expirată
89479067	Nu se poate adăuga o cheie de rezervă dacă licența corespunzătoare expiră înaintea licenței curente
89479068	Lipsește cheia abonamentului actualizat
8947906A	Cod de activare nevalid
8947906B	Cheie este deja activă
8947906C	Tipurile de licențe care corespund cheii active și cheii de rezervă nu se potrivesc
8947906D	Licența nu acceptă componenta
8947906E	Imposibil de adăugat cheia abonamentului drept cheie de rezervă

Cod eroare	Descriere
89479213	Eroare generică a stratului de transport
89479214	Conectarea la serverul de activare a eșuat
89479215	Format adresă web nevalid
89479216	Conversia adresei serverului proxy nu a reușit
89479217	Conversia adresei serverului nu a reușit. Verifică setările conexiunii Internet
89479218	Încercarea de conectare la server nu a reușit
89479219	Acces refuzat la distanță
8947921A	Expirare operațiune
8947921B	Eroare la trimiterea solicitării HTTP
8947921C	Eroare conexiune SSL
8947921D	Operație întreruptă de un apel invers
8947921E	Prea multe redirectări
8947921F	Verificarea destinatarului nu a reușit
89479220	Răspuns gol de la server
89479221	Eroare la trimiterea datelor
89479222	Eroare la primirea datelor
89479223	Problemă legată de certificatul SSL
89479224	Problemă legată de criptarea SSL
89479225	Problemă legată de centrul de certificare SSL
89479226	Conținut nevalid al pachetului de rețea
89479227	Acces la cont refuzat
89479228	Fișier certificat SSL nevalid
89479229	Conexiunea SSL nu poate fi închisă
8947922A	Eroare recurentă
8947922B	Fișier nevalid cu certificate revocate
8947922C	Eroare solicitare certificat SSL
89479401	Eroare de server necunoscută
89479402	Eroare internă server
89479403	Nicio cheie disponibilă pentru codul de activare introdus
89479404	Cheie activă blocată
89479405	Parametrii necesari pentru solicitarea de activare lipsesc
89479406	Număr client sau parolă nevalidă
89479407	Cod de activare nevalid
89479408	Codul de activare nu este compatibil cu această aplicație. Nu se poate activa Kaspersky Endpoint Security for Windows cu un cod de activare pentru altă aplicație. Verifică aplicația instalată
89479409	Codul de activare este necesar
8947940B	Perioada de activare a expirat
8947940C	Numărul de activări cu acest cod a fost depășit
8947940D	Format nevalid al ID-ului solicitării
8947940E	Cod de activare deja în uz

Cod eroare	Descriere
8947940F	Reînnoirea codului de activare nu a reușit
89479410	Codul de activare nu este valid pentru această regiune
89479411	Imposibil de utilizat acest cod de activare pentru această localizare a aplicației
89479412	Codul de activare este destinat versiunii noi a acestei aplicații. Obțineți un alt cod de activare pentru a activa versiunea instalată a aplicației
89479413	Serverul de activare a returnat eroarea 643
89479414	Serverul de activare a returnat eroarea 644
89479415	Serverul de activare a returnat eroarea 645
89479416	Serverul de activare a returnat eroarea 646
89479417	Este necesară versiunea 1.0 a serverului de activare
89479418	Format incorect al codului de activare
89479419	Ora computerului nu este sincronizată cu ora serverului de activare
8947941A	Versiune greșită a aplicației
8947941B	Abonamentul a expirat
8947941C	Număr de activări depășit
8947941D	Semnătură tichet nevalidă
8947941E	Sunt necesare date suplimentare
8947941F	Verificarea datelor nu a reușit
89479420	Abonament inactiv
89479421	Serverul de activare se află în mentenanță
89479501	Eroare neașteptată
89479502	A fost transferat un parametru nevalid. De exemplu, o listă goală de adrese pentru serverul de activare
89479503	Cod de activare nevalid (hash nevalid)
89479504	ID utilizator nevalid
89479505	Parolă de utilizator nevalidă
89479506	Răspuns nevalid de la serverul de activare
89479507	Solicitarea de activare a fost întreruptă
89479509	Serverul de activare a returnat o listă de redirecționare goală

Appendix. Profiluri de aplicații

Un *Profil* este o componentă, o activitate sau o caracteristică a aplicației Kaspersky Endpoint Security. Profilurile sunt utilizate pentru a gestiona aplicația din linia de comandă. Puteți utiliza profiluri pentru a executa comenzile `START`, `STOP`, `STATUS`, `STATISTICS` și `EXPORT`. Folosind profiluri, puteți configura setările aplicației (de exemplu, `STOP DeviceControl`) sau puteți executa activități (de exemplu, `START Scan_My_Computer`).

Sunt disponibile următoarele profiluri:

- `AdaptiveAnomaliesControl` – Control adaptiv al anomaliilor
- `AMSI` – Protecție AMSI

- `AntiCryptor`
- `BehaviorDetection` – Behavior Detection
- `DeviceControl` – Control dispozitive
- `EntAppControl` – Application Control
- `File_Monitoring` sau `FM` – File Threat Protection
- `Firewall` sau `FW` – Firewall
- `HIPS` – Host Intrusion Prevention
- `IDS` – Network Threat Protection
- `IntegrityCheck` – Verificare integritate
- `LogInspector` – Inspecție jurnal
- `Mail_Monitoring` sau `EM` – Mail Threat Protection
- `Rollback` – Derulare înapoi a actualizării (profilul nu poate fi aplicat dacă aplicația este instalată în modul Light Agent)
- `Scan_ContextScan` – Scanare din meniul contextual
- `Scan_IdleScan` – Scanare în fundal
- `Scan_Memory` - Scanare memorie nucleu
- `Scan_My_Computer` – Scanare completă
- `Scan_Objects` – Scanare personalizată
- `Scan_Qscan` - Scanează obiectele care sunt încărcate la pornirea sistemului de operare
- `Scan_Removable_Drive` – Scanare unități amovibile
- `Scan_Startup` sau `STARTUP` – Scanare zone critice
- `Updater` – Actualizare (profilul nu poate fi aplicat dacă aplicația este instalată în modul Light Agent)
- `Web_Monitoring` sau `WM` – Web Threat Protection
- `WebControl` – Control Web

Kaspersky Endpoint Security acceptă, de asemenea, profiluri de serviciu. Profilurile de serviciu pot fi necesare atunci când contactați serviciul de Asistența tehnică Kaspersky.

Gestionarea aplicației prin API REST

Kaspersky Endpoint Security vă permite să configurați setările aplicației, să executați o scanare, să actualizați bazele de date antivirus și să efectuați alte activități folosind soluții terțe. Kaspersky Endpoint Security oferă o API în acest scop. REST API de la Kaspersky Endpoint Security operează prin HTTP și constă dintr-un set de metode de solicitare/răspuns. Cu alte cuvinte, puteți gestiona Kaspersky Endpoint Security printr-o soluție terță și nu interfața aplicației locale sau Consola de administrare Kaspersky Security Center.

Pentru a începe folosind REST API, trebuie să instalați Kaspersky Endpoint Security cu suport pentru REST API. Clientul REST și Kaspersky Endpoint Security trebuie să fie instalate pe același computer.

Pentru a asigura interacțiunea sigură dintre Kaspersky Endpoint Security și clientul REST:

- Configurați protecția clientului REST împotriva accesului neautorizat, conform recomandărilor dezvoltatorului clientului REST. Configurați protecția directorului clientului REST împotriva scrierii cu ajutorul Listei de control al accesului deplin – DACL.
- Pentru a executa clientul REST, utilizați un cont separat cu drepturi de administrator. Refuzați conectarea interactivă la sistem pentru acest cont.

Aplicația este gestionată prin REST API la http://127.0.0.1 sau http://localhost. Nu este posibil să gestionați de la distanță Kaspersky Endpoint Security prin REST API.

DESCHIDE DOCUMENTAȚIA API REST

Instalarea aplicației cu API REST

Pentru a gestiona aplicația prin REST API, trebuie să instalați Kaspersky Endpoint Security cu suport pentru REST API. Dacă gestionați Kaspersky Endpoint Security prin REST API, nu puteți gestiona aplicația folosind Kaspersky Security Center.

Pregătirea pentru instalarea aplicației cu suport API REST

Interacțiunea sigură a Kaspersky Endpoint Security cu clientul REST necesită configurarea identificării solicitării. Pentru aceasta, trebuie să instalați un certificat și ulterior să semnați sarcina fiecărei solicitări.

Pentru a crea un certificat, puteți utiliza, de exemplu, OpenSSL.

Exemplu:

```
$ openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 1825 -nodes
```

Utilizați algoritmul de criptare RSA cu o lungime a cheii de 2048 de biți sau mai mult.

Ca urmare, veți obține un certificat `cert.pem` și o cheie privată `key.pem`.

Instalarea aplicației cu suport API REST

Pentru a instala Kaspersky Endpoint Security cu suport pentru REST API:

1. Executați interpretorul de linii de comandă (cmd.exe) ca administrator.
2. Accesați directorul care conține pachetul de distribuție pentru Kaspersky Endpoint Security versiunea 11.2.0 sau o versiune ulterioară.
3. Instalați Kaspersky Endpoint Security cu următoarele setări:

   - `RESTAPI=1`
   - `RESTAPI_User=<user name>`

     Nume de utilizator pentru gestionarea aplicației folosind REST API. Introduceți numele de utilizator în formatul `<DOMAIN>\<UserName>` (de exemplu, `RESTAPI_User=COMPANY\Administrator`). Puteți gestiona aplicația prin REST API numai sub acest cont. Puteți selecta un singur utilizator pentru a lucra cu API REST.
   - `RESTAPI_Port=<port>`

     Port utilizat pentru gestionarea aplicației prin API REST. Portul 6782 este folosit în mod implicit. Asigurați-vă că portul este liber. Parametru opțional.
   - `RESTAPI_Certificate=<path to certificate>`

     Certificat pentru identificarea solicitărilor (de exemplu, `RESTAPI_Certificate=C:\cert.pem`).

     Puteți instala certificatul după instalarea aplicației sau puteți actualiza certificatul după expirarea certificatului.

     Cum se instalează un certificat pentru identificarea solicitării API REST

     1. Dezactivați Autoprotecție Kaspersky Endpoint Security

        Mecanismul de autoprotecție previne modificarea sau ștergerea fișierelor aplicației de pe unitatea de hard disk, a proceselor de memorie și a intrărilor din registry-ul sistemului.

     2. Accesați cheia de registry care conține setările API REST:
        `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\settings\RestAp`
     3. Introduceți calea către certificat, de exemplu, `Certificate = C:\Folder\cert.pem`.
     4. Activați Autoprotecție Kaspersky Endpoint Security.
     5. Reporniți aplicația.
   - `AdminKitConnector=1`

     Gestionarea aplicațiilor folosind sisteme de administrare. Gestionarea este permisă implicit.

De asemenea, puteți utiliza fișierul setup.ini pentru a defini setările pentru lucrul cu REST API.

Exemplu:

```
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
```

Drept urmare, veți putea gestiona aplicația prin REST API. Pentru a verifica funcționarea acesteia, deschideți documentația REST API folosind o solicitare GET.

Exemplu:
```
GET http://localhost:6782/kes/v1/api-docs
```

Dacă ați instalat aplicația cu suport API REST, Kaspersky Endpoint Security creează automat o regulă de permitere în setările opțiunii Control Web, pentru accesarea resurselor web (*Regulă de serviciu pentru API REST*). Această regulă este necesară pentru a permite clientului REST să acceseze oricând Kaspersky Endpoint Security. De exemplu, dacă ați restricționat accesul utilizatorului la resursele web, acest lucru nu va afecta gestionarea aplicației prin API REST. Vă recomandăm să nu ștergeți regula sau să modificați setările *Regulă de serviciu pentru API REST*. Dacă ștergeți regula, Kaspersky Endpoint Security o va restabili după repornirea aplicației.

Lucrul cu API

Nu este posibil să restricționați accesul la aplicație prin REST API folosind Protecție prin parolă. De exemplu, nu este posibil să blocați un utilizator să dezactiveze protecția prin REST API. Puteți configura funcția Protecție prin parolă prin REST API și restricționa accesul utilizatorului la aplicație prin interfața locală.

Pentru a gestiona aplicația prin REST API, trebuie să executați clientul REST sub contul pe care l-ați specificat la instalarea aplicației cu suport pentru REST API. Puteți selecta un singur utilizator pentru a lucra cu API REST.

DESCHIDE DOCUMENTAȚIA API REST

Gestionarea aplicației prin REST API constă în următorii pași:

1. Obțineți valorile curente ale setărilor aplicației. Pentru aceasta, trimiteți o solicitare GET.

   Exemplu:
   ```
   GET http://localhost:6782/kes/v1/settings/ExploitPrevention
   ```

2. Aplicația va trimite un răspuns cu structura și valorile setărilor. Kaspersky Endpoint Security acceptă formate XML și JSON.

   Exemplu:
   ```
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": true,
   "enabled": true
   }
   ```

3. Editați setările aplicației. Folosiți structura setărilor primită ca răspuns la solicitarea GET.

   Exemplu:
   ```
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": false,
   "enabled": true
   }
   ```

4. Salvați setările aplicației (sarcina) în format JSON (payload.json).

5. Semnați fișierul JSON în formatul PKCS7.

   Exemplu:

   ```
   $ openssl smime -sign -in payload.json -signer cert.pem -inkey key.pem -nodetach -binary -outform pem -out
   signed_payload.pem
   ```

   Ca urmare, primiți un fișier semnat cu sarcina solicitării (`signed_payload.pem`).

6. Editați setările aplicației. Pentru aceasta, trimiteți o solicitare POST și atașați fișierul semnat cu sarcina solicitării (`signed_payload.pem`).

Aplicația aplică noile setări și trimite un răspuns care conține rezultatele configurației aplicației (răspunsul poate fi gol). Puteți verifica dacă setările sunt actualizate utilizând o solicitare GET.

Surse de informații despre aplicație

Această secțiune descrie sursele de informații despre aplicație.

Puteți selecta cea mai convenabilă sursă de informații în funcție de importanța și urgența problemei.

Pagina Kaspersky Endpoint Security de pe site-ul web Kaspersky

Pe pagina Kaspersky Endpoint Security, puteți vizualiza informații generale despre aplicație și despre funcțiile și caracteristicile acesteia.

Pagina Kaspersky Endpoint Security conține un link către magazinul online. Acolo puteți cumpăra sau reînnoi aplicația.

Pagina Kaspersky Endpoint Security în Baza de cunoștințe

Bază de cunoștințe este o secțiune de pe site-ul de Suport tehnic.

Pe pagina Kaspersky Endpoint Security din Baza de cunoștințe, puteți citi articole care oferă informații utile, recomandări și răspunsuri la întrebările frecvente despre cum să cumpărați, să instalați și să utilizați aplicația.

Articolele din Baza de cunoștințe pot răspunde la întrebări legate nu doar de Kaspersky Endpoint Security, ci și de alte aplicații Kaspersky. Articolele din Baza de cunoștințe pot conține, de asemenea, noutăți de la Suportul tehnic.

Discuții despre aplicațiile Kaspersky în Forum

Dacă întrebarea dvs. nu necesită un răspuns urgent, o puteți discuta cu experții Kaspersky și cu alți utilizatori în Forumul nostru.

În Forum, puteți vizualiza subiecte existente, puteți posta propriile comentarii și puteți crea subiecte de discuție noi.

Contactarea Serviciului de asistență tehnică

Dacă nu găsești o soluție pentru problema ta în documentația aplicației sau în alte surse de informații despre Kaspersky Endpoint Security, îți recomandăm să contactezi Suportul tehnic. Specialiștii de la Suport tehnic vor răspunde la întrebările tale despre instalarea și utilizarea aplicației Kaspersky Endpoint Security.

Kaspersky asigură suport pentru Kaspersky Endpoint Security pe parcursul ciclului de viață al aplicației (consultați pagina Ciclul de viață al aplicației). Înainte de a contacta Asistența tehnică, vă rugăm să citiți regulile pentru asistență .

Poți contacta Serviciul de asistență tehnică în următoarele două moduri:

- vizitând site-ul web Suport tehnic
- Trimițând o solicitare către Asistență tehnică Kaspersky prin portalul Kaspersky CompanyAccount

După ce îi informezi pe specialiștii Serviciului de asistență tehnică Kaspersky despre problema ta, este posibil să îți ceară să creezi un *fișier de urmărire*. Fișierul de urmărire vă permite să urmăriți procesul de efectuare a comenzilor aplicațiilor pas cu pas și să determinați etapa de funcționare a aplicației la care apare eroarea.

Specialiștii Serviciului de asistență tehnică pot solicita, de asemenea, informații suplimentarea despre sistemul de operare, procesele care se execută pe computer, rapoarte detaliate despre funcționarea componentelor aplicației.

Atunci când execuți diagnosticarea, experții serviciului de Asistență tehnică este posibil să-ți solicite să modifici setările aplicației astfel:

- Activarea funcționalității pentru primirea de informații de diagnosticare extinse.
- Configurați componente individuale ale aplicației modificând setările speciale care nu sunt accesibile prin intermediul interfeței de utilizator standard.
- Modificarea setărilor pentru stocarea informațiilor de diagnosticare.
- Configurarea interceptării și înregistrării în jurnal a traficului de rețea.

Experții serviciului de Asistență tehnică îți vor furniza toate informațiile necesare pentru a efectua aceste operațiuni (descrierea secvenței de pași, setările de modificat, fișiere de configurare, scripturi, funcționalitate suplimentară în linia de comandă, module de depanare, utilitare speciale etc.) și te vor informa ce datele sunt utilizate în scopul depanării. Informațiile de diagnosticare extinse se salvează pe computerul utilizatorului. Datele nu se transmit automat către Kaspersky.

Operațiunile prezentate mai sus trebuie efectuate numai sub supravegherea specialiștilor din departamentul de Asistență tehnică, în conformitate cu instrucțiunile acestora. Modificarea pe cont propriu setările aplicației în moduri care nu sunt descrise în Ajutor online sau în recomandările Suportului tehnic poate provoca încetinirea sau căderea sistemului de operare, reducerea nivelului de protecție a computerului și poate afecta disponibilitatea și integritatea informațiilor procesate.

Conținutul și zona de stocare pentru fișierele de urmărire

Sunteți personal responsabil pentru siguranța datelor stocate pe computer, în special pentru monitorizarea și restricționarea accesului la date până la trimiterea lor către Kaspersky.

Fișierele de urmărire sunt stocate pe computer cât timp aplicația este în uz și sunt permanent șterse atunci când aplicația este eliminată.

Fișierele de urmărire, cu excepția fișierelor de urmărire ale Agentului de Autentificare, sunt stocate în directorul `%ProgramData%\Kaspersky Lab\KES.14.1\Traces`.

Fișierele de urmărire sunt denumite după cum urmează: `KES<14.1_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.log`.

Poți vizualiza datele salvate în fișierele de urmărire.

Toate fișierele de urmărire conține următoarele date comune:

- Oră eveniment
- Numele firului de execuție

  Fișierul de urmărire pentru Agentul de Autentificare nu conține aceste informații.

- Componenta aplicației care a determinat evenimentul
- Gradul de gravitate a evenimentului (eveniment informațional, avertizare, eveniment critic, eroare)
- O descriere a evenimentului implicând executarea comenzii de către o componentă a aplicației și rezultatul executării acestei comenzi.

Conținutul fișierelor de urmărire SRV.log, GUI.log și ALL.log

Fișierele de urmărire `SRV.log`, `GUI.log` și `ALL.log` pot stoca următoarele informații, pe lângă datele generale:

- Date personale, inclusiv nume de familie, prenume și al doilea prenume, dacă aceste date sunt incluse în calea către fișiere de pe computerul local.
- Date despre hardware-ul instalat pe computer (cum ar fi datele de firmware BIOS/UEFI). Aceste date sunt scrise în fișiere de urmărire atunci când se execută Kaspersky Disk Encryption.
- Numele de utilizator și parola, dacă au fost transmise necodate. Aceste date pot fi înregistrate în fișierele de urmărire în cursul scanării traficului Internet.
- Numele de utilizator și parola, dacă sunt incluse în anteturile HTTP.

- Numele contului Microsoft Windows, dacă acesta este inclus într-un nume de fișier.
- Adresa ta de e-mail sau o adresă Web care conține numele contului tău și parola, dacă acestea sunt incluse în numele obiectului detectat.
- Site-uri Web pe care le vizitezi și redirecționări de la aceste site-uri Web. Aceste date sunt scrise în fișiere de urmărire atunci când aplicația scanează site-uri Web.
- Adresa serverului proxy, numele computerului, adresa IP și numele de utilizator folosit pentru conectare la serverul proxy. Aceste date sunt scrise în fișiere de urmărire dacă aplicația folosește un server proxy.
- Adrese IP la distanță la care a stabilit conexiuni computerul tău.
- Subiectul mesajului, ID-ul, numele expeditorului și adresa paginii Web a expeditorului mesajului de pe o rețea socială. Aceste date sunt scrise în fișiere de urmărire dacă este activată componenta Control Web.
- Date despre traficul de rețea. Aceste date sunt scrise în fișiere de urmărire, în cazul în care componentele de monitorizare a traficului sunt activate (cum ar fi Control Web).
- Date primite de la serverele Kaspersky (cum ar fi versiunea bazelor de date antivirus).
- Stările componentelor Kaspersky Endpoint Security și datele lor de funcționare.
- Date despre activitatea utilizatorului în aplicație.
- Evenimente ale sistemului de operare.

Conținutul fișierelor de urmărire HST.log, BL.log, Dumpwriter.log, WD.log, AVPCon.dll.log

Pe lângă datele generale, fișierul de urmărire `HST.log` conține informații despre executarea unei activități de actualizare a bazei de date și a modulelor aplicației.

Pe lângă datele generale, fișierul de urmărire `BL.log` conține informații despre evenimente apărute în cursul funcționării aplicației, precum și date necesare pentru depanarea erorilor aplicației. Acest fișier este creat dacă aplicația este lansată cu parametrul avp.exe –bl.

Pe lângă datele generale, fișierul de urmărire `Dumpwriter.log` conține informații despre serviciu necesare pentru depanarea erorilor apărute atunci când este scris fișierul de imagine al aplicației.

Pe lângă datele generale, fișierul de urmărire `WD.log` conține informații despre evenimente apărute în cursul funcționării serviciului avpsus, inclusiv eveniment legate de actualizarea modulelor aplicației.

Pe lângă datele generale, fișierul de urmărire `AVPCon.dll.log` conține informații despre evenimente apărute în cursul funcționării modulului de conectivitate al Kaspersky Security Center.

Conținutul fișierelor de urmărire a performanței

Fișierele de urmările a performanței sunt denumite după cum urmează:
`KES<14.1_dateXX.XX_timeXX.XX_pidXXX.>PERF.HAND.etl`.

Pe lângă datele generale, fișierele de urmărire a performanței conțin informații despre încărcarea pe procesor, informații despre timpul de încărcare al sistemului de operare și al aplicațiilor și informații despre procesele care se execută.

Conținutul fișierelor de urmărire ale componentei de protecție AMSI

În afară de date generale, fișierul de urmărire `AMSI.log` conține informații despre rezultatele scanărilor efectuate la solicitarea aplicațiilor terțe.

Conținutul filierelor de urmărire ale componentei Mail Threat Protection

Fișierul de urmărire `mcou.OUTLOOK.EXE.log` poate conține, pe lângă date generale, părți din mesaje de e-mail, inclusiv adrese de e-mail.

Conținutul fișierelor de urmărire ale componentei Scanare din Meniu contextual

Fișierul de urmărire `shellex.dll.log` conține, pe lângă informații generale, informații despre finalizarea activității de scanare și date necesare pentru depanarea aplicației.

Conținutul fișierelor de urmările pentru plug-inul Web al aplicației

Fișierele de urmărire ale plug-inului web al aplicației sunt stocate pe computerul pe care este implementată Kaspersky Security Center Web Console, în directorul `Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs`.

Fișierele de urmărire ale plug-inului web al aplicației sunt denumite după cum urmează: `logs-kes_windows-<type of trace file>.DESKTOP-<date of file update>.log`. Consola Web începe să scrie date după instalare și șterge fișierele de urmărire după eliminarea Consolei Web.

Fișierele de urmările pentru plug-inul Web al aplicației conțin, pe lângă datele generale, următoarele informații:

- Parola de utilizator KLAdmin pentru deblocarea interfeței Kaspersky Endpoint Security (Protecție prin parolă).
- Parola temporară pentru deblocarea interfeței Kaspersky Endpoint Security (Protecție prin parolă).
- Numele de utilizator și parola pentru serverul de e-mail SMTP (Notificări prin e-mail).
- Numele de utilizator și parola pentru serverul proxy Internet (Server proxy).
- Numele de utilizator și parola pentru activitatea *Modificare componente ale aplicației*.
- Acreditările contului și căile specificate în activitățile Kaspersky Endpoint Security și proprietățile politicii.

Conținutul fișierului de urmărire pentru Agentul de Autentificare

Fișierul de urmărire pentru Agentul de Autentificare este stocat în directorul System Volume Information și are următorul nume: `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

Pe lângă datele generale, fișierul de urmărire pentru Agentul de Autentificare conține informații despre funcționarea Agentului de Autentificare și despre acțiunile efectuate de către utilizator cu Agentul de Autentificare.

Urmărirea funcționării aplicațiilor

Urmărire aplicație reprezintă o înregistrare detaliată a acțiunilor efectuate de aplicație și a mesajelor despre evenimentele care apăr pe parcursul funcționării aplicației. În timpul procesului de urmărire, aplicația creează un set de fișiere cu date despre funcționarea diferitelor componente ale aplicației (de exemplu, SRV.log, WD.log și altele).

Urmărirea aplicațiilor trebuie efectuată sub supravegherea Suportului tehnic al Kaspersky.

Pentru a crea un fișier de urmărire a aplicațiilor:

1. În fereastra principală a aplicației, faceți clic pe butonul .
2. În fereastra care se deschide, faceți clic pe butonul **Instrumente de suport**.
3. Utilizați comutatorul **Activează urmărirea aplicațiilor** pentru a activa sau dezactiva urmărirea funcționării aplicației.
4. În lista verticală **Urmărire**, selectați un mod de urmărire a aplicației:
   - **Cu limitarea dimensiunii**. Salvați urmărirea la un număr limitat de seturi de fișiere cu dimensiune limitată și suprascrieți fișierele mai vechi atunci când este atinsă dimensiunea maximă. Dacă este selectat acest mod, puteți defini numărul maxim de seturi de fișiere pentru rotație și dimensiunea maximă pentru fiecare set de fișiere.

     În mod implicit, aplicația salvează cinci seturi de fișiere de urmărire. Dimensiunea fiecărui set de fișiere este de 3072 MO. În acest fel, aveți nevoie de 15 GO de spațiu liber pe disc pentru a salva fișierele de urmărire.
   - **Fără limitări**. Salvați un fișier de urmărire (fără limită de dimensiune).
5. În lista verticală **Nivel**, selectați nivelul de urmărire:
   - **Normal** înseamnă că fișierul de urmărire salvează mesaje referitoare la toate erorile și avertismentele, precum și informații despre funcționarea normală a aplicației (implicit).
   - **Detaliat** înseamnă că fișierul de urmărire salvează toate informațiile referitoare la funcționarea aplicației.

   Sunt disponibile niveluri suplimentare de urmărire dacă gestionați setările de urmărire a aplicațiilor în linia de comandă. Se recomandă clarificarea nivelului de urmărire necesar cu un specialist al departamentului Suport tehnic. În lipsa asistenței din partea departamentului Suport tehnic, setați nivelul de urmărire la **Normal**.

Dacă urmărirea aplicației a fost activată din linia de comandă și a fost setat un alt nivel de urmărire decât **Normal** sau **Detaliat**, lista verticală **Nivel** este setată la **Normal**.

6. Pentru a opri procesul de urmărire, reveniți la fereastra **Instrumente de suport** și dezactivați urmărirea.

Poți crea, de asemenea, fișiere de urmărire la instalarea aplicației din linia de comandă, inclusiv prin utilizarea fișierului setup.ini.

Ca rezultat, fișierele de urmărire a funcționării aplicației sunt create în directorul `%ProgramData%\Kaspersky Lab\KES.14.1\Traces`. După crearea fișierelor de urmărire, trimiteți fișierele către Serviciul de asistență tehnică al Kaspersky.

Kaspersky Endpoint Security șterge automat fișierele de urmărire atunci când aplicația este eliminată. De asemenea, puteți șterge fișierele manual. Pentru aceasta, trebuie să dezactivați urmărirea și să opriți aplicația.

Urmărirea performanței aplicațiilor

Kaspersky Endpoint Security vă permite să primiți informații despre problemele de operare ale computerului în timpul utilizării aplicației. De exemplu, puteți primi informații despre întârzierile la încărcarea sistemului de operare după instalarea aplicației. Pentru aceasta, Kaspersky Endpoint Security creează fișiere de urmărire a performanței. *Urmărirea performanței* se referă la înregistrarea în jurnal a acțiunilor efectuate de aplicație în scopul diagnosticării problemelor de performanță ale Kaspersky Endpoint Security. Pentru a primi informații, Kaspersky Endpoint Security folosește serviciul Event Tracing for Windows (ETW). Serviciul de asistență tehnică al Kaspersky este responsabil pentru diagnosticarea problemelor legate de Kaspersky Endpoint Security și stabilirea motivelor acestor probleme.

Urmărirea aplicațiilor trebuie efectuată sub supravegherea Suportului tehnic al Kaspersky.

Pentru a crea un fișier de urmărire a performanței:

1. În fereastra principală a aplicației, faceți clic pe butonul .
2. În fereastra care se deschide, faceți clic pe butonul **Instrumente de suport**.
3. Utilizați comutatorul **Activează urmărirea performanței** pentru a activa sau dezactiva urmărirea performanței aplicației.
4. În lista verticală **Urmărire**, selectați un mod de urmărire a aplicației:
   - **Cu limitarea dimensiunii**. Salvați urmărirea la un număr limitat de fișiere cu dimensiune limitată și suprascrieți fișierele mai vechi atunci când este atinsă dimensiunea maximă. Dacă este selectat acest mod, puteți defini dimensiunea maximă pentru fiecare fișier.
   - **Fără limitări**. Salvați un fișier de urmărire (fără limită de dimensiune).

5. În lista verticală **Nivel**, selectați nivelul de urmărire:

   - **De bază**. Kaspersky Endpoint Security analizează cele mai importante procese ale sistemului de operare legate de performanță.
   - **Detaliat**. Kaspersky Endpoint Security analizează toate procesele sistemului de operare legate de performanță.

6. În lista verticală **Tip de urmărire**, selectați tipul de urmărire:

   - **Informații de bază**. Kaspersky Endpoint Security analizează procesele în timp ce sistemul de operare este în funcțiune. Utilizați acest tip de urmărire dacă o problemă persistă după încărcarea sistemului de operare, cum ar fi o problemă de accesare a Internetului în browser.
   - **La repornire**. Kaspersky Endpoint Security analizează procesele numai în timp ce sistemul de operare se încarcă. După încărcarea sistemului de operare, Kaspersky Endpoint Security încetează urmărirea. Utilizați acest tip de urmărire dacă problema este legată de încărcarea întârziată a sistemului de operare.

7. Reporniți computerul și încercați să reproduceți problema.

8. Pentru a opri procesul de urmărire, reveniți la fereastra Instrumente de suport și dezactivați urmărirea.

   Ca rezultat, fișierele de urmărire a performanței sunt create în directorul `%ProgramData%\Kaspersky Lab\KES.14.1\Traces`. După crearea fișierului de urmărire, trimiteți fișierul Serviciului de asistență tehnică al Kaspersky.

Scrierea imaginilor

Un fișier de imagine conține toate informațiile despre memoria de lucru a proceselor din Kaspersky Endpoint Security în momentul în care fișierul de imagine a fost creat.

> Fișierele de imagine salvate pot conține date confidențiale. Pentru a controla accesul la date, trebuie să asigurați în mod independent securitatea fișierelor de imagine.

Fișierele de imagine sunt stocate pe un computer cât timp aplicația este în uz și sunt șterse permanent atunci când aplicația este eliminată. Fișierele imagine de memorie sunt stocate în directorul `%ProgramData%\Kaspersky Lab\KES.14.1\Traces`.

Cum se activează scrierea imaginii în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Setări generale → Setări aplicație**.
4. În blocul **Informații depanare**, fă clic pe butonul **Setări**.
5. În fereastra care se deschide, utilizează caseta de selectare **Activează scrierea imaginii** pentru a activa sau dezactiva scrierea imaginii aplicației.
6. Salvați-vă modificările.

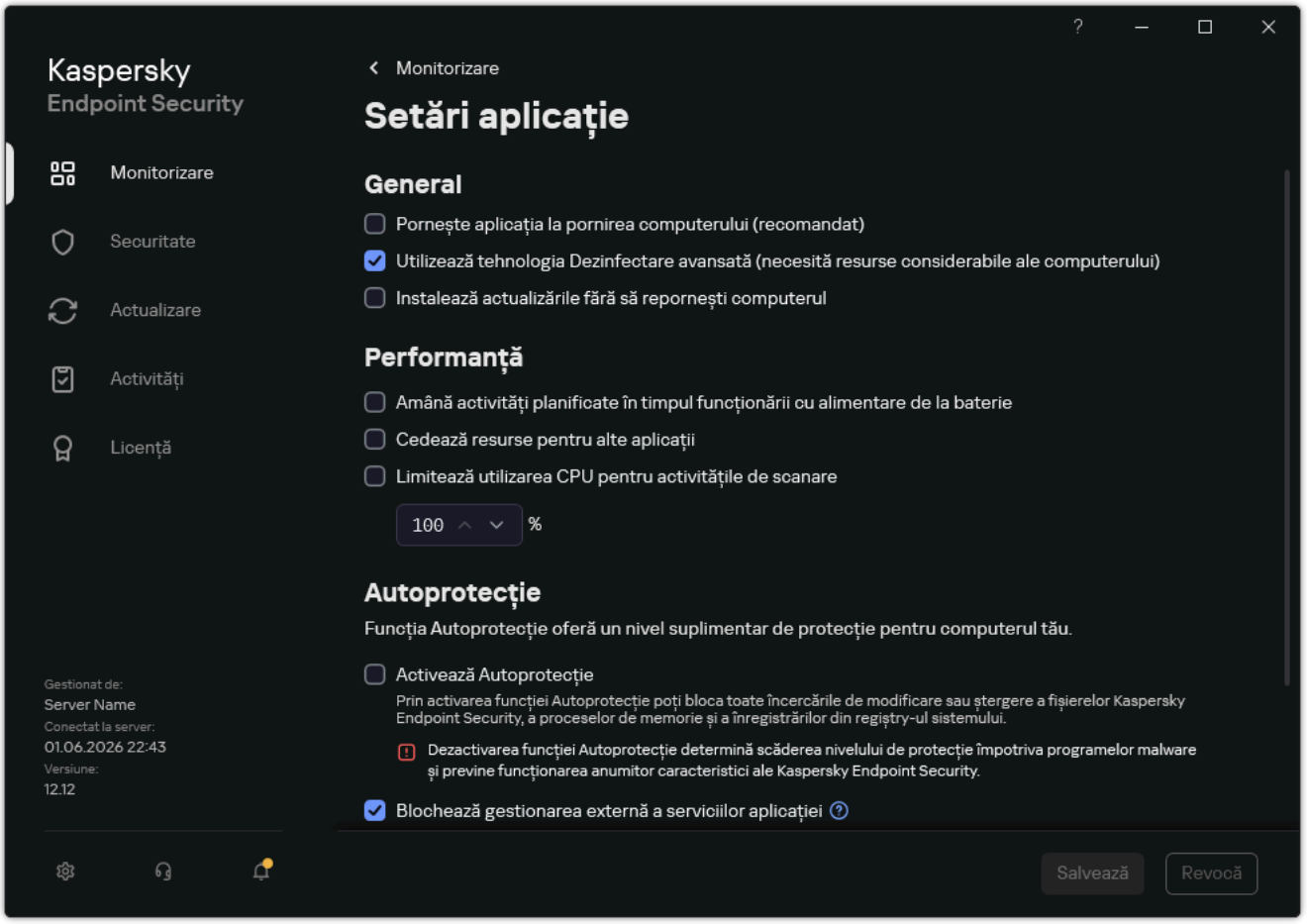
Cum se activează scrierea imaginii în Web Console și Cloud Console

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **General Settings** → **Technical Support**.
5. În blocul **Debug information**, utilizați caseta de selectare **Dump writing ENABLED** pentru a activa sau dezactiva scrierea imaginii aplicației.
6. Salvați-vă modificările.

Cum se activează scrierea imaginii în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Setări generale** → **Setări aplicație**.



Setări Kaspersky Endpoint Security for Windows

3. În blocul **Informații depanare**, utilizați caseta de selectare **Activează scrierea imaginii memoriei** pentru a activa sau dezactiva scrierea imaginii aplicației.
4. Salvați-vă modificările.

Protejarea fișierelor imagine și de urmărire

Fișierele imagine și de urmărire conțin informații despre sistemul de operare și mai pot conține datele utilizatorului. Pentru a împiedica accesul neautorizat la aceste date, poți activa protecția fișierelor imagine și de urmărire.

Dacă este activată protecția fișierelor imagine și de urmărire, fișierele pot fi accesate de către următorii utilizatori:

- Fișierele imagine pot fi accesate de către administratorul de sistem și administratorul local, precum și de către utilizatorul care a activat scrierea fișierelor imagine și de urmărire.
- Fișierele de urmărire pot fi accesate numai de către administratorul de sistem și administratorul local.

Cum se activează protecția fișierelor de imagine și a fișierelor de urmărire în Consola de administrare (MMC)

1. În arborele Consolei de administrare Kaspersky Security Center, selectează **Policies**.
2. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
3. În fereastra politicii, selectați **Setări generale** → **Setări aplicație**.
4. În blocul **Informații depanare**, fă clic pe butonul **Setări**.
5. În fereastra care se deschide, utilizează caseta de selectare **Activează protecția fișierelor imagine memorie și de urmărire** pentru a activa sau dezactiva protecția fișierelor.
6. Salvați-vă modificările.

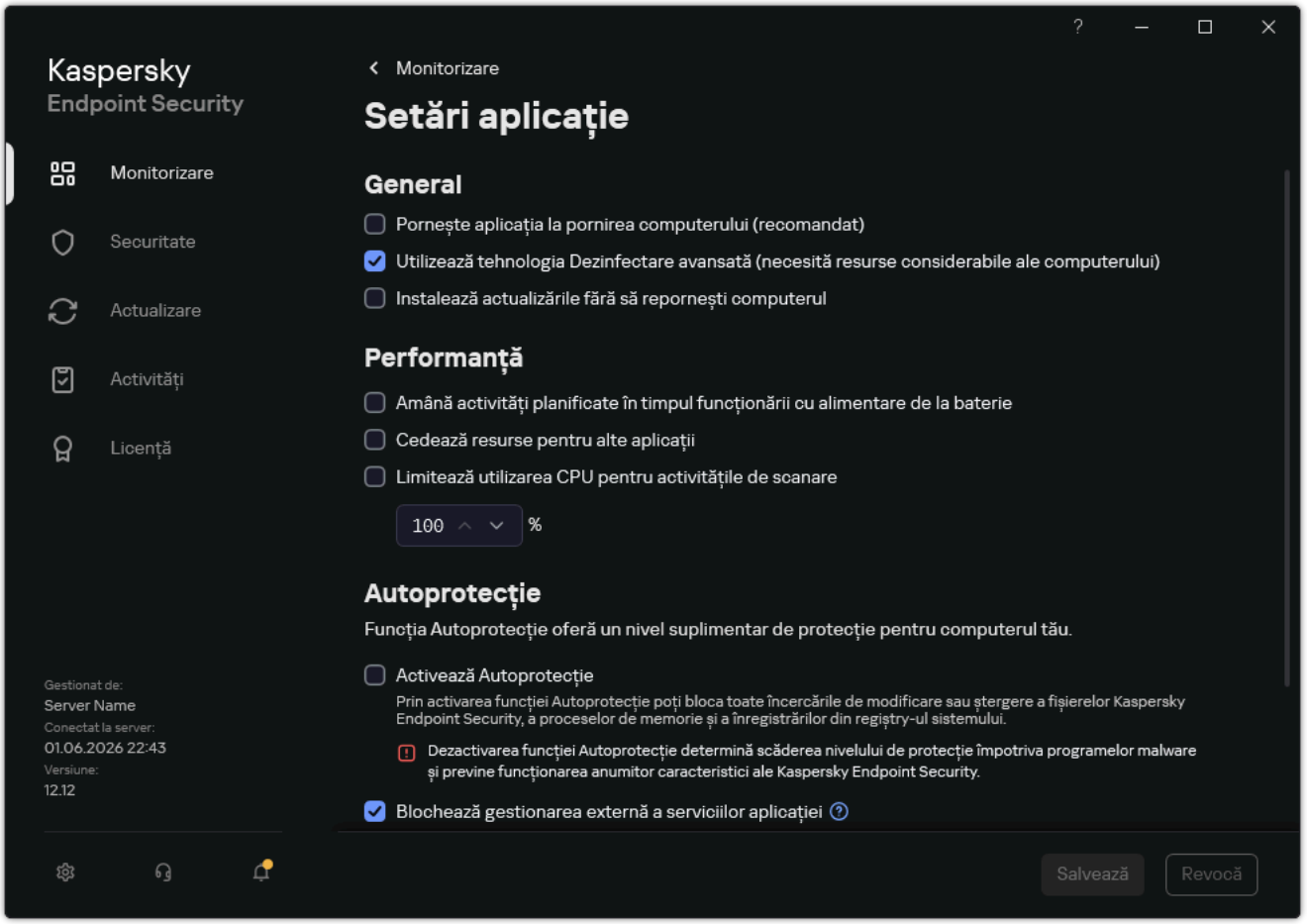
Cum se activează protecția fișierelor de imagine și a fișierelor de urmărire în Consola de administrare (MMC)

1. În fereastra principală a Web Console, selectați **Asset management** → **Policies**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Application settings**.
4. Accesați **General Settings** → **Technical Support**.
5. În blocul **Debug information**, utilizați caseta de selectare **Dump and trace files protection ENABLED** pentru a activa sau dezactiva protecția fișierelor.
6. Salvați-vă modificările.

Cum se activează protecția fișierelor de imagine și a fișierelor de urmărire în Consola de administrare (MMC)

1. În fereastra principală a aplicației, faceți clic pe butonul .
2. În fereastra cu setările aplicației, selectați **Setări generale** → **Setări aplicație**.



Setări Kaspersky Endpoint Security for Windows

3. În blocul **Informații depanare**, utilizați caseta de selectare **Activează protecția fișierelor imagine memorie și de urmărire** pentru a activa sau dezactiva protecția fișierelor.
4. Salvați-vă modificările.

Fișierele de imagine și cele de urmărire care au fost scrise cât timp protecția este activă vor rămâne protejate și după dezactivarea acestei funcții.

Obținerea datelor despre sistemul de operare (Kaspersky Get System Info)

După instalarea aplicației Kaspersky Endpoint Security, este posibil ca sistemul de operare sau o aplicație să nu funcționeze corect. Există un conflict între aplicație și software-ul sau driverele componentelor computerului.

Pentru a identifica cauza problemei, serviciul Suport tehnic Kaspersky are nevoie de un raport de la utilitarul Kaspersky Get System Info (denumit în continuare GSI). Pentru informații detaliate despre utilizarea utilitarului, consultă Baza de cunoștințe Kaspersky.

Limitări și avertizări

Kaspersky Endpoint Security prezintă o serie de limitări care nu sunt critice pentru funcționarea aplicației.

Instalarea aplicației

- Pentru informații detaliate despre asistența pentru sistemele de operare Microsoft Windows 10, Microsoft Windows Server 2016 și Microsoft Windows Server 2019, consultați Baza de cunoștințe a Serviciului de asistență tehnică.
- Pentru informații detaliate despre suport pentru sistemele de operare Microsoft Windows 11 și Microsoft Windows Server 2022, consultați Baza de cunoștințe a Suportului tehnic.
- După ce a fost instalată pe un computer infectat, aplicația nu informează utilizatorul despre necesitatea de a rula o scanare a computerului. Este posibil să aveți probleme la activarea aplicației. Pentru a rezolva aceste probleme, porniți o scanare a zonelor critice.
- Dacă sunt folosite caractere non-ASCII (de exemplu, litere rusești) în fișierele setup.ini și setup.reg, vă recomandăm să editați fișierul utilizând notepad.exe și să salvați fișierul în codificarea UTF-16LE. Alte codificări nu sunt acceptate.
- Aplicația nu acceptă utilizarea de caractere non-ASCII atunci când se specifică calea de instalare a aplicației în setările pachetului de instalare.
- Când setările aplicației sunt importate dintr-un fișier CFG, valoarea setării care definește participarea la Kaspersky Security Network nu este aplicată. După importarea setărilor, vă rugăm să citiți textul Declarației Kaspersky Security Network și să vă oferiți consimțământul de a participa la Kaspersky Security Network. Puteți citi textul Declarației în interfața aplicației sau în fișierul ksn_*.txt aflat în directorul care conține kitul de distribuire a aplicației.
- Dacă doriți să eliminați și apoi să reinstalați criptarea (FLE sau FDE) sau componenta Control dispozitive, trebuie să reporniți sistemul înainte de reinstalare.
- Când utilizați sistemul de operare Microsoft Windows 10, trebuie să reporniți sistemul după ce ați eliminat componenta File Level Encryption (FLE).
- Când eliminați componentele individuale ale aplicației (de exemplu, folosind activitatea *Modificare componente ale aplicației*), poate fi necesară o repornire a computerului.
- În proprietățile activității *Modificare componente ale aplicației*, la comutarea modului de instalare (**Mod separat** / **Mod combinat**), sincronizarea setului de componente între moduri nu este acceptată. Aplicația sincronizează setul de componente între moduri după ce redeschizi proprietățile activității.
- Instalarea aplicației se poate încheia cu o eroare care precizează că *O aplicație al cărei nume lipsește sau nu poate fi citit este instalată pe computer*. Aceasta înseamnă că aplicații incompatibile sau fragmente ale acestora rămân pe computerul dvs. Pentru a elimina artefactele aplicațiilor incompatibile, trimiteți o cerere cu o descriere detaliată a situației către Suportul tehnic Kaspersky prin intermediul Kaspersky CompanyAccount.
- Dacă ai anulat eliminarea componentei Kaspersky Endpoint Security, începe recuperarea aplicației după repornirea computerului.

- Aplicația necesită Microsoft .NET Framework 4.0 sau o versiune ulterioară. Microsoft .NET Framework 4.6.1 conține vulnerabilități. Dacă utilizați Microsoft .NET Framework 4.6.1, trebuie să instalați actualizările de securitate. Pentru detalii despre actualizările de securitate Microsoft .NET Framework, consultați site-ul web Suport tehnic Microsoft.

- Dacă aplicația este instalată fără succes, cu componenta Kaspersky Endpoint Agent selectată într-un sistem de operare server și apare fereastra *Windows Installer Coordinator Error*, consultați instrucțiunile de pe site-ul de asistență Microsoft.

- Dacă aplicația a fost instalată local în mod non-interactiv, utilizați fișierul setup.ini furnizat pentru a înlocui componentele instalate.

- După ce Kaspersky Endpoint Security for Windows este instalat în unele configurații de Windows 7, Windows Defender continuă să funcționeze. Vă sfătuim să dezactivați manual Windows Defender pentru a preveni degradarea performanței sistemului.

- Când se instalează Kaspersky Endpoint Security for Windows pe un server pe care este instalat Kaspersky Security for Windows Server (KSWS) și aplicațiile Windows Defender, trebuie repornit sistemul. Repornirea sistemului este necesară chiar dacă ai activat instalarea aplicației fără repornirea sistemului. Windows Defender for Windows Server este inclus în lista software-urilor care sunt incompatibile cu Kaspersky Endpoint Security for Windows. Înainte de instalarea aplicației, programul de instalare elimină Windows Defender for Windows Server. Eliminarea software-ului incompatibil face necesară repornirea sistemului.

- Înainte de a instala Kaspersky Endpoint Security for Windows (KES) pe un server pe care este instalat Kaspersky Security for Windows Server (KSWS), trebuie să dezactivezi KSWS Password Protection. După migrarea de la KSWS la KES, activează Protecție prin parolă în setările aplicației.

- Pentru a instala aplicația pe computerele pe care se execută Windows 7 sau Windows Server 2008 R2 cu software-ul Veeam Backup & Replication implementat, trebuie să reporniți computerul și să executați instalarea din nou.

- Migrarea de la Kaspersky Small Office Security (KSOS) la Kaspersky Endpoint Security (KES) cu Protecția prin parolă activată este disponibilă începând cu KSOS versiunea 21.16.*.*. Pentru a migra versiunile anterioare ale KSOS, trebuie să dezactivezi Protecția prin parolă sau să elimini manual KSOS. Migrarea de la KSOS la KES cu Protecția prin parolă dezactivată se efectuează corect.

- Nu poți instala Kaspersky Endpoint Security pe o unitate amovibilă de încărcare. La instalare, Kaspersky Endpoint Security afișează un mesaj de eroare: *Ai selectat un director sau o unitate nevalid(ă). Aplicația trebuie instalată pe o unitate hard disk locală*. Dacă reușești să instalezi aplicația pe o unitate amovibilă folosind instrumente terțe, acest lucru poate cauza blocarea sistemului de operare (BSOD) în timpul procesului de încărcare. Aceasta înseamnă că Kaspersky Endpoint Security nu este compatibil cu Windows To Go și soluții similare. Pentru a scana un computer de pe o unitate amovibilă, poți utiliza aplicația gratuită Kaspersky Rescue Disk.

- Instalarea Kaspersky Endpoint Security cu componente de rețea pe un server terminal cu sesiuni RDP multiutilizator implică unele considerații speciale. Sistemele de operare forțează toate sesiunile utilizatorilor să se încheie după încheierea sesiunii Administratorului. Pentru a te conecta la serverul terminal, trebuie să repornești serverul sau să te conectezi la sistem local. Un astfel de comportament este dictat de particularitățile modului în care funcționează sistemul de operare Windows.

- Dacă plug-inurile web Kaspersky Endpoint Security for Windows (versiunea 12.11.0.2004) și Kaspersky Endpoint Security for Linux (versiunea 12.4.0.1354) sunt instalate în Kaspersky Security Center 16.0 sau Kaspersky Security Center 16.1, actualizarea plug-inului web Kaspersky Endpoint Security for Windows la versiunea 12.11.0.6004 poate duce la disfuncționalități în politicile Kaspersky Endpoint Security for Linux.

  Soluție posibilă: accesează fereastra **Settings** → **Web plug-ins** și elimină plug-in-ul web Kaspersky Endpoint Security for Windows, plug-in-ul web Kaspersky Endpoint Security for Linux și Unified Protection and Management Plug-in din listă. Apoi, instalează mai întâi plug-inul web Kaspersky Endpoint Security for Linux, urmat de pluginul web Kaspersky Endpoint Security for Windows.

- În Web Console, lista componentelor este afișată incorect în proprietățile pachetului de instalare al Kaspersky Endpoint Security 12.11 for Windows. O componentă separată, Anti-Cryptor, nu este disponibilă în această versiune a aplicației. Protecția directoarelor partajate împotriva funcționalității de criptare externă este inclusă în componenta Behavior Detection. În Kaspersky Endpoint Security 12.12 for Windows, această funcționalitate este o componentă separată. În același timp, în Consola de administrare (MMC), lista componentelor este afișată corect.

Efectuarea upgrade-ului aplicației

- Începând cu versiunea 11.0.0 a aplicației, poți instala plug-inul MMC al Kaspersky Endpoint Security for Windows peste versiunea anterioară a plug-inului. Pentru a reveni la o versiune anterioară a plug-inului, șterge plug-inul actual și instalează o versiune anterioară a acestuia.

- La efectuarea upgrade-ului componentei Kaspersky Endpoint Security 11.0.0 sau 11.0.1 for Windows, setările planificării activităților locale pentru activitățile *Actualizarea modulelor bazelor de date și ale aplicațiilor*, *Scanare zone critice*, *Scanare personalizată* și *Verificare integritate aplicație* nu sunt salvate.

- Pe computerele care rulează Windows 10 versiunea 1903 și 1909, upgrade-urile de la Kaspersky Endpoint Security 10 for Windows Service Pack 2 Maintenance Release 3 (versiunea 10.3.3.275), Service Pack 2 Maintenance Release 4 (versiunea 10.3.3.304), 11.0.0 și 11.0.1 cu componenta File Level Encryption (FLE) instalată se pot termina cu o eroare. Acest lucru se datorează faptului că criptarea fișierelor nu este acceptată pentru aceste versiuni de Kaspersky Endpoint Security for Windows în Windows 10 versiunea 1903 și 1909. Înainte de a instala această actualizare, vi se recomandă să eliminați componenta de criptare a fișierelor.

- Aplicația necesită Microsoft .NET Framework 4.0 sau o versiune ulterioară. Microsoft .NET Framework 4.6.1 conține vulnerabilități. Dacă utilizați Microsoft .NET Framework 4.6.1, trebuie să instalați actualizările de securitate. Pentru detalii despre actualizările de securitate Microsoft .NET Framework, consultați site-ul web Suport tehnic Microsoft.

- Când efectuați upgrade pentru Kaspersky Endpoint Security, aplicația dezactivează utilizarea KSN până când Kaspersky Security Network Statement este acceptat. Suplimentar, starea computerului poate fi modificată în *Critical* în Kaspersky Security Center; evenimentul *Servere KSN indisponibile* este primit. Dacă utilizați Kaspersky Managed Detection and Response, veți primi evenimente despre utilizarea necorespunzătoare a soluției. Este necesară utilizarea KSN pentru funcționarea Kaspersky Managed Detection and Response. Kaspersky Endpoint Security activează utilizarea KSN după aplicarea politicii în care administratorul acceptă termenii de utilizare ai KSN. Odată ce Declarați Kaspersky Security Network este acceptată, Kaspersky Endpoint Security își reia funcționarea.

- După efectuarea upgrade-ului pentru Kaspersky Endpoint Security la versiunea 11.10.0 sau la o versiune ulterioară fără repornire, pe computer vor fi instalate două aplicații Kaspersky Endpoint Security. Nu elimina manual versiunea anterioară a aplicației. Versiunea anterioară va fi eliminată automat atunci când este repornit computerul.

- După actualizarea Kaspersky Endpoint Security pe un computer pe care se execută Microsoft Windows 11, meniul contextual al fișierului poate afișa elemente atât pentru versiunile anterioare, cât și pentru cele noi ale aplicației. Repornește computerul de două ori pentru a asigura funcționarea corectă a meniului contextual al fișierului.

- Dacă funcția Autoprotecție a aplicației este dezactivată și toate plăcile de rețea sunt oprite, componentele de rețea ale aplicației nu vor funcționa între sfârșitul upgrade-ului aplicației și repornirea computerului. Componentele de rețea ale aplicației includ Web Threat Protection, Mail Threat Protection, Network Threat Protection, Firewall, Host Intrusion Prevention și Control Web. Repornește computerul pentru ca aplicația să funcționeze corect.

- Componenta BadUSB Attack Prevention nu funcționează între sfârșitul upgrade-ului aplicației și repornirea computerului. Repornește computerul pentru ca aplicația să funcționeze corect.

- Aplicația nu poate fi actualizată dacă procesul de actualizare anterior nu a fost finalizat. Repornește computerul pentru ca aplicația să funcționeze corect.

- După ce aplicația este actualizată de la versiuni anterioare Kaspersky Endpoint Security 11 for Windows, computerul trebuie repornit.

- Dacă gestionezi Kaspersky Endpoint Security utilizând Kaspersky Security Center Cloud Console, actualizarea locală a aplicației nu este permisă. Atunci când actualizezi aplicația local, nu este posibil să accepți Acordul privind prelucrarea datelor pentru Kaspersky Security Center Cloud Console.

Suport pentru arhitectura Arm

- Instalarea Kaspersky Endpoint Security în modul Light Agent pe mașinile virtuale bazate pe arhitectura ARM nu este acceptată.

- Kaspersky Disk Encryption nu este acceptat pe computerele bazate pe arhitectura ARM.

- Criptarea fișierelor nu este acceptată pe computerele bazate pe arhitectura Arm.

- Criptarea unităților amovibile nu este acceptată pe computerele bazate pe arhitectura Arm.

- Pe computerele pe care se execută Windows 11 pentru Arm64, Agentul EDR nu este compatibil cu Bitdefender Endpoint Security Tools.

- Funcționalitatea de protecție a semnalului audio și cea de protecție a accesului la camera web nu sunt acceptate pe computerele bazate pe arhitectura Arm.

- Pe computerele bazate pe arhitectura Arm, extensia Mail Threat Protection acceptă versiunile pe 32 de biți și 64 de biți ale Outlook 2016, Outlook 2021, Outlook 2024 și Outlook 365 pentru Arm64.

- Kaspersky Endpoint Security nu trimite obiecte destinate arhitecturii Arm către Kaspersky Sandbox.

- Controlul imprimării nu este acceptat pe computerele bazate pe arhitectura Arm.

- Integrarea cu Kaspersky Endpoint Detection and Response Expert (cloud) nu este acceptată pe computerele bazate pe arhitectura ARM.

- Pe computerele bazate pe arhitectura Arm, activitatea *IOC Scan* acceptă fișiere de e-mail doar de la următorii clienți de e-mail: Versiunile pe 32 și 64 de biți ale Outlook 2016 și Outlook 2021, 2024 și 365 pentru Arm64.

Compatibilitate pentru platforme de servere

- Pe serverele cu *deduplicarea datelor* activată, trebuie să adaugi fișierul fsdmhost.exe la lista de aplicații de încredere. Acest lucru ajută la optimizarea performanței aplicației și la prevenirea încărcării excesive a procesorului.

- Sistemul de fișiere ReFS este acceptat cu limitări:

  - Kaspersky Endpoint Security poate procesa incorect evenimentele de dezinfecție a amenințărilor. De exemplu, dacă aplicația a șters un fișier rău intenționat, raportul ar putea avea o intrare Obiect neprocesat. În același timp, Kaspersky Endpoint Security dezinfectează amenințările în conformitate cu setările aplicației. Kaspersky Endpoint Security poate crea, de asemenea, un duplicat al evenimentului *Obiectul va fi dezinfectat la repornire* pentru același obiect.

  - File Threat Protection poate omite unele amenințări. În același timp, funcția Scanare malware funcționează corect.

  - După pornirea activității *Scanare malware*, excluderile de la scanare adăugate cu iChecker sunt resetate atunci când serverul este repornit.

  - Tehnologia iSwift nu este acceptată. Kaspersky Endpoint Security nu ia în considerare excluderile de la scanare adăugate folosind tehnologie iSwift.

  - Kaspersky Endpoint Security nu detectează fișierele eicar.com și susp-eicar.com dacă fișierul meicar.exe file a existat în computer înainte de instalarea Kaspersky Endpoint Security.

  - Kaspersky Endpoint Security poate afișa incorect notificările de dezinfectare a amenințărilor. De exemplu, aplicația poate afișa o notificare de amenințare pentru o amenințare dezinfectată anterior.

- Tehnologiile File Level Encryption (FLE) și Kaspersky Disk Encryption (FDE) nu sunt acceptate pe platformele de tip server. În același timp, Kaspersky Endpoint Security poate procesa incorect evenimente de criptare a datelor.

- În sistemele de operare server, nu se afișează nicio avertizare cu privire la necesitatea dezinfectării avansate.

- Microsoft Windows Server 2008 a fost exclus din suport. Instalarea aplicației pe un computer care execută sistemul de operare Microsoft Windows Server 2008 nu este acceptată.

- Kaspersky Endpoint Security instalat pe un server pe care este implementat Microsoft Data Protection Manager (DPM) poate face ca DPM să funcționeze defectuos. Acest lucru are legătură cu limitările de funcționare ale DPM. Pentru a elimina funcționarea defectuoasă, trebuie să adaugi driverele serverului local la excluderi pentru componenta File Threat Protection și activitățile *Scanare malware*.

- Modul Server Core este acceptat cu limitări:

  - Interfața grafică locală cu utilizatorul nu este disponibilă, inclusiv notificările, notificări pop-up și alte comenzi ale interfeței. Aplicația nu poate afișa ferestre de comandă, inclusiv următoarele ferestre:

    - fereastra de confirmare a actualizării versiunii aplicației și a modulului;

    - fereastra pentru repornirea computerului;

    - fereastra pentru acreditările de autentificare ale serverului proxy;

    - fereastra pentru obținerea accesului la un dispozitiv (Control dispozitive).

- Următoarele componente nu sunt disponibile: Web Threat Protection, Mail Threat Protection, Control Web, BadUSB Attack Prevention.
- Componenta Anti-Bridging nu este disponibilă.
- Puteți accepta Declarația Kaspersky Security Network numai în politica aplicației din consola Kaspersky Security Center.
- BitLocker Drive Encryption este disponibilă numai cu un Trusted Platform Module (TPM). Un PIN/o parolă nu poate fi utilizat(ă) pentru criptare, deoarece aplicația nu poate afișa fereastra de solicitare a parolei pentru autentificarea prepornire. Dacă sistemul de operare are modul de compatibilitate Standarde federale de procesare a informațiilor (FIPS) activat, conectați o unitate amovibilă pentru salvarea cheii de criptare înainte de a începe criptarea unității.

Compatibilitate pentru platforme virtuale

- Full Disk Encryption (FDE) pe mașinile virtuale Hyper-V nu este acceptată.
- Full Disk Encryption (FDE) pe platformele virtuale Citrix nu este acceptată.
- Se acceptă Windows 10 Enterprise multi-session, cu următoarele limitări:
  - Kaspersky Endpoint Security dezinfectează amenințările active fără să notifice utilizatorul, exact ca atunci când dezinfectează amenințările active de pe servere. Deoarece sistemul de operare continuă să se execute în modul sesiuni multiple, alți utilizatori activi își pot pierde datele dacă amenințarea nu este soluționată imediat.
  - Nu se acceptă Full Disk Encryption (FDE).
  - Nu se acceptă gestionarea BitLocker.
  - Nu se acceptă folosirea Kaspersky Endpoint Security cu unități de memorie externă. Infrastructura Microsoft Azure definește unitățile de memorie externă ca unități de rețea.
- Instalarea și utilizarea criptării la nivel de fișier (FLE) pe platformele virtuale Citrix nu sunt acceptate.
- Pentru a sprijini compatibilitatea Kaspersky Endpoint Security for Windows cu Citrix PVS, efectuați instalarea cu opțiunea **Asigură compatibilitatea cu Citrix PVS** activată. Această opțiune poate fi activată în Expertul de configurare sau utilizând parametrul liniei de comandă `/pCITRIXCOMPATIBILITY=1`. În cazul instalării la distanță, fișierul KUD trebuie editat adăugând următorul parametru: `/pCITRIXCOMPATIBILITY=1`.
- Citrix XenDesktop. Înainte de a începe clonarea, trebuie să dezactivați Autoprotecția pentru a clona mașini virtuale care utilizează vDisk.
- Când pregătiți o mașină șablon pentru imaginea principală Citrix XenDesktop cu Kaspersky Endpoint Security for Windows și Kaspersky Security Center Network Agent preinstalate, adăugați următoarele tipuri de excluderi în fișierul de configurare:

  ```
  [Rule-Begin]
  Type=File-Catalog-Construction
  Action=Catalog-Location-Guest-Modifiable
  name="%ALLUSERSPROFILE%\Kaspersky Lab\**\*"
  name="%ALLUSERSPROFILE%\KasperskyLab\**\*"
  [Rule-End]
  ```

  Pentru detalii despre Citrix XenDesktop, accesați site-ul web de asistență Citrix.

- În unele cazuri, o încercare de a deconecta în siguranță o unitate amovibilă poate fi nereușită pe o mașină virtuală care este implementată pe un hipervizor VMware ESXi. Încercați să deconectați din nou dispozitivul în siguranță.

- Kaspersky Endpoint Security este compatibil cu hipervizorul VMware ESXi, cu următoarele limitări:

  - Kaspersky Endpoint Security poate fi incompatibil cu driverele Guest Introspection (vnetWFP.sys, vnetFLT.sys și altele). Pentru a rezolva incompatibilitatea, actualizează driverele la cea mai recentă versiune sau dezinstalează driverele.

  - În unele cazuri, o încercare de a elimina în siguranță un disc amovibil de pe o mașină virtuală poate să nu aibă succes. Încercați să deconectați din nou dispozitivul în siguranță.

- Instalarea Kaspersky Endpoint Security pe mașini virtuale cu agentul Citrix VDA se poate încheia cu o eroare de compatibilitate. Acest lucru se întâmplă deoarece Citrix Provisioning Services are o compatibilitate limitată cu soluțiile antivirus. Pentru cele mai bune practici de utilizare a soluțiilor antivirus cu Citrix Provisioning Services, consultă site-ul web de asistență Citrix.

- Kaspersky Endpoint Security omite scanarea unei unități amovibile dacă aceasta este conectată la o mașină virtuală pe hipervizorul Citrix (activitatea *Scanare unități amovibile*). Pe astfel de dispozitive, sistemul de operare detectează unitatea amovibilă conectată ca unitate de rețea. În astfel de cazuri, puteți folosi activitatea *Scanare personalizată*. Comportamentul aplicației în modul standard și în modul Light Agent este identic.

- Dacă Kaspersky Endpoint Security este instalat pe o mașină virtuală într-o infrastructură care utilizează tehnologia Citrix App Layering, fișierele detectate de aplicație ca fiind infectate cu starea *Obiectul va fi șters la repornire* nu vor fi eliminate automat la repornirea mașinii virtuale.

  Pentru a șterge astfel de fișiere, trebuie să instalezi fișierul VHDX care conține stratul utilizatorului pe computerul administratorului Citrix App Layering și să execuți o scanare anti-malware pe discul montat.

Compatibilitate cu Kaspersky Security Center

- În Kaspersky Security Center Web Console versiunea 14.1 și anterioară, numele zonelor funcționale pentru componentele Inspecție jurnal și Monitorizare integritate fișier nu sunt afișate în secțiunea cu setările permisiunilor de acces ale utilizatorului din proprietățile Serverului de administrare.

- După repararea aplicației, protecția conexiunii computerului la Serverul de administrare este dezactivată. După repararea aplicației, execută activitatea *Protecție conexiune Server de administrare* din nou.

- În Consola de administrare Kaspersky Security Center, fereastra **Selectează un utilizator sau un grup de utilizatori** afișează doar primii 50.000 de utilizatori din lista de utilizatori Kaspersky Security Center. Consultă Kaspersky Security Center Help pentru mai multe detalii.

- Când căutați dispozitive gestionate în Consola de administrare Kaspersky Security Center, fila **Application components** poate afișa simultan mai multe variante ale denumirii aceleiași componente a aplicației, inclusiv denumiri corespunzătoare versiunilor mai vechi ale Kaspersky Endpoint Security. Este posibil ca numele unor componente să fie duplicate.

  Pentru a căuta după componentă, trebuie doar să selectați una dintre variantele afișate. Pentru mai multe detalii despre descoperirea dispozitivului, consultați Ajutor pentru Kaspersky Security Center.

Licențiere

- Dacă este afișat mesajul de sistem *Eroare la primirea datelor*, verificați dacă computerul pe care efectuați activarea are acces la rețea sau configurați setările de activare prin Kaspersky Security Center Activation Proxy.

- În interfața aplicației, data de expirare a licenței este afișată în ora locală a computerului.

- Instalarea aplicației cu un fișier cheie încorporat pe un computer care are acces instabil la Internet poate duce la afișarea temporară a evenimentelor care afirmă că aplicația nu este activată sau că licența nu permite funcționarea componentelor. Acest lucru este cauzat de faptul că, în timpul procesului de instalare, aplicația activează mai întâi licența trial încorporată. Necesită acces la Internet.

- În perioada versiunii trial, instalarea oricărei actualizări de aplicații sau patch-uri pe un computer care are acces instabil la Internet poate duce la afișarea temporară a evenimentelor care afirmă că aplicația nu este activată. Acest lucru este cauzat de faptul că, în timpul procesului de actualizare, aplicația activează mai întâi licența trial încorporată. Necesită acces la Internet.

- Dacă licența de versiune trial a fost activată automat în timpul instalării aplicației și apoi aplicația a fost eliminată fără a salva informațiile despre licență, aplicația nu va fi activată automat cu licența de versiune trial la reinstalare. În acest caz, activați manual aplicația.

- Dacă utilizați Kaspersky Security Center versiunea 11 și Kaspersky Endpoint Security versiunea 14.1, este posibil ca rapoartele privind performanța componentelor să funcționeze greșit. Dacă ați instalat componente Kaspersky Endpoint Security care nu sunt incluse în licența dvs., Agentul de rețea poate trimite erori privind starea componentei către Jurnalul de evenimente Windows. Pentru a evita erorile, eliminați componentele care nu sunt incluse în licența dvs.

Mail Threat Protection

- Când scanați e-mailuri cu extensia Mail Threat Protection pentru Microsoft Outlook, vi se recomandă să utilizați modul Cache Exchange (opțiunea Utilizare mod Cache Exchange).

- Kaspersky Endpoint Security nu acceptă versiunea pe 64 de biți a clientului de mail Microsoft Outlook. Aceasta înseamnă că Kaspersky Endpoint Security nu scanează fișierele Microsoft Outlook (fișiere PST și OST) dacă pe computer este instalată o versiune de Microsoft Outlook pe 64 de biți, chiar dacă e-mailul este inclus în domeniul de scanare.

- Kaspersky Endpoint Security nu acceptă clientul de e-mail Microsoft Outlook New.

Remediation Engine

- Aplicația restaurează fișiere numai pe dispozitive care au sistemul de fișiere NTFS sau FAT32.

- Aplicația restaurează fișiere cu o dimensiune de până la 100 MB.

- Aplicația poate restaura fișiere cu următoarele extensii: 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.

- Nu este posibilă restaurarea fișierelor aflate pe unități de rețea sau discuri CD/DVD reînregistrabile.

- Nu este posibilă restaurarea fișierelor criptate cu Encryption File System (EFS). Pentru mai multe detalii despre funcționarea EFS, accesează site-ul Web Microsoft.

- Aplicația nu monitorizează modificările fișierelor efectuate de procese la nivelul kernelului sistemului de operare.

Firewall

- Dacă o regulă de pachet de rețea sau o regulă de rețea pentru aplicații specifică nume DNS, Kaspersky Endpoint Security poate trimite solicitări către serverul DNS pentru a determina adresele IP ale acestor resurse. Firewall-ul folosește adrese IP pentru a monitoriza activitatea în rețea. Prin urmare, aplicația rezolvă numele DNS în adrese IP. Este recomandat să utilizezi nume DNS numai pentru computerele LAN sau serviciile interne.

- Pentru a specifica o regulă pentru toate adresele IPv6, adaugă intervalul de adrese ::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff. Firewall nu acceptă masca ::/0.

- Filtrarea pachetelor sau conexiunilor după adresa locală, interfața fizică și durata de livrare a pachetelor (TTL) este acceptată în următoarele cazuri:

  - După adresa locală pentru pachetele de ieșire sau conexiunile din regulile de aplicație pentru TCP și UDP și regulile de pachete.

  - După adresa locală pentru pachetele sau conexiunile de intrare (cu excepția UDP) în regulile de blocare a aplicațiilor și regulile de pachete.

  - După durata de livrare a pachetelor (TTL) în regulile de blocare a pachetelor pentru pachetele de intrare sau de ieșire.

  - După interfața de rețea pentru pachete de intrare și ieșire sau conexiuni în reguli de pachete.

- Dacă ați configurat o placă de rețea sau un pachet de timp de viață (TTL) pentru o regulă de permitere a pachetului, prioritatea acestei reguli este mai mică decât o regulă de blocare a aplicației. Cu alte cuvinte, dacă activitatea de rețea este blocată pentru o aplicație (de exemplu, aplicația se află în grupul de încredere *Restricționat la nivel superior*), nu poți permite activitatea de rețea a aplicației utilizând o regulă de pachet cu aceste setări. În toate celelalte cazuri, prioritatea unei reguli de pachet este mai mare decât o regulă de rețea pentru aplicații.

- Cand se importă regulile de pachet Firewall, Kaspersky Endpoint Security poate modifica numele regulilor. Aplicația determină reguli cu seturi identice de parametri generali: protocol, direcție, porturi la distanță și locale, timp de viață al pachetului (TTL). Dacă acest set de parametri generali este identic pentru mai multe reguli, aplicația atribuie același nume acelor reguli sau adaugă o etichetă cu parametrul la nume. Astfel, Kaspersky Endpoint Security importă toate regulile de pachete, dar numele regulilor care au setări generale identice pot fi modificate.

- Dacă ați activat raportarea evenimentelor aplicației într-o regulă de rețea, la mutarea aplicației într-ul alt grup de încredere, restricțiile acestui grup de încredere nu vor fi aplicate. Astfel, dacă aplicația este în grupul de încredere De încredere, nu va avea nicio restricție de rețea. Apoi ai activat raportarea evenimentelor pentru această aplicație și ai mutat-o în grupul de încredere *Nu este de încredere*. Firewall-ul nu va impune restricțiile de rețea pentru această aplicație. Vă recomandăm ca mai întâi să mutați aplicația în grupul de înceredere corespunzător și apoi să activați raportarea evenimentelor. Dacă această metodă nu este potrivită, puteți configura manual restricțiile pentru aplicație în setările regulii de rețea. Restricția se aplică numai interfeței locale a aplicației. Mutarea aplicației între grupurile de încredere din politică funcționează corect.

- Componentele Firewall și Intrusion Prevention au setări comune: drepturile aplicației și resursele protejate. Dacă modificați aceste setări pentru Firewall, Kaspersky Endpoint Security aplică automat noile setări componentei Intrusion Prevention. Dacă, de exemplu, ați permis modificarea setărilor generale ale politicii Firewall (lacătul este deschis), setările componentei Intrusion Prevention vor deveni, de asemenea, editabile.

- Când este declanșată o regulă pentru pachetele de rețea în Kaspersky Endpoint Security 11.6.0 sau o versiune anterioară, coloana **Nume aplicație** din raportul Firewall va afișa întotdeauna valoarea *Kaspersky Endpoint Security*. În plus, componenta Firewall va bloca conexiunea la nivelul pachetului pentru toate aplicațiile. Acest comportament a fost modificat pentru Kaspersky Endpoint Security 11.7.0 sau ulterior. Coloana **Tip regulă** a fost adăugată în raportul Firewall. Când este declanșată o regulă pentru pachetele de rețea, valoarea din coloana **Nume aplicație** rămâne goală.

- Dacă ai interzis toate activitățile în rețea folosind Firewall-ul, componenta Network Threat Protection poate detecta un atac de tip Scanare port. Acest lucru se poate întâmpla deoarece aplicația pornește Network Threat Protection înainte de Firewall, pentru a detecta activități suspecte în rețea.

BadUSB Attack Prevention

- Kaspersky Endpoint Security resetează expirarea blocării dispozitivului USB atunci când computerul este blocat (de exemplu, timpul de blocare a ecranului a trecut). Adică, dacă introduceți un cod greșit de autorizare a dispozitivului USB de mai multe ori și aplicația blochează dispozitivul USB, Kaspersky Endpoint Security vă permite să repetați încercarea de autorizare după deblocarea computerului. În acest caz, Kaspersky Endpoint Security nu blochează dispozitivul USB pentru o perioadă specificată în Setările componentei BadUSB Attack Prevention.

- Kaspersky Endpoint Security resetează expirarea blocării dispozitivului USB când protecția computerului este întreruptă. Adică, dacă introduceți un cod greșit de autorizare a dispozitivului USB de mai multe ori și aplicația blochează dispozitivul USB, Kaspersky Endpoint Security vă permite să repetați încercarea de autorizare după reluarea protecției computerului. În acest caz, Kaspersky Endpoint Security nu blochează dispozitivul USB pentru o perioadă specificată în Setările componentei BadUSB Attack Prevention.

Kaspersky Security Network

- Kaspersky Endpoint Security nu acceptă HTTPS atunci când se conectează la KSN Proxy (caseta de selectare **Use HTTPS** selectată în setările de conectare KSN Proxy) dacă adresa serverului include litere nelatine (simboluri non-ASCII).

- În Kaspersky Security Center, când comuți de la utilizarea Kaspersky Security Network global la utilizarea Kaspersky Security Network (KPSN) privat sau invers, opțiunea de a participa la Kaspersky Security Network este dezactivată în politica respectivului produs. După comutare, citiți cu atenție textul Declarației Kaspersky Security Network și oferiți-vă consimțământul pentru a participa la KSN. Puteți citi textul Declarației în interfața aplicației sau când editați politica produsului.

- Începând cu Kaspersky Endpoint Security 12.9 for Windows, atunci când comuți de la KPSN la KSN global, trebuie să reconfirmi acordul pentru Declarația Kaspersky Security Network. Pentru a face acest lucru, trebuie să activezi utilizarea Kaspersky Security Network în proprietățile politicii sau în interfața aplicației și să îți confirmi acordul pentru Declarația Kaspersky Security Network. Dacă ai utilizat deja KSN global, trebuie mai întâi să dezactivezi utilizarea KSN, apoi să o activezi din nou și să confirmi acordul pentru Declarația Kaspersky Security Network. Dacă nu ești de acord cu Declarația Kaspersky Security Network, aplicația nu va putea accesa datele Kaspersky Security Network.

- Kaspersky Endpoint Security nu trimite fișiere text (cum ar fi fișiere TXT, CSV, LOG și DOCX fără macrocomenzi) către Kaspersky Security Network pentru scanare. Aplicația trimite fișiere care pot reprezenta o amenințare pentru KSN pentru scanare. Aceste fișiere includ fișiere executabile sau fișiere care pot conține cod executabil (cum ar fi macrocomenzile din fișierele DOCX). Alte componente ale aplicației sunt responsabile pentru scanarea fișierelor text. De asemenea, poți verifica manual reputația unui fișier text din meniul contextual al fișierului. Dacă un fișier text are o reputație *Nu este de încredere (Kaspersky Security Network)*, aplicația ignoră acțiunea definită pentru amenințările detectate.

Application Control

- Când lucrezi cu regulile Application Control, nu este recomandat să adaugi mai mult de 100.000 de condiții de includere și excludere în total pentru aplicații din diferite categorii, cu condiția ca Kaspersky Endpoint Security să se execute pe un computer care îndeplinește cerințele minime privind hardware-ul și funcționează pe Microsoft Windows 10.

- Numai arhivele în format ZIP sunt acceptate atunci când lucrezi cu regulile Application Control în Kaspersky Security Center Web Console. Arhivele în alte formate, cum ar fi RAR sau 7z, nu sunt acceptate. Nu există o astfel de restricție dacă lucrezi cu reguli Application Control în Consola de administrare (MMC).

- Atunci când lucrați cu regulile Application Control. în Kaspersky Security Center Web Console, dimensiunea maximă acceptată a unui fișier încărcat este de 104 MO. Nu există o astfel de restricție dacă lucrezi cu reguli Application Control în Consola de administrare (MMC).

- Când lucrați în Microsoft Windows 10 în modul listă de aplicații respinse, regulile de blocare pot fi aplicate incorect, ceea ce ar putea cauza blocarea aplicațiilor care nu sunt specificate în reguli.

- Dacă ai adăugat noi *reguli predefinite Application Control* la efectuarea upgrade-ului pentru Kaspersky Endpoint Security, nu poți aplica aceste reguli la versiunile anterioare ale aplicației.

- Când aplicațiile web progresive (PWA) sunt blocate de componenta Application Control, appManifest.xml este indicat ca aplicație blocată în raport.

- Când adăugați aplicația standard Notepad la regula Application Control pentru Windows 11, nu este recomandat să specificați calea către aplicație. Pe computerele pe care rulează Windows 11, sistemul de operare folosește Metro Notepad aflat în directorul `C:\Program Files\WindowsApps\Microsoft.WindowsNotepad*\Notepad\Notepad.exe`. În versiunile anterioare ale sistemului de operare, aplicația Notepad se află în următoarele directoare:

  - `C:\Windows\notepad.exe`
  - `C:\Windows\System32\notepad.exe`
  - `C:\Windows\SysWOW64\notepad.exe`

  Când adăugați aplicația Notepad la o regulă Application Control, puteți specifica numele aplicației și hash-ul fișierului din proprietățile aplicației care se execută, de exemplu.

- Când are loc migrarea politicii KSWS la profilul de politică KES, expertul de conversie în loturi a politicilor și activităților (Asistent de migrare) redenumește categoriile de aplicații dacă numele categoriilor conțin caractere interzise: `'` `*` `<` `>` `?` `\` `:` `|`. Expertul de migrare înlocuiește aceste caractere cu caracterele `_`. De exemplu, categoria de aplicații `KSWS::\Everyone:[C61F-3B7C-4D89-96A1]` este redenumită `KSWS_Everyone_[C61F-3B7C-4D89-96A1]`.

Control dispozitive

- Kaspersky Endpoint Security poate înregistra în jurnal evenimentele de conectare și deconectare a dispozitivelor externe. Serviciile Windows folosesc contul de utilizator de sistem pentru a conecta sau deconecta dispozitive. Acest lucru face imposibil să știți care utilizator conectează sau deconectează dispozitivul. Kaspersky Endpoint Security specifică contul de utilizator SISTEM în eveniment.

- Accesul la dispozitivele Imprimantă care au fost adăugate la lista de încredere este blocat de regulile de blocare a dispozitivelor și a magistralelor.

- Pentru dispozitivele MTP, controlul operațiilor de Citire, Scriere și Conectare este acceptat dacă utilizați driverele Microsoft încorporate ale sistemului de operare. Dacă un utilizator instalează un driver personalizat pentru lucrul cu un dispozitiv (de exemplu, ca parte a iTunes sau Android Debug Bridge), controlul operațiilor de Citire și Scriere poate să nu funcționeze.

- Când lucrați cu dispozitive MTP, regulile de acces sunt modificate după reconectarea dispozitivului.

- Componenta Control dispozitive înregistrează evenimente legate de dispozitivele monitorizate, cum ar fi conectarea și deconectarea unui dispozitiv, citirea unui fișier de pe un dispozitiv, scrierea unui fișier pe un dispozitiv și alte evenimente. Kaspersky Endpoint Security înregistrează evenimentele de deconectare numai pentru următoarele tipuri de dispozitive: Dispozitive portabile (MTP), Unități amovibile, Dischete, Unități CD/DVD. Pentru alte tipuri de dispozitive, aplicația nu înregistrează evenimente de deconectare. Aplicația înregistrează operațiunea de conectare a unui dispozitiv la un computer pentru toate tipurile de dispozitive.

- Dacă adăugați un dispozitiv la lista de încredere bazat pe o mască model și utilizați caractere care sunt incluse în ID, dar nu în numele modelului, aceste dispozitive nu sunt adăugate. Pe o stație de lucru, aceste dispozitive vor fi adăugate la lista de încredere bazată pe o mască ID.

- Când se face upgrade aplicației fără repornirea computerului, componenta Control dispozitive nu aplică reguli de acces dispozitivelor care sunt reconectate. Cu toate acestea, dacă dispozitivul a fost conectat înainte de upgrade, componenta Control dispozitive aplică regulile corect. Repornește computerul pentru ca aplicația să funcționeze corect cu dispozitivele care sunt reconectate.

- Pe computerele pe care este instalat Kaspersky Endpoint Security versiunea 12.0, modul de acces la imprimantă **Permite și nu înregistra în jurnal** pentru tipul de dispozitive **Imprimante în rețea** se numește **În funcție de magistrala de conectare**, dacă pe computer este aplicată politica componentei Kaspersky Endpoint Security versiunea 12.1. În aceste moduri aplicația efectuează aceleași acțiuni. În Kaspersky Endpoint Security versiunea 12.1, modul de acces pentru imprimantele în rețea este numit corect **Permite și nu înregistra în jurnal**.

- Începând cu Kaspersky Endpoint Security 12.0 for Windows, aplicația permite configurarea regulilor de imprimare pentru imprimante (control imprimare). După instalarea aplicației cu control imprimare sau efectuarea upgrade-ului aplicației la o versiune cu control imprimare, trebuie să reporniți computerul. Până la repornirea computerului, Kaspersky Endpoint Security nu aplică regulile de imprimare și poate controla doar accesul la imprimante. Dacă repornirea computerului afectează negativ fluxurile de lucru din organizația dvs., puteți reporni doar serviciul spoolsv (Derulator de imprimare). Controlul imprimării nu este acceptat pe computerele bazate pe arhitectura Arm.

- Începând cu Kaspersky Endpoint Security 12.0 for Windows, protocolul WPA3 este acceptat de aplicație pentru dispozitivele de tip **Wi-Fi**. Dacă pe un computer este aplicată o politică Kaspersky Endpoint Security versiunea 12.2, protocolul WPA2 este selectat pe computerele cu Kaspersky Endpoint Security versiunea 11.11.0 și anterioară; WPA2 / WPA3 este selectat pentru versiunile de 12.0 până la 12.1; WPA3 este selectat pentru versiunile 12.2 și versiunile ulterioare.

- Dispozitivele Apple sunt clasificate ca dispozitive portabile (MTP) și dispozitive iTunes. Sistemul de operare poate identifica greșit conexiunea dispozitivului Apple și este posibil să nu determine dispozitivul Apple drept un dispozitiv portabil (MTP). Prin urmare, dispozitivul Apple va fi indisponibil în managerul de fișiere, dar va fi accesibil în aplicația iTunes. Drept urmare, Kaspersky Endpoint Security va controla accesul la dispozitivul Apple numai în aplicația iTunes. Pentru a vă accesa dispozitivul Apple drept dispozitiv portabil (MTP), trebuie să accesați Device Manager și să eliminați Apple Mobile Device USB Driver din lista USB Controllers. După repornirea computerului, sistemul de operare va identifica dispozitivul Apple drept un dispozitiv portabil (MTP) și dispozitiv iTunes. Kaspersky Endpoint Security va controla accesul la dispozitiv atât în aplicația iTunes, cât și în managerul de fișiere.

- În Kaspersky Endpoint Security 12.3 for Windows, setările de acces sunt diferite pentru tipul de dispozitive **Bluetooth**. Dacă ați specificat valoarea **În funcție de magistrala de conectare** în versiunea anterioară a aplicației, atunci, după actualizarea aplicației la versiunea 12.3, valoarea configurată se schimbă în **Permite și nu înregistra în jurnal**. Acest lucru nu modifică comportamentul dispozitivului.

- Componenta Control dispozitive acceptă dispozitive Bluetooth numai prin stiva Bluetooth Microsoft Windows. Componenta Control dispozitive poate funcționa incorect cu stivele Bluetooth terțe.
- Dacă dispozitivul Bluetooth ascunde sau falsifică Clasa de Dispozitiv (COD), componenta Control dispozitive poate funcționa incorect.
- Pe computerele cu Windows 7 sau Windows 8 cu anumite drivere Realtek Bluetooth dongle, ar putea să nu fie posibil să se permită doar conectarea dispozitivelor Bluetooth ca dispozitive de intrare (clasa HID). Adică, dacă interziceți accesul la dispozitivele Bluetooth în setările aplicației și adăugați dispozitivele de intrare la excluderi, este posibil ca componenta Control dispozitive să împiedice în schimb accesul la toate dispozitivele Bluetooth.

Control Web

- Formatele OGV și WEBM nu sunt acceptate.
- Protocolul RTMP nu este acceptat.
- Web Control acceptă numai WSL1. Aplicația nu controlează traficul WSL2.

Control adaptiv al anomaliilor

- Este recomandat să creați automat excluderi pe baza evenimentului. Când adăugați manual o excludere, adăugați caracterul `*` la începutul căii atunci când specificați obiectul țintă.
- Un raport al regulii de control adaptiv al anomaliilor nu poate fi generat dacă eșantionul include chiar și un eveniment al cărui nume conține mai mult de 260 de caractere.
- Adăugarea excluderilor din depozitul Declanșarea controlului anomaliei adaptive a regulilor nu este acceptată dacă proprietățile unui obiect sau ale unui proces au o valoare compusă din mai mult de 256 de caractere (de exemplu, calea către obiect). Puteți adăuga manual o excludere în setările politicii. De asemenea, puteți adăuga o excludere în Raportul privind regulile de Control adaptiv a anomaliilor declanșate.
- Kaspersky Security Center 15.1 nu poate genera un raport detaliat **Raport cu privire la starea regulilor funcției Control adaptiv al anomaliilor** raport pentru o anumită regulă.

Criptare unitate (FDE)

- Kaspersky Disk Encryption nu este acceptat pe computerele bazate pe arhitectura ARM.
- Funcția BitLocker Drive Encryption nu este acceptată pe computerele care execută Windows Home.
- După instalarea aplicației, trebuie să reporniți sistemul de operare astfel încât criptarea hard diskului să funcționeze corect.
- Agentul de Autentificare nu acceptă hieroglifele sau caracterele speciale `|` și `\`.
- Pentru funcționarea optimă a computerului după criptare, este necesar ca procesorul să accepte setul de instrucțiuni AES-NI (Intel Advanced Encryption Standard New Instructions). Dacă procesorul nu acceptă AES-NI, performanța computerului poate să scadă.
- Atunci când există procese care încearcă să acceseze dispozitive criptate înainte ca aplicația să acorde acces la astfel de dispozitive, aplicația afișează un avertisment în care se menționează că astfel de procese trebuie încheiate. Dacă procesele nu pot fi încheiate, reconectați dispozitivele criptate.
- ID-urile unice ale unităților hard disk sunt afișate în statisticile de criptare a dispozitivului în format inversat.
- Nu este recomandat să formatați dispozitivele în timp ce acestea sunt criptate.

- Când mai multe unități amovibile sunt conectate simultan la un computer, politica de criptare poate fi aplicată numai unei singure unități amovibile. Când dispozitivele amovibile sunt reconectate, politica de criptare se aplică corect.

- Criptarea poate să nu pornească pe un hard disk puternic fragmentat. Defragmentați hard diskul.

- Când unitățile hard disk sunt criptate, hibernarea este blocată din momentul în care începe activitatea de criptare până la prima repornire a unui computer care rulează Microsoft Windows 7/8/8.1/10 și după instalarea criptării hard diskului până la prima repornire a sistemelor de operare Microsoft Windows 8/8.1/10. Când hard diskurile sunt decriptate, hibernarea este blocată din momentul în care unitatea de pornire este complet decriptată până la prima repornire a sistemului de operare. Când opțiunea Pornire rapidă este activată în Microsoft Windows 8/8.1/10, blocarea hibernării vă împiedică să închideți sistemul de operare.

- Computerele care rulează Windows 7 nu permit schimbarea parolei în timpul recuperării, atunci când discul este criptat cu tehnologia BitLocker. După introducerea cheii de recuperare și încărcarea sistemului, Kaspersky Endpoint Security nu îi solicită utilizatorului să schimbe parola sau codul PIN. Astfel, este imposibil să setați o nouă parolă sau un cod PIN. Această problemă apare din cauza particularităților sistemului de operare. Pentru a continua, trebuie să criptați din nou unitatea de disc.

- Nu se recomandă utilizarea instrumentului xbootmgr.exe cu furnizori suplimentari activi. De exemplu, Dispatcher, Network sau Drivers.

- Formatarea unei unități amovibile criptate nu este acceptată pe un computer care are instalat Kaspersky Endpoint Security for Windows.

- Formatarea unei unități amovibile criptate cu sistemul de fișiere FAT32 nu este acceptată (unitatea este afișată ca fiind criptată). Pentru a formata o unitate, reformatați-o la sistemul de fișiere NTFS.

- Mai mulți agenți de descărcare nu pot coexista pe un computer criptat.

- O încercare de a restabili o imagine a unui disc GPT bootabil într-o stare necriptată, sistemul de operare poate face sistemul de operare inoperabil. Pentru a evita acest lucru, urmează aceste recomandări:

  - Decriptează complet discul înainte de a restaura imaginea din copia de rezervă.

  - Utilizează copierea sector cu sector când creezi imaginea.

  - Șterge datele de pe primele sectoare ale discului criptat înainte de a restaura imaginea și reinițializează discul.

- Este imposibil să accesați o unitate amovibilă care a fost criptată anterior pe un alt computer atunci când sunt îndeplinite simultan toate condițiile următoare:

  - Nu există nicio conexiune la serverul Kaspersky Security Center.

  - Utilizatorul încearcă autorizarea cu un jeton sau o parolă nouă.

  Dacă apare o situație similară, reporniți computerul. După repornirea computerului, va fi acordat accesul la unitatea amovibilă criptată.

- Este posibil ca descoperirea dispozitivelor USB de către Agentul de Autentificare să nu fie acceptată atunci când modul xHCI pentru USB este activat în setările BIOS.

- Kaspersky Disk Encryption (FDE) pentru partea SSD a unui dispozitiv care este utilizat pentru stocarea în cache a celor mai frecvent utilizate date nu este acceptată pentru dispozitivele SSHD.

- Criptarea unităților hard disk pe sistemele de operare pe 32 de biți Microsoft Windows 8/8.1/10 care rulează în modul UEFI nu este acceptată.

- Reporniți computerul înainte de a cripta din nou un hard disk decriptat.

- Criptarea hard diskului nu este compatibilă cu Kaspersky Anti-Virus for UEFI. Nu este recomandat să utilizați criptarea hard diskului pe computerele care au instalat Kaspersky Anti-Virus for UEFI.

- Crearea conturilor Agent de Autentificare pe baza conturilor Microsoft este acceptată cu următoarele limitări:

  - Tehnologia Single Sign-On nu este acceptată.

  - Crearea automată a conturilor Agent de Autentificare nu este acceptată dacă este selectată opțiunea de a crea conturi pentru utilizatorii care se conectează la sistem în ultimele N zile.

- Dacă numele unui cont de Agent de Autentificare are formatul `<domain>/<Windows account name>`, după schimbarea numelui computerului, trebuie să schimbați și numele conturilor care au fost create pentru utilizatorii locali ai acestui computer. De exemplu, imaginați-vă că există un utilizator local `Ivanov` pe computerul `Ivanov` și un cont de Agent de Autentificare cu numele `Ivanov/Ivanov` a fost creat pentru acest utilizator. Dacă numele computerului `Ivanov` a fost schimbat în `Ivanov-PC`, trebuie să schimbați numele contului de Agent de Autentificare pentru utilizatorul `Ivanov` de la `Ivanov/Ivanov` la `Ivanov-PC/Ivanov`. Puteți schimba numele contului, utilizând activitatea de gestionare a contului local a Agentului de autentificare. Înainte ca numele contului să fie schimbat, autentificarea în mediul de preîncărcare este posibilă utilizând numele vechi (de exemplu, `Ivanov/Ivanov`).

- Dacă unui utilizator i se permite să acceseze un computer care a fost criptat utilizând tehnologia Kaspersky Disk Encryption numai utilizând un jeton și acest utilizator trebuie să finalizeze procedura de recuperare a accesului, asigurați-vă că acestui utilizator i se acordă acces bazat pe parolă la acest computer după ce accesul la computerul criptat a fost restaurat. Parola setată de utilizator la restabilirea accesului ar putea să nu fie salvată. În acest caz, utilizatorul va trebui să finalizeze procedura de restabilire a accesului la computerul criptat din nou la următoarea repornire a computerului.

- Când decriptați un hard disk folosind Instrumentul de recuperare FDE, procesul de decriptare se poate încheia cu o eroare dacă datele de pe dispozitivul sursă sunt suprascrise cu datele decriptate. O parte din datele de pe hard disk vor rămâne criptate. Este recomandat să alegeți opțiunea de a salva datele decriptate într-un fișier în setările de decriptare a dispozitivului atunci când utilizați Instrumentul de recuperare FDE.

- Dacă parola Agentului de Autentificare a fost modificată, apare un mesaj care conține textul *Parola dvs. a fost modificată cu succes. Faceți clic pe OK* și utilizatorul repornește computerul, noua parolă nu este salvată. Vechea parolă trebuie utilizată pentru autentificarea ulterioară în mediul de preîncărcare.

- Criptarea discului este incompatibilă cu tehnologia Intel Rapid Start.

- Criptarea discului este incompatibilă cu tehnologia ExpressCache.

- În unele cazuri, atunci când încercați să decriptați o unitate criptată utilizând Instrumentul de recuperare FDE, instrumentul detectează în mod eronat starea dispozitivului ca „necriptat" după ce procedura „Solicitare-Răspuns" este finalizată. Jurnalul instrumentului arată un eveniment care afirmă că dispozitivul a fost decriptat cu succes. În acest caz, trebuie să reporniți procedura de recuperare a datelor pentru a decripta dispozitivul.

- După ce plug-inul Kaspersky Endpoint Security for Windows este actualizat în Consola Web, proprietățile computerului client nu afișează cheia de recuperare BitLocker până la repornirea serviciului Consolei Web.

- Pentru a vedea celelalte limitări ale compatibilității de criptare completă a discului și o listă de dispozitive pentru care criptarea hard diskurilor este acceptată cu restricții, consultați Baza de cunoștințe a suportului tehnic.

File Level Encryption (FLE)

- Criptarea fișierelor nu este acceptată pe computerele bazate pe arhitectura Arm.
- Criptarea fișierelor și a directoarelor nu este acceptată pe sistemele de operare Microsoft Windows Embedded.
- După ce ați instalat aplicația, trebuie să reporniți sistemul de operare astfel încât criptarea fișierelor și a directoarelor să funcționeze corect.
- Aplicația acceptă criptarea fișierelor numai pe dispozitive cu sisteme de fișiere NTFS și FAT32. Dacă un fișier criptat este transferat pe un dispozitiv cu un sistem de fișiere neacceptat (de exemplu, exFAT), fișierul de pe dispozitivul respectiv nu va fi criptat și va putea fi modificat.
- Dacă un fișier criptat este stocat pe un computer care are funcționalități de criptare disponibile și accesați fișierul de pe un computer în care criptarea nu este disponibilă, va fi furnizat acces direct la acest fișier. Un fișier criptat care este stocat într-un director de rețea pe un computer cu funcționalitate de criptare disponibilă este copiat în formă decriptată pe un computer care nu are funcționalitate de criptare disponibilă.
- Vă recomandăm să decriptați fișierele care au fost criptate cu Encrypting File System înainte de a cripta fișiere cu Kaspersky Endpoint Security for Windows.
- După ce un fișier este criptat, dimensiunea acestuia crește cu 4 KB.
- După ce un fișier este criptat, atributul *Arhivă* este setat în proprietățile fișierului.
- Când copiezi fișierul decriptat, de exemplu, pe un suport amovibil, fișierul poate rămâne criptat. Acest lucru se poate întâmpla deoarece, atunci când managerul de fișiere (de exemplu, explorer.exe) încearcă să obțină acces la fișierul criptat, acesta salvează hash-ul fișierului într-o listă specială a procesului. După decriptarea fișierului, atunci când managerul de fișiere încearcă să obțină acces la fișier, procesul caută hash-ul fișierului în listă. Dacă hash-ul este găsit, Kaspersky Endpoint Security lasă fișierul criptat. Pentru a evita acest lucru, trebuie să golești lista procesului. Sistemul de operare golește automat lista procesului pe măsură ce se umple. Poți să golești lista și manual. Pentru aceasta, poți să repornești computerul, să repornești procesul pe care îl utilizezi pentru a obține acces la fișier (de exemplu, explorer.exe) sau poți să utilizezi alt manager de fișiere pe care nu l-ai folosit pentru accesul la fișierul criptat.
- Dacă un fișier dezarhivat dintr-o arhivă criptată are același nume cu un fișier deja existent pe computerul dvs., fișierul deja existent va fi suprascris de către noul fișier, care este dezarhivat din arhiva criptată. Utilizatorul nu este informat despre operațiunea de suprascriere.
- Înainte să despachetați o arhivă criptată, asigurați-vă că aveți suficient spațiu liber pe disc pentru a găzdui fișierele dezarhivate. Dacă nu aveți suficient spațiu pe disc, dezambalarea arhivei poate fi finalizată, dar fișierele pot fi alterate. În acest caz, este posibil ca Kaspersky Endpoint Security să nu afișeze niciun mesaj de eroare.
- Interfața Manager de fișiere portabil nu afișează mesaje despre erorile care apar în timpul funcționării sale.
- Kaspersky Endpoint Security for Windows nu pornește Manager de fișiere portabil pe un computer care are instalată componenta File Level Encryption.
- Nu puteți utiliza Manager de fișiere portabil pentru a accesa o unitate amovibilă dacă următoarele condiții sunt adevărate simultan:
  - Nu există nicio conexiune la Kaspersky Security Center.
  - Kaspersky Endpoint Security for Windows este instalat pe computer.
  - Criptarea datelor (FDE sau FLE) nu a fost efectuată pe computer.

Accesul nu este posibil chiar dacă știți parola pentru Managerul de fișiere portabil.

- Când se utilizează criptarea fișierelor, aplicația este incompatibilă cu clientul de e-mail Sylpheed.
- Kaspersky Endpoint Security for Windows nu acceptă regulile de restricționare a accesului la fișierele criptate pentru unele aplicații. Acest lucru se datorează faptului că unele acțiuni ale fișierelor sunt executate de o aplicație terță. De exemplu, copierea fișierelor este executată de managerul de fișiere și nu de aplicația în sine. Astfel, dacă accesul la fișierele criptate este refuzat pentru clientul de e-mail Outlook, Kaspersky Endpoint Security va permite clientului de e-mail să acceseze fișierul criptat, dacă utilizatorul a copiat fișierele în mesajul de e-mail, prin intermediul clipboardului sau utilizând funcția glisare și fixare. Operațiunea de copiere a fost executată de un manager de fișiere, pentru care regulile restricționării accesului la fișierele criptate nu sunt specificate, de ex. accesul este permis.
- Când unitățile amovibile sunt criptate cu compatibilitate pentru modul portabil, controlul vârstei parolei nu poate fi dezactivat.
- Modificarea setărilor fișierului de pagină nu este acceptată. Sistemul de operare utilizează valorile implicite în locul valorilor specificate ale parametrilor.
- Utilizați eliminarea sigură atunci când lucrați cu unități amovibile criptate. Nu putem garanta integritatea datelor dacă unitatea amovibilă nu este îndepărtată în siguranță.
- După ce fișierele sunt criptate, originalele necriptate ale acestora sunt șterse în siguranță.
- Sincronizarea fișierelor offline utilizând memoria cache în partea clientului Client-Side Caching (CSC) nu este acceptată. Criptarea fișierelor offline sau tehnologia Branch Caching prin SMB pentru servere nu este acceptată. Se recomandă interzicerea gestionării offline a resurselor partajate la nivel de politică de grup. Fișierele care sunt în modul offline pot fi editate. După sincronizare, modificările aduse unui fișier offline pot fi pierdute.
- Crearea unei arhive criptate în rădăcina hard diskului sistemului nu este acceptată.
- Este posibil să aveți probleme la accesarea fișierelor criptate prin rețea. Vă sfătuim să mutați fișierele într-o altă sursă sau să vă asigurați că computerul utilizat ca server de fișiere este gestionat de același server de administrare Kaspersky Security Center.
- Schimbarea aspectului tastaturii poate cauza blocarea ferestrei de introducere a parolei pentru o arhivă criptată cu auto-extragere. Pentru a rezolva această problemă, închideți fereastra de introducere a parolei, comutați la aspectul implicit al tastaturii din sistemul dvs. de operare și reintroduceți parola pentru arhiva criptată.
- Când criptarea fișierelor este utilizată pe sistemele care au mai multe partiții pe un disc, vi se recomandă să utilizați opțiunea care determină automat dimensiunea fișierului pagefile.sys. După repornirea computerului, fișierul pagefile.sys se poate deplasa între partițiile de disc.
- După aplicarea regulilor de criptare a fișierelor, inclusiv a fișierelor din directorul *Documentele mele*, asigurați-vă că utilizatorii pentru care a fost aplicată criptarea pot accesa cu succes fișierele criptate. Pentru a face acest lucru, solicitați fiecărui utilizator să se conecteze la sistem atunci când este disponibilă o conexiune la Kaspersky Security Center. Dacă un utilizator încearcă să acceseze fișiere criptate fără o conexiune la Kaspersky Security Center, sistemul se poate bloca.
- Dacă fișierele de sistem sunt cumva incluse în domeniul criptării la nivel de fișier, evenimentele referitoare la erori din timpul criptării acestor fișiere pot apărea în rapoarte. Fișierele specificate în aceste evenimente nu sunt de fapt criptate.
- Procesele Pico nu sunt acceptate.

- Căile care țin cont de majuscule și minuscule nu sunt acceptate. Când se aplică reguli de criptare sau reguli de decriptare, căile din evenimentele produsului sunt afișate cu litere mici.

- Nu se recomandă criptarea fișierelor utilizate de sistem la pornire. Dacă aceste fișiere sunt criptate, o încercare de a accesa fișierele criptate fără o conexiune la Kaspersky Security Center poate cauza blocarea sistemului sau poate duce la solicitări de acces la fișiere necriptate.

- Dacă utilizatorii lucrează împreună cu un fișier prin rețea în conformitate cu regulile FLE prin aplicații care utilizează metoda de mapare fișier-memorie (cum ar fi WordPad sau FAR) și aplicații concepute pentru a lucra cu fișiere mari (cum ar fi Notepad++), fișierul într-o formă necriptată poate fi blocat la nesfârșit fără posibilitatea de a-l accesa de pe computerul pe care se află.

- Kaspersky Endpoint Security nu criptează fișierele care se află în spațiul de stocare în cloud OneDrive sau în alte directoare care se numesc OneDrive. Kaspersky Endpoint Security blochează, de asemenea, copierea fișierelor criptate în directoarele OneDrive dacă acele fișiere nu sunt adăugate la regula de decriptare.

- Când este instalată componenta de criptare la nivel de fișier, gestionarea utilizatorilor și a grupurilor nu funcționează în modul WSL (Windows Subsystem for Linux).

- Când este instalată componenta de criptare la nivel de fișier, POSIX (Portable Operating System Interface) pentru redenumirea și ștergerea fișierelor nu este acceptat.

- Nu este recomandat să criptați fișierele temporare, deoarece acest lucru poate provoca pierderi de date. De exemplu, Microsoft Word creează fișiere temporare atunci când procesează un document. Dacă fișierele temporare sunt criptate, dar fișierul original nu este, utilizatorul poate primi o eroare *Acces refuzat* când încercați să salvați documentul. În plus, Microsoft Word ar putea salva fișierul, dar nu va fi posibil să deschideți documentul data viitoare, adică datele se vor pierde. Pentru a preveni pierderea datelor, trebuie să excludeți directorul cu fișiere temporare din regulile de criptare.

Detection and Response (EDR, NDR, MDR, XDR, Sandbox)

- Nu poți scana un obiect carantinat ca urmare a activității *Move file to Quarantine*.

- Nu se poate carantina un Alternate Data Stream (ADS) mai mare de 4 MB. Kaspersky Endpoint Security omite orice ADS-uri atât de mari fără a notifica utilizatorul.

- Kaspersky Endpoint Security nu execută activitățile *IOC Scan* pe unitățile de rețea în cazul în care calea directorului din proprietățile activității începe cu o literă a unității. Kaspersky Endpoint Security acceptă numai formatul de cale UNC pentru activitățile *IOC Scan* pe unitățile de rețea. De exemplu, `\\server\shared_folder`.

- Pentru a vă asigura că activitatea *IOC Scan* care utilizează termenii EmailItem funcționează corect, plug-inul web Kaspersky Endpoint Security trebuie actualizat la cea mai recentă versiune.

- Pe computerele bazate pe arhitectura Arm, activitatea *IOC Scan* acceptă fișiere de e-mail doar de la următorii clienți de e-mail: Versiunile pe 32 și 64 de biți ale Outlook 2016 și Outlook 2021, 2024 și 365 pentru Arm64.

- Importul unui fișier de configurare al aplicației se finalizează cu o eroare dacă setarea Integration with Kaspersky Sandbox este activată în fișierul de configurare. Înainte de exportarea setărilor aplicației, dezactivați Kaspersky Sandbox. Apoi efectuați procedura de export/import. După importarea fișierului de configurare, activați Kaspersky Sandbox.

- La importarea unei politici dintr-un fișier KLP, valoarea parametrului care determină acceptarea termenilor și condițiilor Acordului Kaspersky Detection and Response Expert nu se aplică. Prin urmare, după importarea politicii, Kaspersky Endpoint Security nu va mai îndeplini funcțiile Agentului EDR. Pentru ca Agentul EDR să funcționeze, deschide politica, modifică orice parametru și salvează setările politicii.

- Când un indicator de compromitere este detectat în timpul executării activității *IOC Scan*, aplicația carantinează un fișier numai pentru termenul Fileltem. Carantinarea unui fișier pentru alte termene nu este acceptată.

- Pentru gestionarea detaliilor alertelor este necesar plug-inul web Kaspersky Endpoint Security for Windows 11.7.0 sau o versiune ulterioară. Detaliile alertelor sunt necesare când se lucrează cu soluțiile Endpoint Detection and Response (EDR Optimum și EDR Expert). Detaliile detectărilor sunt disponibile numai în Kaspersky Security Center Web Console și Kaspersky Security Center Cloud Console.

- Migrarea configurației [KES+KEA] la configurația [KES+agent incorporat] se poate finaliza cu o eroare de eliminare a aplicației Kaspersky Endpoint Agent. Eroarea de eliminare a aplicației este remediată în cea mai recentă versiune a Kaspersky Endpoint Agent. Pentru a elimina Kaspersky Endpoint Agent, reporniți computerul și creați o activitate de eliminare a aplicației.

- Configurația [KES+KEA+agent încorporat] nu este acceptată. O astfel de configurație perturbă interacțiunea dintre aplicații și soluția Detection and Response care este implementată în organizația dvs. În plus, utilizarea Kaspersky Endpoint Agent și a agentului încorporat pe același computer poate duce la duplicarea telemetriei și la creșterea încărcării pe computer și rețea. După migrarea la configurația [KES+agent încorporat], asigurați-vă că Kaspersky Endpoint Agent a fost eliminat de pe computer. Dacă Kaspersky Endpoint Agent continuă să funcționeze după migrare, dezinstalați manual aplicația (de exemplu, folosind activitatea *Uninstall application remotely*).

  Programul de instalare vă permite să instalați Kaspersky Endpoint Agent pe un computer pe care este instalat Kaspersky Endpoint Security și agentul încorporat. Kaspersky Endpoint Agent și agentul încorporat pot fi, de asemenea, instalate pe un computer ca urmare a activității *Modificare componente ale aplicației*. Comportamentul depinde de versiunile componentelor Kaspersky Endpoint Security și Kaspersky Endpoint Agent.

- Când generează detalii despre alertă, aplicația furnizează informații despre amenințarea detectată, inclusiv codurile hash ale fișierelor modificate. Kaspersky Endpoint Security calculează hash-ul fișierului în timp ce generează detalii despre alertă. Ține cont de faptul că hash-ul inițial al fișierului atunci când a fost generat evenimentul de modificare a fișierului poate să nu fie același cu hash-ul calculat când au fost generate detaliile alertei.

- Agentul încorporat, EDR (KATA), reia izolarea în rețea a unui computer după repornirea unui computer, chiar dacă perioada de izolare a expirat. Pentru a preveni izolarea repetată a computerului, trebuie să dezactivați izolarea rețelei în consola Kaspersky Anti Targeted Attack Platform.

- Vă recomandăm să efectuați un upgrade aplicației după ce Izolarea rețelei se încheie. După efectuarea upgrade-ului pentru Kaspersky Endpoint Security, Izolarea rețelei poate fi oprită.

- Agenții încorporați pentru EDR (KATA), EDR Optimum și EDR Expert nu sunt compatibili unul cu celălalt. Prin urmare, activarea agentului încorporat EDR cu o licență independentă Kaspersky Endpoint Detection and Response Add-on poate fi omisă dacă ați activat Kaspersky Endpoint Security cu diferite funcționalități EDR. De exemplu, activarea agentului încorporat EDR (KATA) cu o licență independentă este omisă dacă ați activat Kaspersky Endpoint Security cu licența [KES + EDR Optimum].

- În Kaspersky Endpoint Security versiunea 12.1, EDR (KATA) agent încorporat nu acceptă următoarele metafișiere pentru activitatea *Obține metafișiere NTFS*: $Secure:$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. A fost adăugat suport pentru aceste metafișiere în Kaspersky Endpoint Security versiunea 12.2.

- Când se realizează migrarea de la Kaspersky Endpoint Agent la Kaspersky Endpoint Security pentru soluția Kaspersky Anti Targeted Attack Platform (EDR), este posibil să întâmpinați erori atunci când conectați computerul la serverele Central Node. Motivul îl constituie faptul că expertul de migrare Web Console omite următoarele setări ale politicii și nu le migrează:

  - Interzicerea modificării setărilor **Connection settings** („lacăt").

    În mod implicit, setările pot fi modificate („lacătul" este deschis). Prin urmare, setările nu sunt aplicate pe computer. Trebuie să interziceți modificarea setărilor și să închideți „lacătul".

  - Crypto-container.

    Dacă utilizați autentificarea mutuală pentru conectarea la serverele Central Node, trebuie să adăugați din nou cripto-containerul. Expertul de migrare migrează corect certificatul TLS pe server.

  Expertul de migrare a politicii și activității în Consola de administrare (MMC) migrează toate setările pentru soluția Kaspersky Anti Targeted Attack Platform (EDR).

- Starea de activare a aplicației este afișată incorect atunci când aplicația este instalată în modul Endpoint Detection and Response Agent pentru a accepta soluția Kaspersky Managed Detection and Response fără conexiune la Kaspersky Security Center. După descărcarea fișierului BLOB, zona de notificare din bara de activități Windows afișează o stare incorectă: *Aplicația nu este activată*. Cu toate acestea, interfața aplicației afișează corect starea de activare. Repornește computerul pentru ca aplicația să funcționeze corect.

- Kaspersky Endpoint Security permite integrarea cu soluția Kaspersky Anti Targeted Attack Platform folosind componenta EDR (KATA) sau Endpoint Sensor (neacceptat). Reține că poți utiliza doar una dintre componente pentru a interacționa cu Kaspersky Anti Targeted Attack Platform. Pentru a vedea starea componentei, deschide proprietățile computerului în Consola de administrare (MMC), în secțiunea **Applications**, deschide proprietățile Kaspersky Endpoint Security for Windows și accesează secțiunea **Components**. Următoarele considerații speciale se aplică pentru afișarea stării componentelor pentru interacțiunea cu Kaspersky Anti Targeted Attack Platform:

  - Pentru plug-in-ul de gestionare 12.0 și versiunile anterioare, aplicația afișează starea curentă a **Endpoint Sensor**. În Kaspersky Endpoint Security 12.0 și versiunile anterioare, componenta EDR (KATA) nu este disponibilă. Componenta EDR (KATA) a fost introdusă în versiunea 12.1.

  - Pentru plug-in-ul de gestionare 12.1 și versiunile ulterioare, aplicația afișează starea generală a **Endpoint Detection and Response (KATA)**, ceea ce poate însemna fie starea Endpoint Sensor, fie starea componentei EDR (KATA). Aceasta depinde de versiunea aplicației instalată pe computerul utilizatorului și de componentele disponibile pe care le poți utiliza pentru a interacționa cu Kaspersky Anti Targeted Attack Platform.

- Începând cu Kaspersky Endpoint Security versiunea 12.6 și versiunile ulterioare, Kaspersky Security Center Web Console versiunea 14.2 și versiunile anterioare nu afișează corect numele componentei **Endpoint Detection and Response (KATA)** în proprietățile computerului. În locul componentei **Endpoint Detection and Response (KATA)**, aplicația afișează numele componentei **Endpoint Detection and Response Expert (KATA EDR)**. Pentru a vedea lista componentelor, deschide proprietățile computerului în Web Console, în secțiunea **Applications**, deschide proprietățile Kaspersky Endpoint Security for Windows și accesează secțiunea **Components**. Începând cu Kaspersky Security Center Web Console versiunea 15.1 și versiunile ulterioare, aplicația afișează corect numele componentei.

- La actualizarea plug-in-ului de gestionare Kaspersky Endpoint Detection and Response la versiunea 15.3 instalat în versiunile 14.0-14.2 ale Web Console, detaliile alertelor sunt afișate incorect. Pentru ca detaliile alertelor să funcționeze corect, repornește Serverul de administrare Kaspersky Security Center.

- Plug-in-ul de gestionare Kaspersky Endpoint Detection and Response versiunea 15.4 și versiunile ulterioare nu este compatibil cu Kaspersky Security Center versiunea 14.0. După actualizarea plug-in-ului de administrare, detaliile alertelor sunt afișate incorect.

- Soluțiile Kaspersky Extended Detection and Response (XDR) versiunea 1.4 nu sunt compatibile cu plug-in-ul web Kaspersky Endpoint Security for Windows versiunea 12.12 sau o versiune ulterioară. Poți să păstrați versiunea actuală a plug-in-ului web sau să actualizezi soluția XDR la versiunea 2.0 sau o versiune ulterioară.

- Kaspersky Endpoint Security nu trimite obiecte destinate arhitecturii Arm către Kaspersky Sandbox.

- Integrarea cu Kaspersky Endpoint Detection and Response Expert nu este acceptată pe computerele bazate pe arhitectura ARM.

- Kaspersky Endpoint Security acceptă până la 10.000 de reguli de filtrare a evenimentelor de includere și excludere în EDR Expert (on-premises).

- Regulile de filtrare a evenimentelor EDR Expert (on-premises) nu vor fi transmise de la politică la dispozitivele gestionate pe care se execută Kaspersky Endpoint Security versiunea 14.0 sau o versiune anterioară dacă se depășește limita acceptată pentru regulile de filtrare stocate. Aplicația va afișa un avertisment corespunzător.

Alte limitări

- Sistemele de operare Windows, începând cu versiunea 11 24H2, acceptă tehnologia UDP Receive Segment Coalescing Offload (URO). Tehnologia este activată în mod implicit dacă pe computer sunt instalate o placă de rețea și drivere compatibile. Dezactivarea URO pe computerul unui utilizator poate reduce semnificativ performanța aplicației.

- Kaspersky Endpoint Security acceptă subsistemul WSL (Windows Subsystem for Linux) cu restricții:

  - WSL 1. Aplicația monitorizează traficul de rețea și detectează amenințările prin HTTP/HTTPS. Datorită faptului că Kaspersky Endpoint Security utilizează propriul certificat pentru a scana conexiunile HTTPS securizate, funcționarea unor aplicații terțe poate fi întreruptă.

  - WSL 2. Aplicația nu acceptă WSL 2.

- Dacă aplicația returnează erori sau se blochează în cursul operării, este posibil să repornească automat. Dacă aplicația întâlnește erori recurente care determină blocarea ei, aplicația efectuează următoarele operațiuni:

  1. Dezactivează funcțiile de control și protecție (funcționalitatea de criptare rămâne activată).

  2. Îl notifică pe utilizator că funcțiile au fost dezactivate.

  3. Încearcă să restabilească starea operațională a aplicației după actualizarea bazelor de date antivirus sau aplicația unor actualizări ale modulelor aplicației.

- Adresele web adăugate la lista de încredere pot fi procesate incorect.

- În consola Kaspersky Security Center, nu poți salva un fișier pe disc din directorul **Advanced** → **Repositories** → **Active threats**. Pentru a salva fișierul, trebuie să dezinfectezi fișierul infectat. În timpul dezinfectării, aplicația salvează o copie a fișierului în Copie de rezervă. Acum poți salva fișierul pe disc din directorul **Advanced** → **Repositories** → **Backup**.

- Moștenirea setărilor transferului de date pe serverul de administrare (**Setări generale** → **Rapoarte și Spații de stocare** → **Transfer de date pe serverul de administrare**) diferă de moștenirea altor setări. Dacă ai permis modificarea setărilor privind transmiterea datelor în politică („lacătul” este deschis), aceste setări vor fi resetate la valorile implicite în proprietățile computerului local din consolă, dacă nu au fost definite anterior. Dacă aceste setări au fost definite anterior, atunci valorile lor vor fi restaurate. Când ștergi o politică, setările sunt moștenite în același mod. În aceste cazuri, alte setări din proprietățile computerului local sunt moștenite din politică.

- Kaspersky Endpoint Security monitorizează traficul HTTP care corespunde standardelor RFC 2616, RFC 7540, RFC 7541, RFC 7301. Dacă Kaspersky Endpoint Security detectează un alt format de schimb de date în traficul HTTP, aplicația blochează această conexiune pentru a preveni descărcarea fișierelor periculoase de pe Internet.

- Kaspersky Endpoint Security previne comunicarea prin protocolul QUIC. Browserele folosesc protocolul standard de transport (TLS sau SSL) indiferent dacă suportul QUIC este activat în browser sau nu.

- Pot apărea erori de conexiune TLS atunci când software-ul terț funcționează cu biblioteca Libcurl. Acest lucru poate fi legat de certificatul Kaspersky pe care îl folosește Kaspersky Endpoint Security pentru a scana conexiunile criptate. Pentru a continua activitatea, puteți dezactiva validarea certificatului pentru software-ul terț (nu este recomandat) sau puteți adăuga un corp de certificat Kaspersky la stocarea certificatelor cURL. Pentru informații detaliate, consultați Baza de cunoștințe Kaspersky.

- Când Kaspersky Endpoint Security for Windows este pornit pentru prima dată, o aplicație semnată digital poate fi plasată temporar în grupul greșit. Aplicația semnată digital va fi introdusă ulterior în grupul corect.

- În timpul unei rescanări a unui obiect rău intenționat care a fost blocat de un software terț, utilizatorul nu este notificat atunci când amenințarea este detectată din nou. Evenimentul de re-detectare a amenințărilor este afișat în raportul aplicației și în raportul Kaspersky Security Center.

- Raportul Kaspersky Security Center privind criptarea dispozitivului nu va include informații despre dispozitivele care au fost criptate folosind Microsoft BitLocker pe platformele de servere sau pe stațiile de lucru pe care nu este instalată componenta Control dispozitive.

- Nu este posibilă activarea afișării tuturor intrărilor din raport în Kaspersky Security Center Web Console. În Web Console, puteți modifica doar numprul de intrări afișate în rapoarte. În mod implicit, Kaspersky Security Center Web Console afișează 1000 de intrări în raport. Puteți activa afișarea tuturor intrărilor din raport în Consola de administrare (MMC).

- Nu este posibilă setarea afișării a mai mult de 1000 de intrări din raport în Kaspersky Security Center Console. Dacă setați o valoare mai mare de 1000, Kaspersky Security Center Console va afișa doar 1000 de intrări în raport.

- Când utilizați o ierarhie de politici, setările secțiunii Criptare unități amovibile dintr-o politică copil sunt accesibile pentru editare dacă politica părinte interzice modificarea acestor setări.

- Trebuie să activați Audit Logon în setările sistemului de operare pentru a asigura funcționarea corectă a excluderilor pentru protecția directoarelor partajate împotriva criptării externe.

- Dacă protecția directorului partajat este activată, Kaspersky Endpoint Security for Windows monitorizează încercările de criptare a directoarelor partajate pentru fiecare sesiune de acces la distanță care a fost inițiată înainte de pornirea Kaspersky Endpoint Security for Windows, inclusiv dacă computerul de la care a fost inițiată sesiunea de acces la distanță a fost adăugat la excluderi. Dacă nu doriți ca Kaspersky Endpoint Security for Windows să monitorizeze încercările de criptare a directoarelor partajate pentru sesiunile de acces de la distanță care au fost inițiate de pe un computer care a fost adăugat la excluderi și care au fost inițiate înainte de pornirea Kaspersky Endpoint Security for Windows, închideți și restabiliți sesiunea de acces la distanță sau reporniți computerul pe care este instalat Kaspersky Endpoint Security for Windows.

- Dacă activitatea de actualizare se execută cu permisiunile unui anumit cont de utilizator, patch-urile de produs nu vor fi descărcate la actualizarea dintr-o sursă care necesită autorizare.

- Aplicația nu poate porni din cauza performanței insuficiente a sistemului. Pentru a rezolva această problemă, utilizează opțiunea Ready Boot sau crește timpul de expirare al sistemului de operare pentru pornirea serviciilor.

- Aplicația nu poate funcționa în Windows în Safe Mode.

- Nu putem garanta că controlul audio va funcționa până la prima repornire după instalarea aplicației.

- În Consola de administrare (MMC), în setările componentei Intrusion Prevention din fereastra pentru configurarea permisiunilor aplicației, butonul **Elimină** este indisponibil. Puteți elimina o aplicație dintr-un grup de încredere prin meniul contextual al aplicației.

- În Interfața locală a aplicației, în setările Intrusion Prevention, permisiunile aplicației și resursele protejate nu sunt disponibile pentru vizualizare în cazul în care computerul este gestionat de o politică. Sunt disponibile opțiunile de defilare, căutare, filtrare și alte comenzi de control a ferestrelor. Puteți vizualiza permisiunile applicației în proprietățile politicii din Kaspersky Security Center Console.

- Când sunt activate fișierele de urmărire rotite, nu sunt create urmăriri pentru componenta AMSI și plug-inul Outlook.

- Urmărirea performanței nu poate fi colectată manual în Windows Server 2008.

- Urmărirea performanței pentru tipul de urmărire „Repornire" nu este acceptată.

- Înregistrarea în jurnal a dump-ului nu este acceptată pentru procesele pico.

- Dezactivarea opțiunii **Dezactivează gestionarea externă a serviciilor de sistem** nu îți va permite să oprești serviciul aplicației care a fost instalată cu parametrul `AMPPL=1` (în mod implicit, valoarea parametrului este setată la `1` începând cu versiunea Windows 10RS2 a sistemului de operare). Parametrul `AMPPL` cu valoarea `1` permite utilizarea tehnologiei Procese de protecție pentru serviciul produsului.

- Pentru a rula o scanare personalizată a unui director, utilizatorul care pornește scanarea personalizată trebuie să aibă permisiunile pentru a citi atributele acestui director. În caz contrar, scanarea directoarelor personalizate va fi imposibilă și se va termina cu o eroare.

- Când o regulă de scanare definită într-o politică include o cale fără caracterul `\` la sfârșit, de exemplu, `C:\folder1\folder2`, scanarea va fi rulată pentru calea `C:\folder1\`.

- Dacă utilizați politicile de restricționare a software-ului (Software Restriction Policies, SRP), computerul poate să nu se încarce (ecran negru). Pentru a preveni funcționarea defectuoasă, trebuie să permiți utilizarea bibliotecilor aplicației în proprietățile SRP. În proprietățile SRP, adaugă regula cu nivelul de securitate **Nerestricționat** pentru fișierul khkum.dll (elementul de meniu **Regulă hash nouă**). Fișierul se află în directorul `C:\Program Files (x86)\Common Files\Kaspersky Lab\KES.14.1\klhk\klhk_x64\`. Dacă ai selectat această metodă, trebuie să debifezi caseta de selectare **Descarcă actualizările modulelor aplicației** în setările activității *Actualizare* pentru Kaspersky Endpoint Security. Pentru detalii despre utilizarea SRP, consultați documentația Microsoft.

  De asemenea, poți să dezactivezi SRP și să utilizezi componenta Application Control a Kaspersky Endpoint Security pentru a controla utilizarea aplicației.

- În cazul în care computerul aparține unui domeniu sub Obiectul policiticilor de grup Windows (Group Policy Object, GPO) cu parametrul DriverLoadPolicy setat la 8 (Good only), repornirea computerului cu Kaspersky Endpoint Security instalat provoacă un BSOD. Pentru a preveni un eșec, parametrul Early Launch Antimalware (ELAM) din Politici de grup trebuie să fie setat la 1 (Good and unknown). Setările ELAM sunt localizate în politică în: **Computer Configuration** → **Administrative Templates** → **System** → **Early Launch Antimalware**.

- Gestionarea setărilor plug-inului Outlook prin API-ul Rest nu este acceptată.

- Setările de rulare a activităților pentru un anumit utilizator nu pot fi transferate între dispozitive printr-un fișier de configurare. După ce setările sunt aplicate dintr-un fișier de configurare, specificați manual numele de utilizator și parola.

- După instalarea unei actualizări, activitatea de verificare a integrității nu funcționează până când sistemul nu este repornit pentru a aplica actualizarea.

- Când nivelul de urmărire rotit este modificat prin utilitarul de diagnosticare la distanță, Kaspersky Endpoint Security for Windows afișează incorect o valoare necompletată pentru nivelul de urmărire. Cu toate acestea, fișierele de urmărire sunt scrise în conformitate cu nivelul de urmărire corect. Când nivelul de urmărire rotit este modificat prin interfața locală a aplicației, nivelul de urmărire este corect modificat, dar utilitarul de diagnosticare la distanță afișează incorect nivelul de urmărire care a fost definit ultima dată de utilitar. Acest lucru poate determina ca administratorul să nu aibă informații actualizate despre nivelul curent de urmărire, iar informațiile relevante pot fi absente din urmăriri dacă un utilizator schimbă manual nivelul de urmărire în interfața locală a aplicației.

- În interfața locală, setările protecției prin parolă nu permit schimbarea numelui contului de administrator (KLAdmin în mod implicit). Pentru a schimba numele contului de administrator, trebuie să dezactivați Protecție prin parolă, apoi să activați Protecție prin parolă și să specificați un nou nume pentru contul de administrator.

- Când aplicația Kaspersky Endpoint Security este instalată pe un server Windows Server 2019 este incompatibilă cu Docker. Implementarea containerelor Docker pe un computer cu Kaspersky Endpoint Security cauzează o eroare (BSOD).

- Dacă Kaspersky Endpoint Security este instalat pe un server al DBMS-ului SQL Server, aplicația trimite cereri către instanța serverului. Acest lucru este necesar pentru a scana activitățile Agentului SQL Server și a împiedica executarea activităților rău intenționate. Kaspersky Endpoint Security utilizează contul de utilizator SQL Server pentru a scana activități. Aplicația trimite cereri către server atunci când se scanează memoria sistemului și după actualizarea bazelor de date antivirus.

- Compatibilitatea Kaspersky Endpoint Security și software-ul Secret Net Studio este limitată:

  - Aplicația Kaspersky Endpoint Security nu este compatibilă cu componenta Antivirus a software-ului Secret Net Studio.

    Aplicația nu poate fi instalată pe un computer unde Secret Net Studio este implementat cu componenta Antivirus. Pentru a face posibilă interoperabilitatea, trebuie să elimini componenta Antivirus din Secret Net Studio.

  - Aplicația Kaspersky Endpoint Security nu este compatibilă cu componenta Protecție disk și criptare date a software-ului Secret Net Studio.

    Aplicația nu poate fi instalată pe un computer pe care Secret Net Studio este implementat alături de componenta Protecție disc și criptare date. Pentru a face posibilă interoperabilitatea, trebuie să elimini componenta Protecție disk și criptare date din Secret Net Studio.

  - Secret Net Studio nu este compatibil cu componenta File Level Encryption (FLE) a Kaspersky Endpoint Security.

    Când instalezi Kaspersky Endpoint Security cu componenta File Level Encryption (FLE), Secret Net Studio poate funcționa cu erori. Pentru a asigura interoperabilitatea, trebuie să elimini componenta File Level Encryption (FLE) din Kaspersky Endpoint Security.

- La importul regulilor componentei Monitorizare integritate sistem, aplicația verifică ID-ul și numele regulii. Dacă ID-urile regulilor sunt aceleași, Kaspersky Endpoint Security înlocuiește regulile existente cu noua regulă. La exportul regulilor, aplicația atribuie automat ID-uri. Pot exista reguli cu ID-uri identice, de exemplu, dacă ați editat manual fișierele XML cu reguli exportate. Dacă ID-urile regulilor sunt unice, dar numele regulilor sunt aceleași, Kaspersky Endpoint Security adaugă `(1)` și așa mai departe la numele regulii.

- Începând cu versiunea 12.11 a Kaspersky Endpoint Security for Windows, nu este posibil să vizualizați setările unei politici părinte deschise într-un grup copil în Consola Web. Consola Web afișează și un avertisment: *This policy is inherited. You can edit the policy settings only in the administration group in which it was created*.

- Notificările pop-up mai lungi de 256 de caractere nu sunt afișate în Consola de administrare (MMC).

- Numele componentelor din politică și din pachetul de instalare pot fi diferite. De exemplu, produsul Endpoint Detection and Response Expert (on-premises) poate fi denumit Endpoint Detection and Response (KATA), Endpoint Detection and Response Expert (on-premises) sau Kaspersky Anti Targeted Attack Platform Integration. Denumirile componentelor pot varia, de asemenea, în funcție de versiunea aplicației.

Glosar

Activitate

Funcții efectuate de aplicația Kaspersky ca activități, de exemplu: Protecția fișierelor în timp real, Scanare completă dispozitiv, Actualizare bază de date.

Adresă normalizată pentru o resursă Web

Forma normalizată a adresei unei resurse Web este o reprezentare textuală, obținută prin normalizare, a adresei resursei Web. *Normalizarea* este un proces prin care reprezentarea textuală a adresei resursei web este modificată în conformitate cu anumite reguli (de exemplu, excluderea numelui de conectare a utilizatorului, a parolei și a portului de conectare din reprezentarea textuală a adresei resursei web; de asemenea, adresa resursei web este modificată din caractere majuscule în caractere minuscule).

În ceea ce privește funcționarea componentelor protecției, scopul normalizării adresei unei resurse Web este evitarea scanării adreselor de site-uri Web care pot diferi ca sintaxă deși sunt echivalente fizic.

Exemplu:

Formă nenormalizată a unei adrese: www.Exemplu.com\.

Formă normalizată a unei adrese: www.exemplu.com\.

Agent de Autentificare

Interfață care îți permite să finalizezi autentificarea pentru a accesa unități hard disc criptate și a încărca sistemul de operare după criptarea unității hard disc de încărcare.

Agent de rețea

O componentă Kaspersky Security Center care permite interacțiunea dintre serverul de administrare și aplicațiile Kaspersky care sunt instalate într-un nod de rețea specific (stație de lucru sau server). Această componentă este comună pentru toate aplicațiile Kaspersky care se execută în Windows. Versiunile dedicate de Agent de rețea sunt destinate aplicațiilor care se execută în alte sisteme de operare.

Alarmă falsă

O alarmă falsă apare atunci când aplicația Kaspersky raportează un fișier neinfectat ca fiind infectat, deoarece semnătura fișierului este asemănătoare cu aceea a unui virus.

Arhivă

Unul sau mai multe fișiere împachetate într-un singur fișier comprimat. Pentru împachetarea și despachetarea datelor este necesară o aplicație specializată denumită arhivator.

Autentificare Kerberos

Mecanism de autentificare mutuală între client și server, înainte de stabilirea unei conexiuni între ei, ceea ce permite comunicarea prin rețele nesecurizate. Mecanismul se bazează pe un tichet, pe care utilizatorul îl obține de la un centru de autentificare de încredere.

Bază de date de adrese Web de phishing

O listă de adrese Web pe care specialiștii Kaspersky le-au stabilit ca fiind legate de activitatea de phishing. Baza de date este actualizată cu regularitate și face parte din kitul de distribuție a aplicației Kaspersky.

Bază de date de adrese Web periculoase

O listă de adrese Web al căror conținut poate fi considerat periculos. Lista este creată de specialiștii Kaspersky. Ea este actualizată cu regularitate și este inclusă în kitul de distribuție a aplicației Kaspersky.

Baze de date antivirus

Baze de date care conțin informații despre amenințările la adresa securității computerului cunoscute de Kaspersky la momentul lansării bazei de date antivirus. Semnăturile din baza de date antivirus ajută la detectarea codului rău intenționat din obiectele scanate. Bazele de date antivirus sunt create de specialiștii Kaspersky și sunt actualizate din oră în oră.

Certificat licență

Un document pe care Kaspersky îl transferă utilizatorului odată cu fișierul cheie sau codul de activare. Conține informații despre licența acordată utilizatorului.

Cheie activă

O cheie care este utilizată curent de aplicație.

Cloud Discovery

Cloud Discovery gestionează accesul utilizatorilor la serviciile cloud. Serviciile cloud includ, de exemplu, Microsoft Teams, Salesforce și Microsoft Office 365. Serviciile cloud sunt grupate în categorii, de exemplu, *Partajare fișiere*, *Programe de mesagerie*, *E-mail*.

Dezinfectare

O metodă de procesare a obiectelor infectate, care conduce la recuperarea totală sau parțială a datelor. Nu toate obiectele infectate pot fi dezinfectate.

Domeniu de protecție

Obiectele care sunt scanate constant de către componenta Essential Threat Protection atunci când aceasta se execută. Proprietățile domeniilor de protecție diferă de la o componentă la alta.

Domeniu de scanare

Obiectele pe care le scanează aplicația Kaspersky Endpoint Security atunci când efectuează o activitate de scanare.

Emitent certificat

Centrul de certificare care a emis certificatul.

Fișier infectabil

Un fișier care, din cauza structurii sau formatului său, poate fi utilizat de intruși ca „recipient" pentru stocarea și răspândirea de cod rău intenționat. De regulă, acesta este un fișier executabil, cu extensia .com, .exe sau .dll. Riscul de pătrundere a codului rău intenționat în astfel de fișiere este destul de ridicat.

Fișier infectat

Un fișier care conține cod rău intenționat (cod al unui malware cunoscut detectat la scanarea fișierului). Kaspersky nu recomandă utilizarea unor astfel de fișiere, deoarece pot infecta computerul.

Fișier IOC

Un fișier care conține un set de indicatori de compromitere (IOC) pe care aplicația încearcă să-l potrivească pentru a contoriza o detectare. Probabilitatea de detectare poate fi mai mare dacă se găsesc potriviri exacte cu mai multe fișiere IOC pentru obiect ca urmare a scanării.

Grup de administrare

Un set de dispozitive care partajează funcții comune și un set de aplicații Kaspersky instalate pe ele. Dispozitivele sunt grupate astfel încât pot fi gestionate convenabile ca o singură unitate. Un grup poate include alte grupuri. Este posibilă crearea de politici de grup și activități de grup pentru fiecare aplicație instalată din grup.

IOC

Indicator de compromitere. Un set de date despre un obiect sau o activitate rău intenționată.

Light Agent

Componenta Kaspersky Endpoint Security for Virtualization Light Agent. Este instalată pe fiecare mașină virtuală care trebuie protejată.

Manager de fișiere portabil

Aceasta este o aplicație care furnizează o interfață pentru lucrul cu fișiere criptate de pe unități amovibile atunci când pe computer nu este disponibilă funcționalitatea de criptare.

Mască

Reprezentarea numelui și a extensiei unui fișier utilizând metacaractere

Măștile de fișier pot conține orice caractere permise în numele de fișiere, inclusiv metacaractere:

- Caracterul `*` (asterisc) ține locul oricărui set de caractere, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\*\*.txt` va include toate căile către fișierele cu extensia TXT din directoarele de pe unitatea C:, dar nu și din subdirectoare.

- Două caractere `*` consecutive țin locul oricărui set de caractere (inclusiv un set gol) din numele de fișier sau director, inclusiv caracterele `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\**\*.txt` va include toate căile către fișierele cu extensia TXT localizată în directoarele imbricate în `Folder`, cu excepția `Folder` în sine. Masca trebuie să includă cel puțin un nivel de imbricare. Masca `C:\**\*.txt` nu este o mască validă. Masca ** este disponibilă numai pentru crearea excluderilor de la scanare.

- `?` (semn de întrebare) ține locul oricărui caracter individual, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\???.txt` va include căi pentru toate fișierele din directorul denumit `Folder` care au extensia TXT și un nume format din trei caractere.

Obiect OLE

Un fișier atașat sau un fișier încorporat într-un alt fișier. Aplicațiile Kaspersky permit scanarea obiectelor OLE pentru identificarea virușilor. De exemplu, dacă inserați un tabel Microsoft Office Excel® într-un document Microsoft Office Word, tabelul este scanat ca obiect OLE.

OpenIOC

Standard deschis al descrierilor indicatorului de compromitere (IOC) bazat pe XML și care include peste 500 de indicatori de compromitere diferiți.

Server de integrare

Componenta Kaspersky Endpoint Security for Virtualization Light Agent. Interacționează între componentele Kaspersky Endpoint Security și infrastructura virtuală.

SVM

Mașină virtuală securizată – o mașină virtuală specială pe care este instalat serviciul scanserver (Server de protecție, o componentă a Kaspersky Endpoint Security for Virtualization Light Agent).

Trusted Platform Module

Un microcip dezvoltat pentru a furniza funcții de bază legate de securitate (de exemplu, pentru stocarea cheilor de criptare). De obicei un Trusted Platform Module este instalat pe placa de bază a computerului și interacționează cu alte componente ale sistemului prin magistrala hardware.

Anexe

Această secțiune conține informații care completează corpul documentului.

Anexa 1. Setări aplicație

Puteți utiliza o politică, activități sau interfața aplicației pentru a configura Kaspersky Endpoint Security. Informații detaliate despre componentele aplicației sunt furnizate în secțiunile corespunzătoare.

File Threat Protection

Componenta File Threat Protection îți permite să previi infectarea sistemului de fișiere al unui computer. În mod implicit, componenta File Threat Protection se află permanent în memoria RAM a computerului și scanează în timp real toate fișierele deschise, salvate sau executate. Componenta scanează fișierele de pe toate unitățile computerului, inclusiv de pe unitățile conectate. Componenta oferă protecție computerului cu ajutorul bazelor de date antivirus, a serviciului cloud Kaspersky Security Network și a analizei euristice.

Componenta scanează fișierele accesate de un utilizator sau de o aplicație. Dacă este detectat un fișier periculos, Kaspersky Endpoint Security blochează utilizarea fișierului. Aplicația apoi dezinfectează sau șterge fișierul periculos, în funcție de setările componentei File Threat Protection.

Atunci când se încearcă accesarea unui fișier al cărui conținut este stocat în spațiul de stocare cloud OneDrive, Kaspersky Endpoint Security descarcă și scanează conținutul fișierului.

Setările componentei File Threat Protection

Parametru	Descriere
Nivel de securitate *(disponibil numai în Consola de administrare (MMC) și în interfața Kaspersky Endpoint Security)*	Pentru File Threat Protection, Kaspersky Endpoint Security poate aplica diferite grupuri de setări. Aceste grupuri de setări care sunt stocate în aplicație sunt denumite *niveluri de securitate*: • **Ridicat**. Atunci când este selectat acest nivel de securitate pentru fișiere, componenta File Threat Protection efectuează controlul cel mai strict asupra tuturor fișierelor deschise, salvate și pornite. Componenta File Threat Protection scanează toate tipurile de fișiere, de pe toate unitățile de hard disk, de pe toate unitățile amovibile și de pe toate unitățile de rețea ale computerului. De asemenea, componenta Antivirus pentru fișiere scanează arhivele, pachetele de instalare și obiectele OLE încorporate. • **Recomandat**. Acest nivel de securitate pentru fișiere este recomandat de specialiștii Kaspersky Lab. Componenta File Threat Protection scanează doar tipurile de fișiere specificate, de pe toate unitățile de hard disk, de pe toate unitățile amovibile și de pe toate unitățile de rețea ale computerului, precum și obiectele OLE încorporate. Componenta File Threat Protection nu scanează arhivele și pachetele de instalare. • **Redus**. Setările acestui nivel de securitate pentru fișiere asigură viteza de scanare maximă. Componenta File Threat Protection scanează numai fișierele cu extensiile specificate, de pe toate unitățile de hard disk, de pe toate unitățile amovibile și de pe toate unitățile de rețea ale computerului. Componenta File Threat Protection nu scanează fișierele compuse.
Tipuri de fișiere *(disponibil numai în Consola de administrare (MMC) și în interfața Kaspersky Endpoint Security)*	**Toate fișierele**. Dacă se activează această setare, Kaspersky Endpoint Security verifică toate fișierele, fără excepție (toate formatele și toate extensiile). **Fișiere scanate după format**. Dacă se activează această setare, aplicația scanează numai fișierele infectabile. Înainte de scanarea unui fișier pentru detectarea de cod rău intenționat, se analizează antetul intern al fișierului pentru a se determina formatul fișierului (de exemplu, .txt, .doc sau .exe). De asemenea, scanarea caută fișiere cu anumite extensii de fișiere. **Fișiere scanate după extensie**. Dacă se activează această setare, aplicația scanează numai fișierele infectabile. Formatul fișierului se determină în funcție de extensia sa.

Parametru	Descriere
Domeniu de scanare	Conține obiecte care sunt scanate de către componenta File Threat Protection. Un obiect de scanat poate fi o unitate hard disk, o unitate amovibilă, o unitate de rețea, un director, un fișier sau mai multe fișiere definite de o mască. În mod implicit, componenta File Threat Protection scanează fișierele lansate pe oricare dintre unitățile de hard disk, unitățile amovibile sau unitățile de rețea. Domeniul de protecție pentru aceste obiecte nu poate fi modificat sau șters. Poți doar să excluzi un obiect (cum ar fi unități amovibile) de la scanări.
Învățare programată și analiza semnăturilor *(disponibil numai în Consola de administrare (MMC) și în interfața Kaspersky Endpoint Security)*	Tehnologia Machine și analiza semnăturilor utilizează bazele de date Kaspersky Endpoint Security, care conțin descrieri ale amenințărilor cunoscute și metode de neutralizare a acestora. Protecția care utilizează această metodă asigură un nivel de securitate minim acceptabil. În urma recomandărilor experților Kaspersky, tehnologia Machine learning și analiza semnăturilor este activată în permanență.
Analiză euristică *(disponibil numai în Consola de administrare (MMC) și în interfața Kaspersky Endpoint Security)*	Tehnologia a fost dezvoltată pentru detectarea amenințărilor care nu se pot detecta utilizând versiunea curentă a bazelor de date ale aplicației Kaspersky. Aceasta detectează fișiere care este posibil să fie infectate cu un virus necunoscut sau cu o variație nouă a unui virus cunoscut. Când scanează fișierele pentru codul rău intenționat, analizatorul euristic execută instrucțiunile din fișierele executabile. Numărul de instrucțiuni executate de analizorul euristic depinde de nivelul specificat pentru analizorul euristic. Nivelul analizei euristice asigură un echilibru între gradul de detaliere a căutării de amenințări noi, gradul de solicitare a resurselor sistemului de operare și durata analizei euristice.
Acțiune la detectarea amenințării	**Dezinfectează; șterge dacă dezinfectarea nu reușește**. Dacă selectezi această opțiune, aplicația încearcă automat să dezinfecteze fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, aplicația șterge fișierul. **Dezinfectează; blochează dacă dezinfectarea nu reușește**. Dacă selectezi această opțiune, aplicația încearcă automat să dezinfecteze fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, aplicația blochează fișierul. **Blochează**. Dacă este selectată această opțiune, aplicația blochează automat fișierul infectat fără a încerca să îl dezinfecteze sau să îl șteargă. Înainte de a încerca să dezinfectați sau să ștergeți un fișier infectat, aplicația creează o copie de rezervă a fișierului în cazul în care trebuie să restaurați fișierul sau dacă acesta poate fi dezinfectat în viitor.
Scanează numai fișierele noi și modificate	Scanează numai fișierele noi și acele fișiere care au fost modificate de la ultima dată când au fost scanate. Acest lucru reduce durata unei scanări. Acest mod se aplică atât fișierelor simple, cât și celor compuse.
Scanare arhive	Scanarea arhivelor ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE și a altor arhive. Aplicația scanează arhivele nu doar după extensie, dar și după format. La verificarea arhivelor, aplicația efectuează o dezarhivare recursivă. Acest lucru permite detectarea amenințărilor din arhivele cu mai multe niveluri (o arhivă într-o arhivă).
Scanează pachetele de distribuție	Scanarea pachetelor de distribuție ale aplicațiilor terțe.
Scanează fișierele în formate Microsoft Office	Scanează fișierele Microsoft Office (DOC, DOCX, XLS, PPT și alte extensii Microsoft). Fișierele în format Office includ și obiecte OLE. Aplicația scanează fișierele în format office mai mici de 1 MO, indiferent dacă această casetă de selectare este bifată sau nu.
Scanează fișierele în format de e-mail	Scanează fișiere în format de e-mail. Aplicația scanează fișierele MSG și EML. Fișierele în format de e-mail includ obiecte OLE și fișiere MHT. Kaspersky Endpoint Security scanează fișierele în format de e-mail mai mici de 1 MO, indiferent dacă această casetă de selectare este bifată sau nu.
Nu dezarhiva fișierele compuse mari	Dacă această casetă de selectare este bifată, aplicația nu scanează fișierele compuse a căror dimensiune depășește valoarea specificată. În cazul în care această casetă de selectare este nebifată, aplicația scanează fișierele compuse indiferent de dimensiuni. Aplicația scanează fișierele mari extrase din arhive, indiferent dacă această casetă de selectare este bifată sau nu.

Parametru	Descriere
Dezarhivează fișierele compuse în fundal	În cazul în care caseta de selectare este selectată, aplicația asigură acces la fișierele compuse care sunt mai mari decât valoarea specificată înainte de scanarea acestor fișiere. În acest caz, Kaspersky Endpoint Security despachetează și scanează fișierele compuse în fundal. Aplicația asigură acces la fișierele compuse care sunt mai mici decât această valoare doar după despachetarea și scanarea acestor fișiere. În cazul în care caseta de selectare nu este selectată, aplicația asigură acces la fișierele compuse numai după despachetarea și scanarea fișierelor de orice dimensiune.
Mod de scanare *(disponibil numai în Consola de administrare (MMC) și în interfața Kaspersky Endpoint Security)*	Kaspersky Endpoint Security scanează fișierele accesate de utilizator, sistemul de operare sau o aplicație care rulează sub contul utilizatorului. **Mod inteligent**. În acest mod, componenta File Threat Protection scanează un obiect pe baza analizei operațiilor efectuate asupra obiectului. De exemplu, atunci când se lucrează cu un document Microsoft Office, Kaspersky Endpoint Security scanează fișierul la prima deschidere și la ultima închidere a acestuia. Operațiunile intermediare care suprascriu fișierul nu determină scanarea acestuia. **La accesare și modificare**. În acest mod, componenta File Threat Protection scanează obiecte la fiecare încercare de deschidere sau modificare a acestora. **La accesare**. În acest mod, File Threat Protection scanează obiecte doar la o încercare de deschidere/modificare a acestora. **La executare**. În acest mod, File Threat Protection scanează obiecte numai la o încercare de executare a acestora.
Folosește tehnologia iSwift *(disponibil numai în Consola de administrare (MMC) și în interfața Kaspersky Endpoint Security)*	Această tehnologie permite creșterea vitezei de scanare excluzând de la scanare anumite fișiere. Fișierele sunt excluse de la scanări utilizând un algoritm special care ia în considerare data lansării bazelor de date Kaspersky Endpoint Security, data celei mai recente scanări a fișierului și orice modificare adusă setărilor scanării. Tehnologia iSwift reprezintă o versiune îmbunătățită a tehnologiei iChecker și este destinată sistemului de fișiere NTFS.
Folosește tehnologia iChecker *(disponibil numai în Consola de administrare (MMC) și în interfața Kaspersky Endpoint Security)*	Această tehnologie permite creșterea vitezei de scanare excluzând de la scanare anumite fișiere. Fișierele sunt excluse de la scanări utilizând un algoritm special care ia în considerare data lansării bazelor de date Kaspersky Endpoint Security, data celei mai recente scanări a fișierului și orice modificare adusă setărilor scanării. Există limitări ale tehnologiei iChecker: aceasta nu funcționează în cazul fișierelor mari și se aplică numai la fișierele cu o structură pe care aplicația o recunoaște (de exemplu, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP și RAR).
Pune în pauză File Threat Protection *(disponibil numai în Consola de administrare (MMC) și în interfața Kaspersky Endpoint Security)*	Aceasta oprește temporar și automat funcționarea componentei File Threat Protection la momentul specificat sau când lucrați cu aplicațiile specificate.
Scanarea operațiunilor cu fișiere executate în containerele Windows	Dacă o amenințare este detectată în interiorul unui container, aplicația aplică acțiunea selectată pentru componenta File Threat Protection. **Oprește containerul dacă dezinfectarea eșuează**. Este posibil ca aplicația să nu aibă suficiente drepturi de citire și scriere pentru obiectul detectat. În acest caz, dezinfectarea sau ștergerea obiectului detectat este imposibilă. Dacă această casetă de selectare este bifată, aplicația blochează obiectul detectat și oprește containerul. Dacă această casetă de selectare este debifată, aplicația blochează doar obiectul detectat. **Nu scana operațiunile cu fișiere executate în containerele Windows**. Dacă această casetă de selectare este bifată, aplicația scanează containerul numai la pornirea acestuia. Dacă această casetă de selectare este debifată, aplicația scanează continuu containerul în timp real.

Web Threat Protection

Componenta Web Threat Protection previne descărcarea de pe Internet a fișierelor rău intenționate și, de asemenea, blochează site-urile web rău intenționate și de phishing. Componenta oferă protecție computerului cu ajutorul bazelor de date antivirus, a serviciului cloud Kaspersky Security Network și a analizei euristice.

Kaspersky Endpoint Security scanează traficul HTTP, HTTPS și FTP. Kaspersky Endpoint Security scanează adresele URL și adresele IP.

Pentru a utiliza componenta Web Threat Protection, trebuie să finalizezi configurarea inițială a aplicației:

- Pentru monitorizarea traficului HTTPS, activează scanarea conexiunilor criptate (activată în mod implicit).
- Selectează porturile pe care Kaspersky Endpoint Security trebuie să monitorizeze (implicit, aplicația monitorizează toate porturile).
- Selectează aplicațiile al căror trafic dorești să îl monitorizeze Kaspersky Endpoint Security. Majoritatea browserelor sunt deja prezente în lista de aplicații recomandate de Kaspersky. Dacă browserul tău lipsește din listă, adaugă-l manual.
- Îți recomandăm să injectezi un script de interacțiune a paginii web în traficul web (în mod implicit, injectarea de script este dezactivată). Acest script permite înregistrarea evenimentelor Web Threat Protection pentru jurnalul de evenimente al aplicației, jurnalul de evenimente al sistemului de operare și rapoarte.

Când un utilizator încearcă să deschidă un site web periculos sau de tip phishing, Kaspersky Endpoint Security va bloca accesul și va afișa un avertisment.

Setările componentei Web Threat Protection

Parametru	Descriere
Nivel de securitate *(disponibil numai în Consola de administrare (MMC) și în interfața Kaspersky Endpoint Security)*	Pentru Web Threat Protection, aplicația poate aplica diferite grupuri de setări. Aceste grupuri de setări care sunt stocate în aplicație sunt denumite *niveluri de securitate*: • **Ridicat**. Nivelul de securitate la care componenta Web Threat Protection efectuează o scanare maximă a traficului web pe care un computer îl primește prin protocoalele HTTP și FTP. Web Threat Protection scanează detaliat toate obiectele de trafic Web, utilizând setul complet de baze de date ale aplicației, și efectuează cea mai riguroasă analiză euristică posibil. • **Recomandat**. Nivelul de securitate care asigură raportul optim între performanțele aplicației și securitatea traficului Web. Componenta Web Threat Protection efectuează analiza euristică la nivelul Scanare medie. Acest nivel de securitate a traficului Web este recomandat de specialiștii Kaspersky. • **Redus**. Setările acestui nivel de securitate a traficului web asigură viteza maximă de scanare a traficului web. Componenta Web Threat Protection efectuează analiza euristică la nivelul Scanare ușoară.
Acțiune la detectarea amenințării	**Blochează**. Dacă această opțiune este selectată și un obiect infectat este detectat în traficul web, componenta Web Threat Protection blochează accesul la obiectul respectiv și afișează un mesaj în browser. **Informează**. Dacă această opțiune este selectată și un obiect infectat este detectat în traficul web, Kaspersky Endpoint Security permite descărcarea acestui obiect pe computer, dar adaugă informații despre obiectul infectat în lista de amenințări active.
Verifică adresa web în baza de date cu adrese web rău intenționate *(disponibil numai în Consola de administrare (MMC) și în interfața Kaspersky Endpoint Security)*	Scanarea linkurilor pentru a determina dacă sunt incluse în baza de date cu adrese URL rău intenționate vă permite să urmăriți site-urile web care au fost adăugate în lista respinse. Baza de date de adrese Web rău intenționate este întreținută de Kaspersky, fiind inclusă în pachetul de instalare a aplicației și actualizată prin actualizări ale bazei de date Kaspersky Endpoint Security.
Utilizează analiza euristică *(disponibil numai în Consola de administrare (MMC) și în interfața Kaspersky Endpoint Security)*	Tehnologia a fost dezvoltată pentru detectarea amenințărilor care nu se pot detecta utilizând versiunea curentă a bazelor de date ale aplicației Kaspersky. Aceasta detectează fișiere care este posibil să fie infectate cu un virus necunoscut sau cu o variație nouă a unui virus cunoscut. Atunci când traficul web este scanat pentru viruși și alte aplicații care prezintă o amenințare, analizorul euristic execută instrucțiunile din fișierele executabile. Numărul de instrucțiuni executate de analizorul euristic depinde de nivelul specificat pentru analizorul euristic. Nivelul analizei euristice asigură un echilibru între gradul de detaliere a căutării de amenințări noi, gradul de solicitare a resurselor sistemului de operare și durata analizei euristice.

Parametru	Descriere
Verifică adresa web în baza de date cu adrese web de phishing *(disponibil numai în Consola de administrare (MMC) și în interfața Kaspersky Endpoint Security)*	Baza de date de adrese Web de phishing include adresele Web ale site-urilor Web despre care se cunoaște în prezent că sunt utilizate pentru a lansa atacuri de phisihing. Kaspersky completează această bază de date cu linkuri de phishing cu adrese obținute de la organizația internațională cunoscută ca Anti-Phishing Working Group. Baza de date de adrese de phishing este inclusă în pachetul de instalare a aplicației și completată cu actualizări ale bazei de date Kaspersky Endpoint Security.
Nu se scanează traficul web de la adresele web de încredere	Dacă este selectată această opțiune, componenta Web Threat Protection nu scanează conținutul paginilor sau al site-urilor web ale căror adrese sunt incluse în lista de adrese web de încredere. Puteți adăuga la o listă de adrese URL de încredere atât adresa, cât și masca de adresă a unei pagini/unui site Web. Poți, de asemenea, să creezi o listă generală de excluderi pentru conexiunile criptate. În acest caz, Kaspersky Endpoint Security nu scanează traficul HTTPS al adreselor web de încredere atunci când componentele Web Threat Protection, Mail Threat Protection și Control Web își fac treaba.

Mail Threat Protection

Componenta Mail Threat Protection scanează atașările mesajelor de e-mail primite și trimise în vederea detectării virușilor și a altor amenințări. Componenta oferă protecție computerului cu ajutorul bazelor de date antivirus, a serviciului cloud Kaspersky Security Network și a analizei euristice.

Mail Threat Protection poate scana atât mesajele primite, cât și cele trimise. Aplicația acceptă POP3, SMTP, IMAP și NNTP în următorii clienți de e-mail:

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail
- MyOffice Mail
- R7-Office Organizer

Pentru a scana traficul în clienții de e-mail Mozilla Thunderbird, MyOffice Mail și R7-Office Organizer, trebuie să adaugi un certificat Kaspersky la magazinul de certificate și să selectezi propriul magazin de certificate.

Mail Threat Protection nu acceptă alte protocoale și clienți de e-mail.

Este posibil ca Mail Threat Protection să nu poată obține întotdeauna acces *la nivel de protocol* la mesaje (de exemplu, atunci când utilizați soluția Microsoft Exchange). Din acest motiv, Mail Threat Protection include o extensie pentru Microsoft Office Outlook. Extensia permite scanarea mesajelor la *nivelul clientului de mail*. Extensia Mail Threat Protection acceptă versiunile pe 32 de biți și pe 64 de biți ale Outlook 2010, 2013, 2016, 2019, 2021, 2024 și 365. Pe computerele bazate pe arhitectura Arm, extensia Mail Threat Protection acceptă versiunile pe 32 de biți și 64 de biți ale Outlook 2016, Outlook 2021, Outlook 2024 și Outlook 365 pentru Arm64.

Componenta Mail Threat Protection nu scanează mesajele dacă clientul de e-mail este deschis într-un browser.

Când un fișier rău intenționat este detectat într-un atașament, Kaspersky Endpoint Security adaugă informații despre acțiunea efectuată la subiectul mesajului, de exemplu, *[Mesajul a fost procesat]<subiect mesaj>*.

Parametru	Descriere
Nivel de securitate *(disponibil numai în Consola de administrare (MMC) și în interfața Kaspersky Endpoint Security)*	Pentru Mail Threat Protection, aplicația poate aplica diferite grupuri de setări. Aceste grupuri de setări care sunt stocate în aplicație sunt denumite *niveluri de securitate*: • **Ridicat**. Atunci când este selectat acest nivel de securitate pentru e-mail, componenta Mail Threat Protection scanează mesajele de e-mail cât mai complet. Componenta Mail Threat Protection scanează mesajele primite și trimise și efectuează o analiză euristică profundă. Nivelul Ridicat de securitate a e-mailurilor este recomandat pentru mediile cu risc ridicat. Un exemplu de astfel de mediu este o conexiune la un serviciu de e-mail gratuit de la o rețea de domiciliu neapărată de o protecție pentru e-mail centralizată. • **Recomandat**. Nivelul de securitate pentru e-mail care asigură echilibrul optim între performanțele aplicației și securitatea pentru e-mail. Componenta Mail Threat Protection scanează mesajele de e-mail primite și trimise și efectuează o analiză euristică de nivel mediu. Acest nivel de securitate pentru e-mail este recomandat de specialiștii de la Kaspersky. • **Redus**. Atunci când este selectat acest nivel de securitate pentru e-mail, componenta Mail Threat Protection scanează numai mesajele de e-mail primite, efectuează o analiză euristică rapidă și nu scanează arhivele atașate la mesaje de e-mail. La acest nivel de securitate pentru e-mail, componenta Mail Threat Protection scanează mesajele de e-mail la viteză maximă și utilizează un minim de resurse ale sistemului de operare. Nivelul Redus de securitate pentru e-mail este recomandat pentru lucrul în medii bine protejate. Un exemplu de astfel de mediu poate fi o rețea LAN de întreprindere care deține securitate centralizată pentru e-mail.
Acțiune la detectarea amenințării	**Dezinfectează; șterge dacă dezinfectarea nu reușește**. Când un obiect infectat este detectat într-un mesaj de intrare sau de ieșire, aplicația încearcă să dezinfecteze obiectul detectat. Utilizatorul va putea accesa mesajul cu o atașare sigură. Dacă obiectul nu poate fi dezinfectat, aplicația șterge obiectul infectat. Aplicația adaugă informații despre acțiunea efectuată la subiectul mesajului: *[Mesajul a fost procesat] <subiect mesaj>*. **Dezinfectează; blochează dacă dezinfectarea nu reușește**. Când un obiect infectat este detectat într-un mesaj de intrare, aplicația încearcă să dezinfecteze obiectul detectat. Utilizatorul va putea accesa mesajul cu o atașare sigură. Dacă obiectul nu poate fi dezinfectat, aplicația adaugă un avertisment subiectului mesajului. Utilizatorul va putea accesa mesajul cu atașarea originală. Când un obiect infectat este detectat într-un mesaj de ieșire, aplicația încearcă să dezinfecteze obiectul detectat. Dacă obiectul nu poate fi dezinfectat, aplicația blochează transmiterea mesajului, iar clientul de e-mail afișează o eroare. **Blochează**. Dacă un obiect infectat este detectat într-un mesaj de intrare, aplicația adaugă un avertisment la subiectul mesajului. Utilizatorul va putea accesa mesajul cu atașarea originală. Dacă un obiect infectat este detectat într-un mesaj de ieșire, aplicația blochează transmiterea mesajului, iar clientul de e-mail afișează o eroare.
Domeniu de protecție *(disponibil numai în Consola de administrare (MMC) și în interfața Kaspersky Endpoint Security)*	*Domeniul de protecție* include obiecte pe care componenta le verifică atunci când este executată: mesaje primite și trimise sau numai mesaje primite. Pentru a vă proteja calculatoarele, trebuie să scanați doar mesajele primite. Puteți activa scanarea mesajelor trimise pentru a preveni trimiterea fișierelor infectate în arhive. De asemenea, puteți activa scanarea mesajelor trimise dacă doriți să împiedicați trimiterea fișierelor în anumite formate, cum ar fi fișierele audio și video, de exemplu.
Scanează traficul POP3, SMTP, NNTP și IMAP	Scanarea efectuată de componenta Mail Threat Protection a traficului transferat prin protocoalele POP3, SMTP, NNTP și IMAP.
Conectează extensia Microsoft Outlook	Dacă această casetă de selectare este bifată, scanarea mesajelor de e-mail transmise prin protocoalele POP3, SMTP, NNTP, IMAP este activată în extensia integrată în Microsoft Outlook. Dacă mesajele de e-mail sunt scanate folosind extensia pentru Microsoft Outlook, se recomandă folosirea modului Cached Exchange Mode. Pentru informații mai detaliate despre modul Cached Exchange și recomandări privind utilizarea sa, consultați Baza de cunoștințe Microsoft.
Analiză euristică *(disponibil numai în Consola de administrare (MMC) și în interfața Kaspersky Endpoint Security)*	Tehnologia a fost dezvoltată pentru detectarea amenințărilor care nu se pot detecta utilizând versiunea curentă a bazelor de date ale aplicației Kaspersky. Aceasta detectează fișiere care este posibil să fie infectate cu un virus necunoscut sau cu o variație nouă a unui virus cunoscut. Când scanează fișierele pentru codul rău intenționat, analizatorul euristic execută instrucțiunile din fișierele executabile. Numărul de instrucțiuni executate de analizorul euristic depinde de nivelul specificat pentru analizorul euristic. Nivelul analizei euristice asigură un echilibru între gradul de detaliere a căutării de amenințări noi, gradul de solicitare a resurselor sistemului de operare și durata analizei euristice.
Scanează arhivele atașate	Scanarea arhivelor ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE și a altor arhive. Aplicația scanează arhivele nu doar după extensie, dar și după format. La verificarea arhivelor, aplicația efectuează o dezarhivare recursivă. Acest lucru permite detectarea amenințărilor din arhivele cu mai multe niveluri (o arhivă într-o arhivă). Dacă în timpul scanării, aplicația detectează o parolă pentru o arhivă în textul mesajului, această parolă va fi folosită pentru a scana conținutul arhivei în căutarea unor aplicații rău intenționate. În acest caz, parola nu este salvată. O arhivă este dezarhivată în timpul scanării. Dacă apare o eroare a aplicației în timpul procesului de dezarhivare, puteți șterge manual fișierele dezarhivate care sunt salvate pe următoarea cale: %systemroot%\temp. Fișierele au prefixul PR.
Scanează fișierele atașate în formate Microsoft Office	Scanează fișierele Microsoft Office (DOC, DOCX, XLS, PPT și alte extensii Microsoft). Fișierele în format Office includ și obiecte OLE. Aplicația scanează fișierele în format office mai mici de 1 MO, indiferent dacă această casetă de selectare este bifată sau nu.

Parametru	Descriere
Nu scana arhivele mai mari de N MB	Dacă această casetă de selectare este bifată, componenta Mail Threat Protection exclude de la scanare arhivele atașate la mesaje de e-mail, dacă dimensiunea acestora depășește valoarea specificată. Dacă această casetă este debifată, componenta Mail Threat Protection scanează arhivele atașate la mesaje de e-mail indiferent de dimensiunea lor.
Limitează timpul pentru verificarea arhivelor la N sec	Atunci când caseta de selectare este bifată, intervalul de timp alocat pentru scanarea arhivelor atașate la mesaje de e-mail este limitat la perioada specificată.
Filtrare atașări	Filtrarea atașărilor nu se aplică mesajelor de e-mail expediate. **Dezactivează filtrarea**. Dacă este selectată această opțiune, componenta Mail Threat Protection nu filtrează fișierele atașate la mesaje de e-mail. **Redenumește atașările de tipurile selectate**. Dacă această opțiune este selectată, componenta Mail Threat Protection va înlocui ultimul caracter din extensie găsit în fișierele atașate din tipurile specificate cu caracterul de subliniere (de exemplu, attachment.doc_). Astfel, pentru a deschide fișierul, utilizatorul trebuie să redenumească fișierul. **Șterge atașările de tipurile selectate**. Dacă este selectată această opțiune, componenta Mail Threat Protection șterge fișierele atașate de tipurile specificate din mesajele de e-mail. În lista de măști de fișier poți specifica tipurile de fișiere atașate de redenumit sau șters din mesaje de e-mail.

Network Threat Protection

Componenta *Network Threat Protection* (numită și Intrusion Detection System, IDS) monitorizează traficul de rețea de intrare pentru activitatea caracteristică atacurilor de rețea. Când aplicația detectează o încercare de atac asupra rețelei pe computerul unui utilizator, aceasta blochează conexiunea la rețea cu respectivul computer atacator. Descrierile tipurilor de atacuri de rețea cunoscute în prezent și ale modurilor de combatere a acestora sunt furnizate în bazele de date ale aplicației. Lista de atacuri de rețea pe care le detectează componenta Network Threat Protection este actualizată în cursul actualizărilor bazelor de date și modulelor aplicației.

Setările componentei Network Threat Protection

Parametru	Descriere
Tratează scanarea porturilor și supraîncărcarea rețelei ca atacuri	*Supraîncărcare rețea* este un atac asupra resurselor rețelei unei organizații (cum ar fi serverele web). Acest atac constă în trimiterea unui număr mare de soliciăr pentru a supraîncărca lățimea de bandă a resurselor rețelei. Când se întâmplă acest lucru, utilizatorii nu mai pot accesa resursele rețelei organizației. Un atac de tip *Scanare port* constă în scanarea porturilor UDP, TCP și a serviciilor de rețea de pe computer. Acest atac permite atacatorului să identifice gradul de vulnerabilitate al computerului înainte să efectueze tipuri mai periculoase de atacuri de rețea. De asemenea, atacul de tip Scanare port permite atacatorului să identifice sistemul de operare de pe computer și să selecteze atacurile de rețea corespunzătoare pentru acest sistem de operare. Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security monitorizează traficul de rețea pentru a detecta aceste atacuri. Dacă este detectat un atac, aplicația notifică utilizatorul și trimite evenimentul corespunzător către Kaspersky Security Center. Aplicația oferă informații despre computerul atacator, care sunt necesare pentru acțiuni de răspuns la amenințări în timp util. Puteți dezactiva detectarea acestor tipuri de atacuri în cazul în care unele dintre aplicațiile permise efectuează operații tipice pentru aceste tipuri de atacuri. Acest lucru va ajuta la evita alarmelor false.
Blochează dispozitivele atacatoare timp de N min	Dacă această opțiune este activată, componenta Network Threat Protection adaugă computerul atacator la lista de computere blocate. Aceasta înseamnă că componenta Network Threat Protection blochează conectarea rețelei cu un computer agresor după prima încercare de atac asupra rețelei, pentru perioada de timp specificată. Acest lucru protejează automat computerul utilizatorului împotriva posibilelor viitoare atacuri de rețea inițiate de la aceeași adresă. Durata minimă pe care un computer atacator trebuie să o petreacă în lista blocului este de un minut. Durata maximă este de 999 de minute. Puteți vizualiza lista obiectelor blocate în fereastra instrumentului Monitor rețea. Kaspersky Endpoint Security golește lista cu obiecte blocate atunci când aplicația este repornită și când setările componentei Network Threat Protection sunt modificate.

Parametru	Descriere
Excluderi	Lista conține adrese IP de la care componenta Network Threat Protection nu va bloca atacuri de rețea. Puteți adăuga o adresă IP cu portul și protocolul specificate. Aplicația nu înregistrează în jurnal informații despre atacurile de rețea de la adrese IP care se găsesc în lista de excluderi.
Protecție falsificare MAC	Un *atac de falsificare a adresei MAC* constă în schimbarea adresei MAC a unui dispozitiv de rețea (placă de rețea). Drept urmare, un atacator poate redirecționa datele trimise către un dispozitiv către un alt dispozitiv și poate avea acces la aceste date. Kaspersky Endpoint Security vă permite să blocați atacurile de falsificare a adresei MAC și să primiți notificări despre atacuri.

Firewall

Componenta Firewall blochează conexiunile neautorizate la un computer în timp ce lucrezi pe Internet sau într-o rețea locală. Firewall-ul controlează, de asemenea, activitatea de rețea a aplicațiilor de pe computer. Acest lucru vă permite să vă protejați rețeaua LANI corporativă împotriva furturilor de identitate și a altor atacuri. Componenta oferă protecție computerului cu ajutorul bazelor de date antivirus, a serviciului cloud Kaspersky Security Network și a *regulilor de rețea* predefinite.

Agentul de rețea este utilizat pentru interacțiunea cu Kaspersky Security Center. Firewall-ul creează automat regulile de rețea necesare pentru ca aplicația și Agentul de rețea să funcționeze. Ca urmare, componenta Firewall deschide mai multe porturi pe computer. Ce porturi sunt deschise depinde de rolul computerului (de exemplu, punct de distribuție). Pentru a afla mai multe despre porturile care vor fi deschise pe computer, consultă Ajutor Kaspersky Security Center.

Reguli rețea

Puteți configura regulile de rețea la următoarele niveluri:

- *Reguli pentru pachete de rețea*. Regulile pentru pachete de rețea impun restricții asupra pachetelor de rețea, indiferent de aplicație. Astfel de reguli restricționează traficul de rețea la intrare și la ieșire desfășurat prin anumite porturi ale protocolului de date selectat. Kaspersky Endpoint Security are reguli pentru pachetele de rețea predefinite cu permisiunile recomandate de experții Kaspersky.
- *Reguli de rețea pentru aplicații*. Regulile de rețea pentru aplicație impun restricții asupra activității de rețea a unei anumite aplicații. Ele iau în calcul nu numai caracteristicile pachetului de rețea, dar și aplicația căreia îi este adresat sau cea care a emis acest pachet de rețea.

Accesul controlat al aplicațiilor la resursele, procesele sistemului de operare și la datele cu caracter personal este oferit de componenta Host Intrusion Prevention prin utilizarea *drepturilor de aplicație*.

În timpul primei porniri a aplicației, Firewall-ul efectuează următoarele acțiuni:

1. Verifică securitatea aplicației folosind bazele de date antivirus descărcate.
2. Verifică securitatea aplicației în Kaspersky Security Network.

   Vă recomandăm să participați la Kaspersky Security Network pentru a ajuta componenta Firewall să funcționeze mai eficient.

3. Pune aplicația într-unul dintre grupurile de încredere: *De încredere*, *Restricționat la nivel inferior*, *Restricționat la nivel superior*, *Nu este de încredere*.

   Un grup de încredere definește drepturile la care se referă Kaspersky Endpoint Security atunci când controlează activitatea aplicațiilor. Kaspersky Endpoint Security plasează o aplicație într-un grup de încredere în funcție de nivelul de pericol pe care îl poate prezenta această aplicație pentru computer.

   Kaspersky Endpoint Security plasează o aplicație într-un grup de încredere pentru componentele Firewall și Host Intrusion Prevention. Nu poți schimba grupul de încredere numai pentru componentele Firewall sau Host Intrusion Prevention.

   Dacă ați refuzat să participați la KSN sau nu există o rețea, Kaspersky Endpoint Security plasează aplicația într-un grup de încredere, în funcție de setările componentei Host Intrusion Prevention. După primirea reputației aplicației de la KSN, grupul de încredere poate fi schimbat automat.

4. Blochează activitatea de rețea a aplicației în funcție de grupul de încredere. De exemplu, aplicațiile din grupul de încredere *Restricționat la nivel superior* nu au permisiunea să utilizeze conexiunile la rețea.

La următoarea pornire a aplicației, Kaspersky Endpoint Security verifică integritatea aplicației. Dacă aplicația este nemodificată, componenta folosește pentru aceasta regulile curente pentru rețea. Dacă aplicația a fost modificată, Kaspersky Endpoint Security analizează aplicația ca și cum ar fi fost pornită pentru prima dată.

Priorități ale regulilor de rețea

Fiecare regulă are o prioritate. Cu cât o regulă este mai sus în listă, cu atât prioritatea sa este mai mare. Dacă activitatea de rețea este adăugată la mai multe reguli, Firewall-ul reglementează activitatea de rețea în conformitate cu regula cu cea mai mare prioritate.

Regulile pentru pachete de rețea au o prioritate mai mare decât regulile de rețea pentru aplicații. Dacă pentru același tip de activitate de rețea sunt specificate atât reguli pentru pachete de rețea, cât și reguli de rețea pentru aplicații, activitatea de rețea este tratată conform regulilor pentru pachete de rețea.

Regulile de rețea pentru aplicații funcționează într-un anumit mod. Regula de rețea pentru aplicații include reguli de acces bazate pe starea rețelei: *Rețea publică*, *Rețea locală*, *Rețea de încredere*. De exemplu, aplicațiilor din grupul de încredere *Restricționat la nivel superior* nu le este permisă, mod implicit, nicio activitate de rețea în rețele cu toate stările. Dacă o regulă de rețea este specificată pentru o aplicație individuală (aplicație principală), atunci procesele secundare ale altor aplicații vor fi executate conform regulii de rețea a aplicației principale. Dacă nu există o regulă de rețea pentru aplicație, procesele secundare vor fi executate conform regulii de acces la rețea a grupului de încredere al aplicației.

De exemplu, ați interzis orice activitate de rețea în rețele cu toate stările pentru toate aplicațiile, cu excepția browserului X. Dacă începeți instalarea browserului Y (proces secundar) din browserul X (aplicația principală), atunci instalatorul browserului Y va accesa rețeaua și va descărca fișierele necesare. După instalare, browserului Y i se va refuza orice conexiuni la rețea conform setărilor Firewall. Pentru a interzice activitatea de rețea a instalatorului browserului Y ca proces secundar, trebuie să adăugați o regulă de rețea pentru instalatorul browserului Y.

Tipuri de conexiune la rețea

Firewall-ul îți permite să controlezi activitatea în rețea în funcție de tipul conexiunii la rețea. Kaspersky Endpoint Security primește tipul conexiunii la rețea de la sistemul de operare al computerului. Tipul conexiunii la rețea în sistemul de operare este setat de utilizator atunci când configurează conexiunea. Poți schimba tipul conexiunii la rețea în setările Kaspersky Endpoint Security. Firewall-ul va monitoriza activitatea rețelei în funcție de tipul rețelei specificat în setările Kaspersky Endpoint Security și nu în sistemul de operare.

Sunt disponibile următoarele tipuri de conexiune la rețea:

- **Rețea publică**. Rețeaua nu este protejată de aplicații antivirus, firewall-uri sau filtre (cum ar fi rețeaua Wi-Fi dintr-o cafenea). Când utilizatorul folosește un computer conectat la o astfel de rețea, Firewall blochează accesul la fișierele și imprimantele acestui computer. Utilizatorii externi nu pot accesa, de asemenea, date prin directoare partajate și acces la distanță la desktopul acestui computer. Firewall filtrează activitatea de rețea a fiecărei aplicații potrivit regulilor de rețea setate pentru ea.

  Firewall atribuie în mod implicit tipul *Rețea publică* Internetului. Nu poți modifica tipul pentru Internet.

- **Rețea locală**. Rețea pentru utilizatorii cu acces restricționat la fișierele și imprimantele de pe acest computer (cum ar fi pentru o rețea LAN sau o rețea de domiciliu).

- **Rețea de încredere**. Rețea securizată în care computerul nu este expus la atacuri sau încercări neautorizate de accesare a datelor. Firewall permite orice activitate de rețea în rețelele cu această stare.

Setările componentei Firewall

Parametru	Descriere
Reguli de pachet	Tabel cu o listă de reguli pentru pachetul de rețea. Regulile pentru pachete de rețea servesc la impunerea de restricții asupra pachetelor de rețea indiferent de aplicație. Astfel de reguli restricționează traficul de rețea la intrare și la ieșire desfășurat prin anumite porturi ale protocolului de date selectat. Tabelul listează regulile pentru pachete de rețea preconfigurate recomandate de Kaspersky pentru protecție optimă a traficului de rețea pentru computerele care execută sisteme de operare Microsoft Windows. Firewall setează prioritatea de execuție a fiecărei reguli pentru pachete de rețea. Firewall procesează regulile pentru pachete de rețea în ordinea în care ele apar în lista de reguli pentru pachete de rețea, de sus în jos. Componenta Firewall localizează regula pentru pachete de rețea cea mai de sus care este potrivită pentru conexiunea la rețea și o aplică, permițând sau blocând activitatea în rețea. Firewall-ul ignoră apoi toate regulile ulterioare pentru pachetele de rețea pentru conexiunea la rețea respectivă. Regulile pentru pachete de rețea au o prioritate mai mare decât regulile de rețea pentru aplicații.
Rețele disponibile	Acest tabel conține informații despre conexiunile de rețea detectate de componenta Firewall pe computer. Starea pentru *Rețea publică* este atribuită, în mod implicit, pentru Internet. Nu poți modifica starea pentru Internet.
Reguli pentru aplicații	**Aplicație**. Tabel cu aplicațiile controlate de componenta Firewall. Aplicațiile sunt atribuite unor grupuri de încredere. Un grup de încredere definește drepturile utilizate de Kaspersky Endpoint Security atunci când controlează activitatea de rețea a aplicațiilor. Puteți să selectați o aplicație dintr-o singură listă a tuturor aplicațiilor instalate pe computere sub influența unei politici și să adăugați aplicația la un grup de încredere. **Reguli de rețea**. Tabel cu regulile de rețea pentru aplicațiile care fac parte dintr-un grup de încredere. Conform acestor reguli, componenta Firewall reglementează activitatea de rețea a aplicațiilor. Tabelul afișează regulile de rețea predefinite recomandate de experții Kaspersky. Aceste reguli de rețea au fost adăugate pentru a proteja în mod optim traficul de rețea al computerelor care execută sisteme de operare Windows. Nu este posibilă ștergerea regulilor de rețea predefinite.

BadUSB Attack Prevention

Unii viruși modifică firmware-ul dispozitivelor USB pentru a păcăli sistemul de operare să detecteze dispozitivul USB ca tastatură. Ca urmare, virusul poate executa comenzi în contul dvs. de utilizator pentru a descărca programe malware, de exemplu.

Componenta BadUSB Attack Prevention împiedică dispozitivele USB infectate care emulează o tastatură să se conecteze la computer.

Atunci când un dispozitiv USB este conectat la un computer și este identificat drept tastatură de sistemul de operare, aplicația solicită utilizatorului să introducă un cod numeric generat de aplicație de la tastatură sau folosind Tastatura de pe ecran, dacă este disponibilă (consultă figura de mai jos). Această procedură este cunoscută sub numele de Autorizare tastatură.

Dacă a fost introdus corect codul, aplicația salvează parametrii de identificare – VID/PID pentru tastatură și numărul portului la care a fost conectată – în lista de tastaturi autorizate. Autorizarea tastaturii nu trebuie repetată atunci când tastatura este reconectată sau după repornirea sistemului de operare.

Atunci când tastatura autorizată este conectată la un alt port USB al computerului, aplicația afișează din nou o solicitare de autorizare a acestei tastaturi.

Dacă a fost introdus incorect codul numeric, aplicația generează un cod nou. Puteți configura numărul de încercări pentru introducerea codului numeric. În cazul în care codul numeric este introdus incorect de mai multe ori sau fereastra de autorizare a tastaturii este închisă (a se vedea figura de mai jos), aplicația blochează intrarea de pe această tastatură. Atunci când intervalul de blocare al dispozitivului USB trece sau după ce sistemul de operare este repornit, aplicația solicită utilizatorului să efectueze din nou autorizarea tastaturii.

Aplicația permite utilizarea unei tastaturi autorizate și blochează o tastatură care nu a fost autorizată.

Componenta BadUSB Attack Protection nu este instalată implicit. Dacă aveți nevoie de componenta BadUSB Attack Prevention, puteți adăuga componenta în proprietățile pachetului de instalare înainte de a instala aplicația sau de a modifica componentele disponibile ale aplicației după instalarea aplicației.



Autorizare tastatură

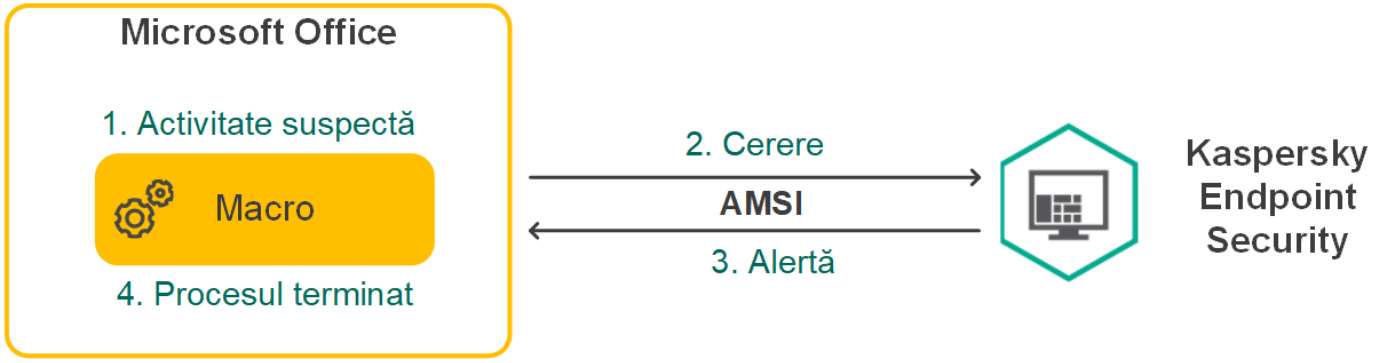
Setările componentei BadUSB Attack Prevention

Parametru	Descriere
Interzice utilizarea Tastaturii de pe ecran pentru autorizarea dispozitivelor USB	În cazul în care comutatorul este activat, aplicația blochează utilizarea Tastaturii de pe ecran pentru autorizarea unui dispozitiv USB, de la care un cod de autorizare nu poate fi introdus.
Interzice utilizarea unui cod de bare pentru autorizarea dispozitivelor USB	Dacă acest comutator este activat, aplicația nu afișează codul de bare în notificarea de autentificare a scanerului de coduri de bare.
Numărul maxim de încercări de autorizare a dispozitivului USB	Blocarea automată a dispozitivului USB în cazul în care codul de autorizare este introdus incorect de numărul specificat de ori. Valorile valide sunt de la 1 la 10. De exemplu, dacă permiți cinci încercări de introducere a codul de autorizare, aplicația blochează dispozitivul USB după a cincea încercare eșuată. Kaspersky Endpoint Security afișează durata blocării dispozitivului USB. După expirarea acestui timp, vei avea din nou 5 încercări de introducere a codului de autorizare.
Expiră când este atins numărul maxim de încercări	Durata blocării dispozitivului USB după numărul specificat de încercări nereușite de introducere a codului de autorizare. Valorile valide sunt de la 1 la 180 (minute).

Protecție AMSI

Componenta Protecție AMSI are rolul de a susține interfața Antimalware Scan Interface de la Microsoft. *Antimalware Scan Interface (AMSI)* permite aplicațiilor terțe cu suport AMSI să trimită obiecte (de exemplu, scripturi PowerShell) către Kaspersky Endpoint Security pentru scanare suplimentară și primește apoi rezultatele scanării pentru aceste obiecte. Aplicațiile terțe pot include, de exemplu, aplicații Microsoft Office (vezi figura de mai jos). Pentru detalii despre AMSI, consultați documentația Microsoft.

Componenta Protecție AMSI poate doar să detecteze o amenințare și să notifice o aplicație terță despre aceasta. O aplicație terță, după primirea unei notificări despre o amenințare, nu permite efectuarea de acțiuni rău intenționate (de exemplu, aceasta încheie acțiunea).



Exemplu funcționare AMSI

Componenta Protecție AMSI poate refuza o solicitare de la o aplicație terță, de exemplu dacă această aplicație depășește numărul maxim de solicitări într-un interval specificat. Kaspersky Endpoint Security trimite informații despre o solicitare respinsă de la o aplicație terță către Serverul de administrare. Componenta AMSI Protection nu respinge solicitările de la acele aplicații terțe pentru care integrarea continuă cu componenta AMSI Protection este activată.

Componenta Protecție AMSI este disponibilă pentru următoarele sisteme de operare pentru stații de lucru și servere:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multi-session;
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise.

- Windows Server 2016 Essentials / Standard / Datacenter (inclusiv modul Server Core);
- Windows Server 2019 Essentials / Standard / Datacenter (inclusiv modul Server Core);
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (inclusiv modul Server Core);
- Windows Server 2025 Standard / Datacenter.

Setări protecție AMSI

Parametru	Descriere
Scanează arhivele	Scanarea arhivelor ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE și a altor arhive. Aplicația scanează arhivele nu doar după extensie, dar și după format. La verificarea arhivelor, aplicația efectuează o dezarhivare recursivă. Acest lucru permite detectarea amenințărilor din arhivele cu mai multe niveluri (o arhivă într-o arhivă).
Scanează pachetele de distribuție	Scanarea pachetelor de distribuție ale aplicațiilor terțe.
Scanează fișierele în formate Microsoft Office	Scanează fișierele Microsoft Office (DOC, DOCX, XLS, PPT și alte extensii Microsoft). Fișierele în format Office includ și obiecte OLE. Aplicația scanează fișierele în format office mai mici de 1 MO, indiferent dacă această casetă de selectare este bifată sau nu.
Nu dezarhiva fișierele compuse mari	Dacă această casetă de selectare este bifată, aplicația nu scanează fișierele compuse a căror dimensiune depășește valoarea specificată. În cazul în care această casetă de selectare este nebifată, aplicația scanează fișierele compuse indiferent de dimensiuni. Aplicația scanează fișierele mari extrase din arhive, indiferent dacă această casetă de selectare este bifată sau nu.

Exploit Prevention

Componenta Exploit Prevention detectează codul programului care profită de vulnerabilitățile de pe un computer pentru a exploata privilegiile de administrator sau pentru a efectua activități dăunătoare. De exemplu, exploiturile pot utiliza un atac de supraîncărcare a memoriei tampon. Pentru a face acest lucru, exploitul trimite o cantitate mare de date unei aplicații vulnerabile. Atunci când prelucrează aceste date, aplicația vulnerabilă execută un cod rău intenționat. În urma acestui atac, exploitul poate porni instalarea neautorizată a unui program malware. Atunci când se încearcă executarea unui fișier executabil al unei aplicații vulnerabile care nu a fost efectuată de utilizator, Kaspersky Endpoint Security blochează executarea acestui fișier sau notifică utilizatorul.

Componenta Exploit Prevention monitorizează suplimentar porturile de rețea pentru procese ale aplicațiilor care pot amenința securitatea computerului. Aplicația obține informații despre astfel de procese cu ajutorul bazelor de date antivirus.

Setările componentei Exploit Prevention

Parametru	Descriere
La detectarea exploatării	**Blochează**. Dacă este selectat acest element, atunci când este detectat un exploit, Kaspersky Endpoint Security blochează operațiunile acestui exploit și înregistrează în jurnal informațiile despre acest exploit. **Informează**. Dacă este selectat acest element, atunci când Kaspersky Endpoint Security detectează o exploatare, înregistrează în jurnal informațiile despre exploatare și adaugă informațiile despre aceasta în lista amenințărilor active.
Activează protecția memoriei pentru procese de sistem	Dacă acest buton de comutare este pornit, Kaspersky Endpoint Security blochează procesele externe care încearcă să acceseze memoria pentru procese de sistem.

Behavior Detection

Componenta Behavior Detection primește date despre acțiunile aplicațiilor de pe computer și transmite aceste informații altor componente de protecție pentru a le îmbunătăți performanța. Componenta Behavior Detection utilizează Semnăturile de flux de comportamental (Behavior Stream Signatures, BSS) pentru aplicații. Dacă activitatea aplicației corespunde unei semnături de șir comportamental, Kaspersky Endpoint Security execută acțiunea de răspuns selectată. Funcționalitatea Kaspersky Endpoint Security se bazează pe semnături de flux comportamental și oferă o apărare proactivă pentru computer.

Componenta Behavior Detection monitorizează suplimentar porturile de rețea pentru procese ale aplicațiilor care pot amenința securitatea computerului. Aplicația obține informații despre astfel de procese cu ajutorul bazelor de date antivirus.

Setările componentei Behavior Detection

Parametru	Descriere
Acțiune la detectarea activității malware	**Șterge**. Dacă această opțiune este selectată, atunci când detectează o activitate periculoasă, Kaspersky Endpoint Security șterge fișierul executabil al aplicației periculoase și creează o copie de rezervă a fișierului în Copie de rezervă. **Blochează**. Dacă această opțiune este selectată, la detectarea unei activități rău intenționate Kaspersky Endpoint Security termină această aplicație. **Informează**. Dacă această opțiune este selectată și se detectează o activitate periculoasă a unei aplicații, Kaspersky Endpoint Security nu oprește aplicația, dar adaugă informații despre activitatea periculoasă a acestei aplicații în lista de amenințări active.

Host Intrusion Prevention

Componenta Host Intrusion Prevention împiedică aplicațiile să execute acțiuni care ar putea fi periculoase pentru sistemul de operare și asigură controlul accesului la resursele sistemului de operare și la datele personale. Componenta oferă protecție computerului cu ajutorul bazelor de date antivirus și a serviciului cloud Kaspersky Security Network.

Componenta controlează funcționarea aplicațiilor folosind *drepturi de aplicație*. Drepturile de aplicație includ următorii parametri de acces:

- Acces la resursele sistemului de operare (de exemplu, opțiuni de pornire automată, chei de registru)
- Acces la date cu caracter personal (de exemplu, fișiere și aplicații)

Activitatea în rețea a aplicațiilor este controlată de componenta Firewall folosind *regulile de rețea*.

În timpul primei porniri a aplicației, componenta Host Intrusion Prevention realizează următoarele acțiuni:

1. Verifică securitatea aplicației folosind bazele de date antivirus descărcate.
2. Verifică securitatea aplicației în Kaspersky Security Network.

Vă recomandăm să participați în Kaspersky Security Network pentru a ajuta componenta Host Intrusion Prevention să funcționeze mai eficient.

3. Pune aplicația într-unul dintre grupurile de încredere: *De încredere*, *Restricționat la nivel inferior*, *Restricționat la nivel superior*, *Nu este de încredere*.

   Un grup de încredere definește drepturile la care se referă Kaspersky Endpoint Security atunci când controlează activitatea aplicațiilor. Kaspersky Endpoint Security plasează o aplicație într-un grup de încredere în funcție de nivelul de pericol pe care îl poate prezenta această aplicație pentru computer.

   Kaspersky Endpoint Security plasează o aplicație într-un grup de încredere pentru componentele Firewall și Host Intrusion Prevention. Nu poți schimba grupul de încredere numai pentru componentele Firewall sau Host Intrusion Prevention.

   Dacă ați refuzat să participați la KSN sau nu există o rețea, Kaspersky Endpoint Security plasează aplicația într-un grup de încredere, în funcție de setările componentei Host Intrusion Prevention. După primirea reputației aplicației de la KSN, grupul de încredere poate fi schimbat automat.

4. Blochează acțiunile aplicației în funcție de grupul de încredere. De exemplu, aplicațiilor din grupul de încredere *Restricționat la nivel superior* le este refuzat accesul la modulele sistemului de operare.

La următoarea pornire a aplicației, Kaspersky Endpoint Security verifică integritatea aplicației. Dacă aplicația este nemodificată, componenta folosește pentru aceasta drepturile curente pentru aplicații. Dacă aplicația a fost modificată, Kaspersky Endpoint Security analizează aplicația ca și cum ar fi fost pornită pentru prima dată.

Setările componentei Host Intrusion Prevention

Parametru	Descriere
Drepturi aplicație	Tabel cu aplicațiile care sunt monitorizate de componenta Host Intrusion Prevention. Aplicațiile sunt atribuite unor grupuri de încredere. Un grup de încredere definește drepturile la care se referă Kaspersky Endpoint Security atunci când controlează activitatea aplicațiilor. Puteți să selectați o aplicație dintr-o singură listă a tuturor aplicațiilor instalate pe computere sub influența unei politici și să adăugați aplicația la un grup de încredere. Drepturile de acces al aplicațiilor sunt prezentate în următoarele tabele: • **Fișiere și registry de sistem**. Tabel cu drepturi de acces pentru resursele sistemului de operare și datele personale pentru aplicațiile care aparțin grupului de încredere. • **Drepturi**. Tabel cu drepturi de acces pentru procesele și resursele sistemului de operare pentru aplicațiile aparținând grupului de încredere. • **Reguli de rețea**. Tabel cu regulile de rețea pentru aplicațiile care fac parte dintr-un grup de încredere. Conform acestor reguli, componenta Firewall reglementează activitatea de rețea a aplicațiilor. Tabelul afișează regulile de rețea predefinite recomandate de experții Kaspersky. Aceste reguli de rețea au fost adăugate pentru a proteja în mod optim traficul de rețea al computerelor care execută sisteme de operare Windows. Nu este posibilă ștergerea regulilor de rețea predefinite.
Resurse protejate	Tabelul conține resursele computerului pe categorii. Componenta Host Intrusion Prevention monitorizează încercările altor aplicații de a accesa resursele din tabel. O resursă poate fi o categorie de registru, un fișier sau director sau o cheie de registru.
Grup de încredere pentru aplicațiile pornite înainte de a porni Kaspersky Endpoint Security	Un grup de încredere în care Kaspersky Endpoint Security va plasa aplicațiile pornite înainte de Kaspersky Endpoint Security.
Actualizează reguli pentru aplicațiile anterior necunoscute de la KSN	Dacă această casetă de selectare este bifată, componenta Host Intrusion Prevention actualizează drepturile pentru aplicații necunoscute anterior utilizând baza de date Kaspersky Security Network.
Ai încredere în aplicațiile semnate digital	Dacă această casetă de selectare este bifată, componenta Host Intrusion Prevention plasează aplicațiile cu semnătura digitală a producătorilor de încredere în grupul *De încredere*. *Producătorii de încredere* sunt acei producători de software în care Kaspersky are încredere. De asemenea, puteți adăuga manual certificatul producătorului în depozitul de certificate de încredere. Dacă această casetă de selectare nu este bifată, componenta Host Intrusion Prevention nu consideră aceste aplicații ca fiind de încredere și folosește alți parametri pentru a determina grupul lor de încredere.

Parametru	Descriere
Șterge regulile pentru aplicațiile nepornite de mai mult de N zile (între 1 și 90)	În cazul în care caseta de selectare este selectată, Kaspersky Endpoint Security șterge automat informațiile despre aplicație (grup de încredere și drepturi de acces) dacă sunt îndeplinite următoarele condiții: • Ați pus manual aplicația într-un grup de încredere sau i-ați configurat drepturile de acces. • Aplicația nu a început în perioada de timp definită. Dacă grupul de încredere și drepturile unei aplicații au fost determinate automat, Kaspersky Endpoint Security șterge informațiile despre această aplicație după 30 de zile. Nu este posibilă modificarea termenului de stocare a informațiilor despre aplicație sau oprirea ștergerii automate. Data viitoare când porniți această aplicație, Kaspersky Endpoint Security analizează aplicația ca și cum ar porni pentru prima dată.
Grup de încredere pentru aplicații care nu au fost incluse în alte grupuri	Elementele din această listă verticală determină grupul de încredere căruia Kaspersky Endpoint Security îi va atribui o aplicație necunoscută. Poți alege unul dintre următoarele elemente: • **Restricționat la nivel inferior**. • **Restricționat la nivel superior**. • **Nu este de încredere**.

Remediation Engine

Componenta Remediation Engine permite Kaspersky Endpoint Security să deruleze înapoi acțiuni care au fost executate de către programe malware în sistemul de operare.

Atunci când se derulează înapoi activitatea programelor malware în sistemul de operare, Kaspersky Endpoint Security tratează următoarele tipuri de activități ale programelor malware:

- **Activitate cu fișiere**

  Kaspersky Endpoint Security efectuează următoarele acțiuni:

  - Șterge fișierele executabile create de malware (pe toate suporturile, cu excepția unităților de rețea).
  - Șterge fișierele executabile create de programe infiltrate de malware.
  - Restaurează fișierele modificate sau șterse de malware.

  Caracteristica de recuperare a fișierelor are un număr de limitări.

- **Activitate de registry**

  Kaspersky Endpoint Security efectuează următoarele acțiuni:

  - Șterge cheile de registru create de malware.
  - Nu restaurează cheile de registru modificate sau șterse de malware.

- **Activitate de sistem**

  Kaspersky Endpoint Security efectuează următoarele acțiuni:

  - Termină procesele care au fost inițiate de malware.
  - Termină procesele în care a pătruns o aplicație rău intenționată.
  - Nu reia procesele care au fost oprite de malware.

- **Activitate în rețea**

  Kaspersky Endpoint Security efectuează următoarele acțiuni:

  - Blochează activitatea de rețea a programelor malware.
  - Blochează activitatea de rețea a proceselor care au fost infiltrate de malware.

O derulare înapoi a acțiunilor unui malware poate fi pornită de componenta File Threat Protection sau Behavior Detection sau în cursul unei scanări malware.

Derularea înapoi a operațiunilor programelor malware afectează un set de date strict definit. Restaurarea nu are efecte adverse asupra sistemului de operare sau asupra integrității datelor computerului tău.

Kaspersky Security Network



Pentru a-ți proteja mai eficient computerul, Kaspersky Endpoint Security folosește informații primite de la utilizatori de pe întregul glob. Kaspersky Security Network este conceput pentru a obține aceste date.

Este posibil ca funcționalitatea KSN să nu fie disponibilă în software în SUA.

Kaspersky Security Network (KSN) este o infrastructură de servicii în cloud care oferă acces la Baza de cunoștințe online Kaspersky, care conține informații despre reputația fișierelor, a resurselor Web și a programelor software. Utilizarea datelor de la Kaspersky Security Network asigură răspunsul mai rapid prin Kaspersky Endpoint Security la noile amenințări, îmbunătățește eficiența unor componente ale protecției și reduce posibilitatea alarmelor false. Dacă participați la Kaspersky Security Network, serviciile KSN furnizează componentei Kaspersky Endpoint Security informații despre reputația adreselor web scanate, precum și informații despre categoria și reputația fișierelor scanate. Pentru mai multe detalii despre configurarea accesului la KSN, consultă Ajutor pentru Kaspersky Security Center.

Utilizarea Kaspersky Security Network este facultativă. Aplicația îți solicită să utilizezi KSN în cursul configurării inițiale a aplicației. Utilizatorii pot începe sau pot întrerupe participarea la KSN în orice moment.

Pentru informații mai detaliate despre trimiterea informațiilor statistice Kaspersky generate în cursul participării la KSN și despre stocarea și distrugerea acestor informații, consultați Kaspersky Security Network Statement și site-ul Web Kaspersky. Fișierul ksn_<ID limbă>.txt care conține textul Declarației Kaspersky Security Network este inclus în kitul de distribuție al aplicației.

Infrastructura bazelor de date Kaspersky privind reputația

Kaspersky Endpoint Security acceptă următoarele soluții de infrastructură pentru lucrul cu bazele de date Kaspersky privind reputația:

- *Kaspersky Security Network (KSN)* este soluția folosită de majoritatea aplicațiilor Kaspersky. Participanții KSN primesc informații de la Kaspersky Security Network și trimit către Kaspersky informații despre obiecte detectate pe computerul utilizatorului, pentru a fi analizate suplimentar de analiștii Kaspersky și pentru a fi incluse în bazele de date privind reputația și în cele statistice.

- *Kaspersky Private Security Network (KPSN)* este o soluție care permite utilizatorilor de computere care găzduiesc Kaspersky Endpoint Security sau alte aplicații Kaspersky să obțină acces la bazele de date privind reputația ale Kaspersky și la alte date statistice, fără a trimite date către Kaspersky de la propriile lor computere. KPSN este conceput pentru clienții corporativi care nu pot participa la Kaspersky Security Network din oricare dintre următoarele motive:

  - Stațiile de lucru locale nu sunt conectate la Internet.

Transmiterea oricăror date în afara țării sau în afara rețelei locale corporative este interzisă prin lege sau restricționată de politicile de securitate corporativă.

Setări pentru Kaspersky Security Network

Parametru	Descriere
Activează modul KSN extins	*Mod KSN extins* este un mod în care Kaspersky Endpoint Security trimite date suplimentare către Kaspersky. Kaspersky Endpoint Security folosește KSN pentru a detecta amenințările, indiferent de poziția de comutare.
Activează modul Cloud	*Mod cloud* se referă la modul de operare al aplicației în care Kaspersky Endpoint Security utilizează o versiune light a bazelor de date antivirus. Kaspersky Security Network acceptă funcționarea aplicației atunci când sunt utilizate baze de date antivirus light. Versiunea light a bazelor de date antivirus vă permite să utilizați aproximativ jumătate din memoria RAM a computerului care ar fi, altfel, utilizată cu bazele de date obișnuite. Dacă nu participați la Kaspersky Security Network sau dacă modul cloud este dezactivat, Kaspersky Endpoint Security descarcă versiunea completă a bazelor de date antivirus de pe serverele Kaspersky. Dacă butonul de comutare este pornit, Kaspersky Endpoint Security folosește versiunea redusă a bazelor de date antivirus, ceea ce reduce încărcarea resurselor sistemului de operare. Kaspersky Endpoint Security descarcă versiunea redusă a bazelor de date antivirus la următoarea actualizare după bifarea casetei de selectare. Dacă butonul de comutare este oprit, Kaspersky Endpoint Security folosește versiunea completă a bazelor de date antivirus. Kaspersky Endpoint Security descarcă versiunea completă a bazelor de date antivirus la următoarea actualizare după debifarea casetei de selectare.
Stare computer atunci când serverele KSN sunt indisponibile *(disponibil numai în consola Kaspersky Security Center)*	Elementele din această listă verticală determină starea unui computer în Kaspersky Security Center atunci când nu sunt disponibile servere KSN.

Parametru	Descriere
Utilizează Serverul de administrare ca server proxy KSN *(disponibil numai în consola Kaspersky Security Center)*	În cazul în care caseta de selectare este bifată, Kaspersky Endpoint Security folosește serviciul KSN Proxy. Puteți configura setările serviciului Proxy KSN în proprietățile Serverului de administrare.
Utilizează serverele Kaspersky Security Network dacă serverul proxy KSN este indisponibil *(disponibil numai în consola Kaspersky Security Center)*	În cazul în care caseta de selectare este bifată, Kaspersky Endpoint Security folosește servere KSN atunci când serviciul KSN Proxy este indisponibil. Serverele KSN pot fi localizate atât la Kaspersky, cât și la terți (atunci când se folosește Kaspersky Private Security Network).

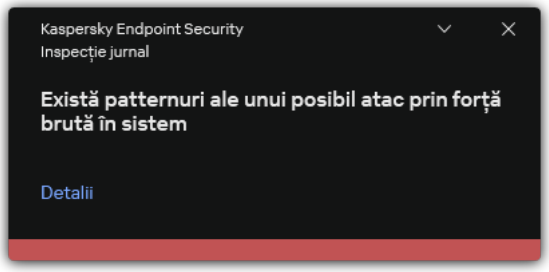
Inspecție jurnal

Această componentă este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Windows pentru servere. Această componentă este indisponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Windows pentru stații de lucru.

Începând cu versiunea 11.11.0, Kaspersky Endpoint Security for Windows include componenta Inspecție jurnal. Componenta Inspecție jurnal monitorizează integritatea mediului protejat pe baza analizei jurnalului de evenimente Windows. Când aplicația detectează semne de comportament atipic în sistem, informează administratorul, deoarece acest comportament poate indica o tentativă de atac cibernetic.

Kaspersky Endpoint Security analizează jurnalele de evenimente Windows și detectează încălcările în conformitate cu regulile. Componenta include reguli predefinite. Regulile predefinite sunt susținute de analiza euristică. Poți, de asemenea, să adăugi propriile reguli (reguli personalizate). Când se declanșează o regulă, aplicația creează un eveniment cu starea *Critical* (vezi figura de mai jos).

Dacă dorești să utilizezi componenta Inspecție jurnal, asigură-te că setările de securitate ale politicii de audit sunt configurate și că sistemul înregistrează în jurnal evenimentele relevante (pentru detalii, consultă site-ul web pentru suport tehnic Microsoft.).



Notificare Inspecție jurnal

Parametru	Descriere
Reguli predefinite	Lista regulilor Inspecție jurnal. Regulile predefinite includ șabloane de activitate anormală pe computerul protejat. Activitatea anormală poate semnifica o tentativă de atac.
Reguli personalizate	Lista regulilor Inspecție jurnal adăugate de utilizator. Puteți seta propriile criterii de declanșare a regulii Inspecție jurnal. Pentru a face acest lucru, trebuie să introduceți un ID de eveniment și să selectați o sursă a evenimentului. Puteți selecta o sursă a evenimentului dintre jurnalele standard: *Application*, *Security* sau *System*. De asemenea, puteți specifica jurnalul unei aplicații terțe.

Anti-Cryptor

Componenta Anti-Cryptor analizează activitatea din directoarele partajate. Dacă această activitate corespunde unei semnături de flux comportamental care este tipică pentru criptare externă, Kaspersky Endpoint Security execută acțiunea selectată.

Kaspersky Endpoint Security împiedică criptarea externă doar pentru acele fișiere amplasate pe medii cu sistem de fișiere NTFS și care nu sunt criptate de sistemul EFS.

Parametru	Descriere
Excluderi după nume sau adresă IP	**Excluderi după nume sau adresă IP**. Lista de computere de la care nu vor fi monitorizate încercările de criptare a directoarelor partajate. Pentru a aplica lista de excluderi a computerelor de la protecția directoarelor partajate împotriva criptării externe, trebuie să activați serviciul Audit Logon în politica de audit de securitate Windows. Audit Logon este dezactivat în mod implicit. Pentru mai multe detalii despre politica de audit de securitate Windows, vizitați site-ul Web Microsoft. **Excluderi după mască**. Excluderi de la domeniul de protecție. Excluderea unui director de la domeniul de protecție poate reduce numărul de alarme false dacă organizația ta folosește criptarea datelor atunci când face schimb de fișiere utilizând directoarele partajate. De exemplu, Behavior Detection poate declanșa alarme false atunci când utilizatorul lucrează cu fișiere cu extensia ENC într-un director partajat. O astfel de activitate corespunde unui model de comportament care este tipic pentru criptarea externă. Dacă ai criptat fișierele dintr-un director pentru protejarea datelor, adaugă acel director la excluderi. Folosiți măști: • Caracterul `*` (asterisc) ține locul oricărui set de caractere, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\*\*.txt` va include toate căile către fișierele cu extensia TXT din directoarele de pe unitatea C:, dar nu și din subdirectoare. • Două caractere `*` consecutive țin locul oricărui set de caractere (inclusiv un set gol) din numele de fișier sau director, inclusiv caracterele `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\**\*.txt` va include toate căile către fișierele cu extensia TXT localizată în directoarele imbricate în `Folder`, cu excepția `Folder` în sine. Masca trebuie să includă cel puțin un nivel de imbricare. Masca `C:\**\*.txt` nu este o mască validă. • `?` (semn de întrebare) ține locul oricărui caracter individual, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\???.txt` va include căi pentru toate fișierele din directorul denumit `Folder` care au extensia TXT și un nume format din trei caractere.
Acțiune la detectarea amenințării	• **Informează**. Dacă această opțiune este selectată, la detectarea unei încercări de modificare a fișierelor din directoarele partajate, Kaspersky Endpoint Security adaugă informații despre această încercare în lista amenințărilor active, adaugă o intrare în rapoartele interfeței aplicației locale și trimite informații despre activitatea rău intenționată detectată către Kaspersky Security Center. • **Blochează conexiunea pentru (min) N min**. Dacă această opțiune este selectată, atunci când Kaspersky Endpoint Security detectează o încercare de modificare a fișierelor din directoarele partajate, acesta blochează accesul la modificarea fișierelor pentru sesiunea care a inițiat activitatea rău intenționată și creează copii de rezervă ale fișierelor modificate. Dacă activată componenta Remediation Engine este și este selectată opțiunea **Blochează conexiunea pentru (min) N min**, fișierele modificate sunt restaurate din copiile de rezervă.
Domeniu de protecție	*Domeniul de protecție* este o listă de căi către directoarele partajate în care Kaspersky Endpoint Security monitorizează activitatea fișierelor. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști. În mod implicit, aplicația identifică automat directoarele partajate și monitorizează activitatea fișierelor din toate directoarele.

Control Web

Componenta Control Web gestionează accesul utilizatorilor la resursele web. Acest lucru ajută la reducerea traficului și la utilizarea necorespunzătoare a timpului de muncă. Când un utilizator încearcă să deschidă un site web care este restricționat de Control Web, Kaspersky Endpoint Security va bloca accesul sau va afișa un avertisment (vedeți figura de mai jos).

Pentru a utiliza componenta Control Web, trebuie să finalizezi configurarea inițială a aplicației:

- Pentru monitorizarea traficului HTTPS, activează scanarea conexiunilor criptate (activată în mod implicit).
- Selectează porturile pe care Kaspersky Endpoint Security trebuie să monitorizeze (implicit, aplicația monitorizează toate porturile).

- Selectează aplicațiile al căror trafic dorești să îl monitorizeze Kaspersky Endpoint Security. Majoritatea browserelor sunt deja prezente în lista de aplicații recomandate de Kaspersky. Dacă browserul tău lipsește din listă, adaugă-l manual.

- Îți recomandăm să injectezi un script de interacțiune a paginii web în traficul web (în mod implicit, injectarea de script este dezactivată). Acest script permite înregistrarea evenimentelor Control Web pentru jurnalul de evenimente al aplicației, jurnalul de evenimente al sistemului de operare și rapoarte.

Metode de gestionare a accesului la site-uri web

Componenta Control Web vă permite să configurați accesul la site-uri web folosind următoarele metode:

- **Categorie site web**. Site-urile web sunt clasificate în funcție de serviciul cloud Kaspersky Security Network, analiza euristică și baza de date a site-urilor web cunoscute (incluse în bazele de date ale aplicațiilor). De exemplu, puteți restricționa accesul utilizatorului la categoria *Rețele de socializare* sau la alte categorii.

- **Tipul de date**. Poți restricționa accesul utilizatorilor la datele de pe un site web și poți ascunde imaginile, de exemplu. Kaspersky Endpoint Security determină tipul de date pe baza formatului fișierului și nu pe baza extensiei sale.

  Kaspersky Endpoint Security nu scanează fișierele din arhive. De exemplu, dacă fișierele imagine au fost plasate într-o arhivă, Kaspersky Endpoint Security identifică tipul de date *Arhive* și nu *Grafică*.

- **Adresă individuală**. Puteți introduce o adresă web sau puteți folosi măști.

Puteți utiliza simultan mai multe metode pentru reglementarea accesului la site-uri web. De exemplu, poți restricționa accesul la tipul de date *Fișiere ale aplicațiilor Office* doar pentru categoria de site-uri web *E-mail bazat pe web*.

Regulile de acces la site-urile web

Componenta Control Web gestionează accesul utilizatorilor la site-urile web utilizând *reguli de acces*. Puteți configura următoarele setări avansate pentru o regulă de acces la site-urile web:

- Utilizatori cărora li se aplică regula.

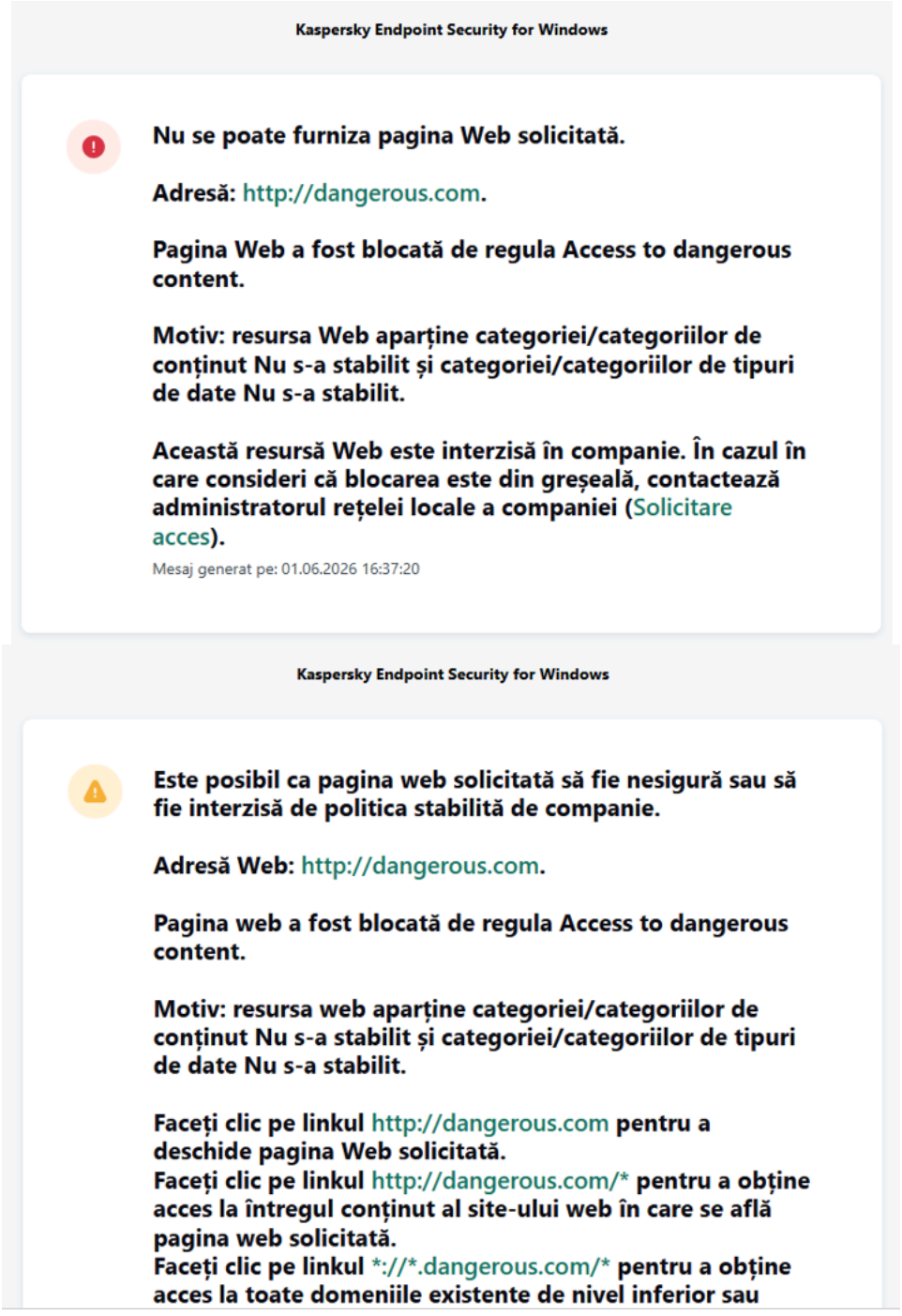
  De exemplu, puteți restricționa accesul la Internet printr-un browser pentru toți utilizatorii companiei, cu excepția departamentului IT.

- Planificare regulă.

  De exemplu, puteți restricționa accesul la Internet printr-un browser doar în timpul programului de lucru.

Priorități pentru reguli de acces

Fiecare regulă are o prioritate. Cu cât o regulă este mai sus în listă, cu atât prioritatea sa este mai mare. Dacă un site web a fost adăugat mai multor reguli, componenta Control Web reglementează accesul la site-ul web pe baza regulii cu cea mai mare prioritate. De exemplu, Kaspersky Endpoint Security poate identifica un portal corporativ ca o rețea socială. Pentru a restricționa accesul la rețelele sociale și a oferi acces la portalul web corporativ, creați două reguli: o regulă de blocare pentru categoria site-urilor web *Rețele de socializare* și una de permitere pentru portalul web corporativ. Regula de acces pentru portalul web corporativ trebuie să aibă o prioritate mai mare decât regula de acces pentru rețelele sociale.



Mesajele componentei Control Web

Parametru	Descriere
Reguli de acces la resurse Web	Lista cu regulile de acces la resurse Web. Fiecare regulă are o prioritate. Cu cât o regulă este mai sus în listă, cu atât prioritatea sa este mai mare. Dacă un site web a fost adăugat mai multor reguli, componenta Control Web reglementează accesul la site-ul web pe baza regulii cu cea mai mare prioritate.
Regulă implicită	*Regulă implicită* este o regulă de acces la resurse web care nu sunt acoperite de nici o altă regulă. Sunt disponibile următoarele opțiuni: • **Permite tot cu excepția listei de reguli**, cunoscută și sub numele de listă respinse pentru site-urile web interzise. • **Refuză tot cu excepția listei de reguli**, cunoscută și sub numele de listă permise pentru site-urile web permise.
Termină sesiunile browserului utilizatorului activ după aplicarea regulii	Dacă este bifată caseta de selectare, componenta Control Web întrerupe conexiunea la resursele web blocate imediat după aplicarea politicii. Browserul oprește imediat descărcarea datelor de pe pagina web. Atunci când reîmprospătezi pagina web sau accesați o altă pagină web interzisă, aplicația afișează un avertisment. Controlul web permite deconectarea imediată a resurselor web numai în browserele web. Pentru alte aplicații, Web Control restricționează doar conexiunile noi. În cazul în care caseta de selectare este debifată, componenta Control Web restricționează numai conexiunile noi la resursele web interzise. Componenta Control Web nu oprește conexiunile active.
Șabloane	**Avertisment**. Câmpul de intrare conține șablonul mesajului care se afișează dacă se declanșează o regulă sau o avertizare despre încercări de accesare a unei resurse Web nedorite. **Mesaj despre blocare**. Câmpul de introducere conține șablonul mesajului care apare dacă se declanșează o regulă care blochează accesul la o resursă web. **Mesaj către administrator**. Șablonul mesajului care va fi trimis administratorului rețelei LAN în cazul în care utilizatorul consideră că blocarea s-a făcut din greșeală. După ce utilizatorul solicită accesul, Kaspersky Endpoint Security trimite un eveniment către Kaspersky Security Center: **Mesaj către administrator privind blocarea accesului la paginile Web**. Descrierea evenimentului conține un mesaj către administrator cu variabile înlocuite. Puteți vizualiza aceste evenimente în consola Kaspersky Security Center, utilizând selecția de evenimente predefinită **User requests**. Dacă organizația dvs. nu are instalat Kaspersky Security Center sau nu există nicio conexiune la serverul de administrare, aplicația va trimite un mesaj administratorului la adresa de e-mail specificată. Sunt furnizate variabile speciale pentru gestionarea șabloanelor de mesaje (de exemplu, `%USER_NAME%`). Variabilele permit utilizarea unui singur șablon de mesaj pentru computere diferite.
Înregistrați în jurnal deschiderea paginilor permise	Kaspersky Endpoint Security înregistrează în jurnal datele privind vizitele pe toate site-urile web, inclusiv pe cele permise. Kaspersky Endpoint Security trimite evenimente la Kaspersky Security Center, la jurnalul local al Kaspersky Endpoint Security și la Jurnalul de evenimente Windows. Pentru a monitoriza activitatea pe Internet a utilizatorului, trebuie să configurați setările pentru salvarea evenimentelor. Browsere care acceptă funcția de monitorizare: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Yandex Browser, Mozilla Firefox. Monitorizarea activității utilizatorului nu funcționează în alte browsere. Monitorizarea activității pe Internet a utilizatorului poate necesita mai multe resurse ale computerului atunci când se decriptează traficul HTTPS.

Control dispozitive

Componenta Control dispozitive gestionează accesul utilizatorilor la dispozitivele instalate pe sau conectate la un computer (de exemplu, hard diskuri, camere video sau module Wi-Fi). Acest lucru îți permite să protejezi computerul împotriva infectării atunci când sunt conectate astfel de dispozitive și să împiedici pierderea sau scurgerea datelor.

Dacă Control dispozitive este activată, aplicația transmite informații despre dispozitivele conectate la Kaspersky Security Center. Puteți vizualiza lista dispozitivelor conectate în Kaspersky Security Center în directorul **Advanced** → **Repositories** → **Hardware**.

Nivelurile de acces ale dispozitivului

Componenta Control dispozitive controlează accesul la următoarele niveluri:

- **Device type**. De exemplu, imprimante, unități amovibile și unități CD/DVD.

  Poți configura accesul la dispozitive după cum urmează:

  - Permite – .
  - Blochează – .
  - Conform regulilor (numai imprimante și dispozitive portabile) – .
  - În funcție de magistrala de conectare (cu excepția Wi-Fi) – .
  - Blochează cu excepții (doar Wi-Fi) – .

- **Magistrală de conectare**. O *magistrală de conectare* este o interfață utilizată pentru conectarea dispozitivelor la computer (de exemplu, USB sau FireWire). Dacă modul **În funcție de magistrala de conectare** este selectat pentru tipul de dispozitiv, aplicația permite sau interzice accesul la dispozitiv în funcție de interfața de conectare (ex. USB).

  Poți configura accesul la dispozitive după cum urmează:

  - Permite – .
  - Blochează – .

- **Dispozitive de încredere**. *Dispozitivele de încredere* sunt dispozitivele la care utilizatorii specificați în setările pentru dispozitive de încredere au acces complet în orice moment.

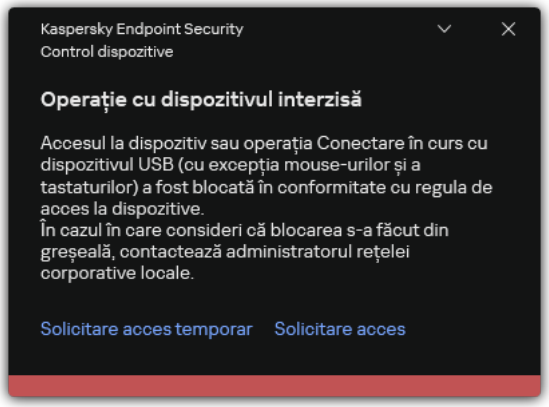
  Poți adăuga dispozitive de încredere pe baza următoarelor date:

  - **Dispozitive după ID**. Fiecare dispozitiv are un identificator unic (ID-ul hardware sau HWID). Poți vedea ID-ul în proprietățile dispozitivului utilizând instrumentele sistemului de operare. Exemplu de ID dispozitiv: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Adăugarea dispozitivelor după ID este convenabilă dacă doriți să adăugați mai multe dispozitive specifice.
  - **Dispozitive după model**. Fiecare dispozitiv are un ID de vânzător (VID) și un ID de produs (PID). Poți vedea ID-urile în proprietățile dispozitivului utilizând instrumentele sistemului de operare. Șablon pentru introducerea VID și PID: `VID_1234&PID_5678`. Adăugarea dispozitivelor după model este convenabilă dacă utilizați dispozitive ale unui anumit model în organizația dvs. În acest fel, puteți adăuga toate dispozitivele acestui model.
  - **Dispozitive după masca de ID**. Dacă utilizați mai multe dispozitive cu ID-uri similare, puteți adăuga dispozitive la lista de încredere folosind măști. Caracterul `*` înlocuiește orice set de caractere. Kaspersky Endpoint Security nu acceptă caracterul `?` atunci când introduceți o mască. De exemplu, `WDC_C*`.
  - **Dispozitive după masca modelului**. Dacă utilizați mai multe dispozitive cu VID sau PID similare (de exemplu, dispozitive de la același producător), puteți adăuga dispozitive la lista de încredere folosind măști. Caracterul `*` înlocuiește orice set de caractere. Kaspersky Endpoint Security nu acceptă caracterul `?` atunci când introduceți o mască. De exemplu, `VID_05AC&PID_*`.

Componenta Control dispozitive reglementează accesul utilizatorilor la dispozitive utilizând *reguli de acces*. Componenta Control dispozitive îți permite, de asemenea, să salvezi evenimente de conectare/deconectare a dispozitivelor. Pentru a salva evenimente, trebuie să configurezi înregistrarea evenimentelor într-o politică.

Dacă accesul la un dispozitiv depinde de magistrala de conectare (starea), Kaspersky Endpoint Security nu salvează evenimente de conectare/deconectare a dispozitivului. Pentru a permite Kaspersky Endpoint Security să salveze evenimente de conectare/deconectare a dispozitivului, permite accesul la tipul corespunzător de dispozitiv (starea) sau adaugă dispozitivul la lista de încredere.

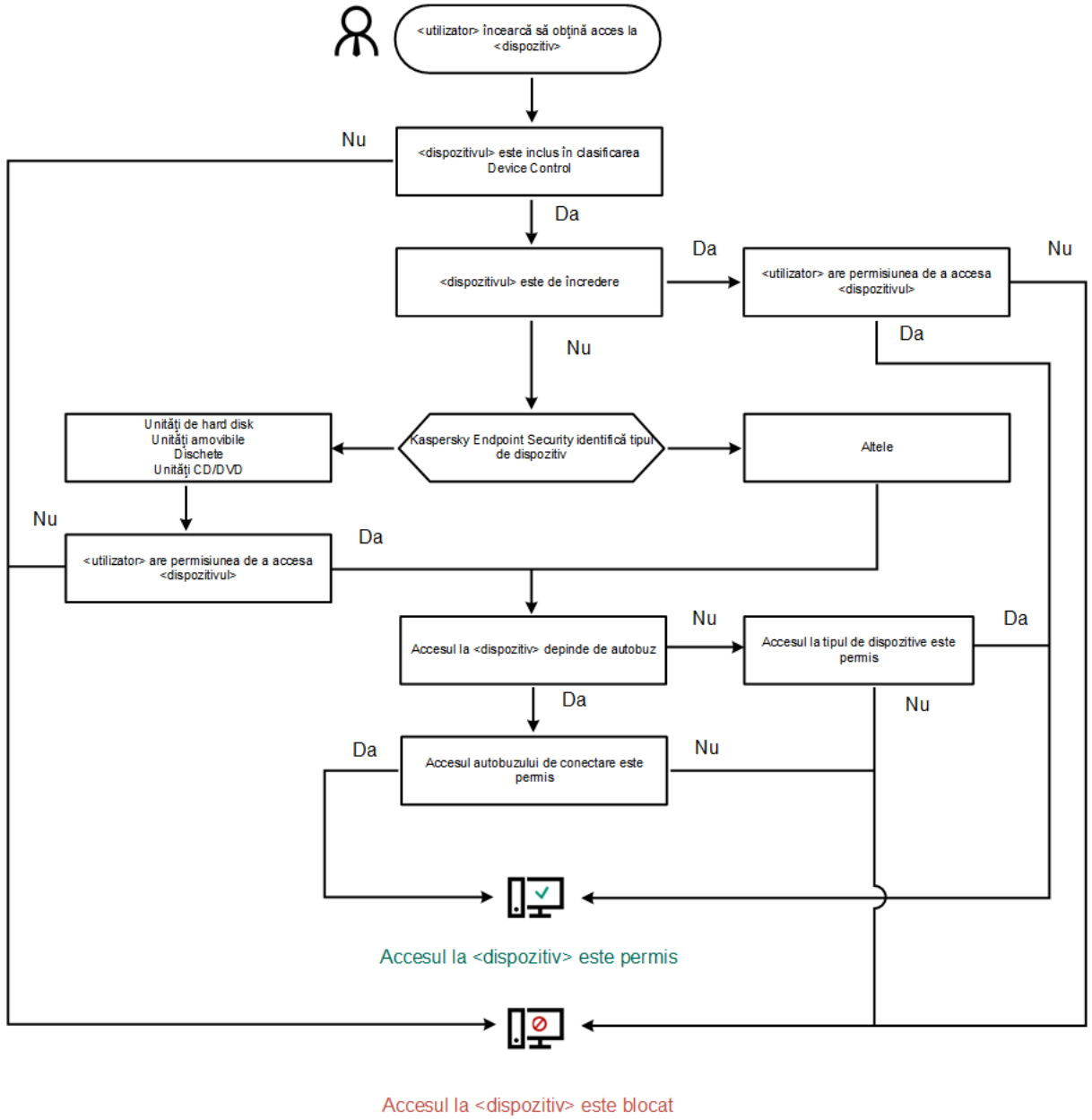
Atunci când un dispozitiv blocat de componenta Control dispozitive este conectat la computer, Kaspersky Endpoint Security va bloca accesul și va afișa o notificare (vezi figura de mai jos).



Notificări ale componentei Control dispozitive

Algoritmul de funcționare a componentei Control dispozitive

După ce utilizatorul conectează un dispozitiv la computer, Kaspersky Endpoint Security decide dacă permite accesul la dispozitivul respectiv (consultați figura de mai jos).



Algoritmul de funcționare a componentei Control dispozitive

Dacă un dispozitiv este conectat și accesul este permis, puteți edita regula de acces și bloca accesul. În acest caz, data următoare când cineva încearcă să acceseze dispozitivul (cum ar fi să vizualizeze arborele directorului sau să efectueze operațiuni de citire sau scriere), Kaspersky Endpoint Security blochează accesul. Un dispozitiv fără sistem de fișiere este blocat numai după următoarea conectare a dispozitivului.

Dacă un utilizator al computerului pe care este instalat Kaspersky Endpoint Security trebuie să solicite accesul la un dispozitiv care a fost blocat din greșeală, trimite utilizatorului instrucțiunile de solicitare acces.

Parametru	Descriere
Permite solicitările accesului temporar *(disponibil numai în consola Kaspersky Security Center)*	Dacă această casetă de selectarea este bifată, butonul **Solicitare acces** este disponibil în interfața locală a Kaspersky Endpoint Security. Utilizând acest buton, utilizatorul poate solicita acces temporar la un dispozitiv blocat.
Dispozitive și rețele Wi-Fi	Acest tabel conține toate tipurile posibile de dispozitive, în conformitate cu clasificarea componentei Control dispozitive și starea accesului la aceste tipuri de dispozitive.
Magistrale de conectare	O listă a tuturor magistralelor de conectare disponibile, în conformitate cu clasificarea componentei Control dispozitive și starea accesului la aceste magistrale. Kaspersky Endpoint Security permite sau refuză accesul la dispozitive în funcție de tipul magistralei de conectare, dacă este selectat modul **În funcție de magistrala de conectare**.
Dispozitive de încredere	Lista dispozitivelor de încredere și a utilizatorilor cărora li se acordă acces la aceste dispozitive.
Îmbină valorile în momentul moștenirii *(disponibil numai în consola Kaspersky Security Center)*	Aceasta combină lista dispozitivelor de încredere din politicile părinte și copil din cadrul Kaspersky Security Center. Pentru a îmbina listele, politica copil trebuie să fie configurată pentru a moșteni setările politicii părinte a Kaspersky Security Center. Dacă este bifată caseta de selectare, elementele de listă din politica părinte Kaspersky Security Center sunt afișate în politicile copil. În acest fel, poți crea, de exemplu, o listă consolidată de dispozitive de încredere pentru întreaga organizație. Elementele de listă moștenite dintr-o politică copil nu pot fi șterse sau editate. Elementele de pe lista de dispozitive de încredere care sunt îmbinate în timpul moștenirii pot fi șterse și editate numai în politica părinte. Puteți adăuga, edita sau șterge elemente de listă în politicile de nivel inferior. Dacă elementele din listele politicii copil și părinte se potrivesc, aceste elemente sunt afișate ca același element al politicii părinte. Dacă nu este bifată caseta de selectare, elementele listei nu sunt îmbinate la moștenirea setărilor politicilor Kaspersky Security Center. Această funcționalitate permite, de asemenea, îmbinarea listelor în profilurile de politici. Pentru a îmbina liste, în profilul cu cea mai mare prioritate, activează moștenirea setărilor dintr-un profil cu prioritate mai mică. Pentru mai multe detalii despre prioritățile profilului politicii, vezi secțiunea Ajutor pentru Kaspersky Security Center.
Anti-Bridging	Funcția Anti-Bridging inhibă crearea de punți de rețea prin împiedicarea creării simultane a mai multor conexiuni la rețea pentru un computer. Acest lucru vă permite să protejați o rețea corporativă împotriva atacurilor prin rețelele neprotejate și neautorizate. Anti-Bridging blochează stabilirea de conexiuni multiple în funcție de prioritățile dispozitivelor. Cu cât un dispozitiv este mai sus în listă, cu atât prioritatea acestuia este mai mare. Dacă o conexiune activă și o nouă conexiune sunt de același tip (de exemplu, Wi-Fi), Kaspersky Endpoint Security blochează conexiunea activă și permite stabilirea noii conexiuni. Dacă o conexiune activă și o nouă conexiune sunt de diferite tipuri (de exemplu, un adaptor de rețea și Wi-Fi), Kaspersky Endpoint Security blochează conexiunea cu prioritatea inferioară și permite conexiunea cu prioritatea superioară. Anti-punte acceptă funcționarea cu următoarele tipuri de dispozitive: adaptor de rețea, Wi-Fi și modem.
Șabloane de mesaje	**Mesaj despre blocare**. Șablon al mesajului care apare când un utilizator încearcă să acceseze un dispozitiv blocat. Acest mesaj apare, de asemenea, atunci când un utilizator încearcă să efectueze o operație asupra conținutului dispozitivului care a fost blocat pentru acest utilizator. **Mesaj către administrator**. Șablonul mesajului care va fi trimis administratorului rețelei LAN în cazul în care utilizatorul consideră că accesul la un dispozitiv a fost blocat sau o operațiune cu conținutul de pe dispozitiv a fost interzisă din greșeală. După ce utilizatorul solicită accesul, Kaspersky Endpoint Security trimite un eveniment către Kaspersky Security Center: **Mesaj către administrator privind blocarea accesului la dispozitiv**. Descrierea evenimentului conține un mesaj către administrator cu variabile înlocuite. Puteți vizualiza aceste evenimente în consola Kaspersky Security Center, utilizând selecția de evenimente predefinită **User requests**. Dacă organizația dvs. nu are instalat Kaspersky Security Center sau nu există nicio conexiune la serverul de administrare, aplicația va trimite un mesaj administratorului la adresa de e-mail specificată.

Application Control

Application Control administrează pornirea aplicațiilor pe computerele utilizatorilor. Acest lucru vă permite să implementați o politică de securitate corporativă atunci când utilizați aplicații. Application Control reduce, de asemenea, riscul de infectare a computerului prin restricționarea accesului la aplicații.

Configurarea componentei Application Control constă în următorii pași:

1. Crearea categoriilor de aplicații.

   Administratorul creează categorii de aplicații pe care administratorul dorește să le administreze. Categoriile de aplicații sunt destinate tuturor computerelor din rețeaua corporativă, indiferent de grupurile de administrare. Pentru a crea o categorie, puteți utiliza următoarele criterii: Categoria KL (de exemplu, *Browsere* sau altă categorie), cod hash fișier, producător aplicație și alte criterii.

2. Crearea regulilor Application Control.

   Administratorul creează reguli pentru componenta Application Control în politica pentru grupul de administrare. Regula include categoriile de aplicații și starea de pornire a aplicațiilor din aceste categorii: blocate sau permise. Administratorul poate crea mai multe reguli. O aplicație poate îndeplini criteriile mai multor reguli. Prioritatea pentru o regulă de blocare este mai mare decât prioritatea pentru o regulă de permitere. Kaspersky Endpoint Security verifică dacă o aplicație corespunde unei reguli de fiecare dată când este pornită. Kaspersky Endpoint Security compară secvențial aplicația cu toate regulile Application Control.

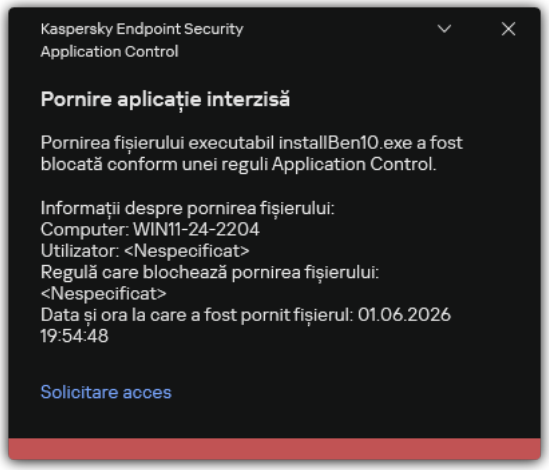
3. Selectarea modului Application Control.

   Administratorul alege modul de lucru cu aplicațiile care nu sunt incluse în niciuna dintre reguli (lista de aplicații respinse sau lista permise).

Când un utilizator încearcă să pornească o aplicație interzisă, Kaspersky Endpoint Security va bloca pornirea aplicației și va afișa o notificare (consultați figura de mai jos).

Este oferit un *mod de testare* pentru a verifica configurația componentei Application Control. În acest mod, Kaspersky Endpoint Security face următoarele:

- Permite pornirea aplicațiilor, inclusiv a celor interzise.
- Afișează o notificare despre pornirea unei aplicații interzise și adaugă informații la raportul de pe computerul utilizatorului.
- Trimite date despre pornirea aplicațiilor interzise către Kaspersky Security Center.



Notificarea Application Control

Modurile de funcționare pentru componenta Application Control

Componenta Application Control funcționează în două moduri:

- **Listă respinse**. În acest mod, Application Control permite utilizatorilor să pornească toate aplicațiile, cu excepția aplicațiilor care sunt interzise în regulile Application Control.

  Acest mod al componentei Application Control este activat în mod implicit.

- **Listă permise**. În acest mod, Application Control blochează posibilitatea utilizatorilor să pornească orice aplicații, cu excepția aplicațiilor care sunt permise și nu sunt interzise în regulile Application Control.

  Dacă regulile de permitere Application Control sunt complet configurate, componenta blochează pornirea tuturor aplicațiilor noi care nu au fost verificate de administratorul rețelei LAN, permițând însă funcționarea sistemului de operare și a aplicațiilor de încredere pe care utilizatorii se bazează în activitatea lor.

  Puteți citi recomandările privind configurarea regulilor Application Control în modul listei permise.

Componenta Application Control poate fi configurată să funcționeze în aceste moduri atât folosind interfața locală Kaspersky Endpoint Security, cât și folosind Kaspersky Security Center.

Cu toate acestea, Kaspersky Security Center oferă instrumente care nu sunt disponibile în interfața locală Kaspersky Endpoint Security, cum ar fi instrumentele care sunt necesare pentru următoarele activități:

- Crearea categoriilor de aplicații.

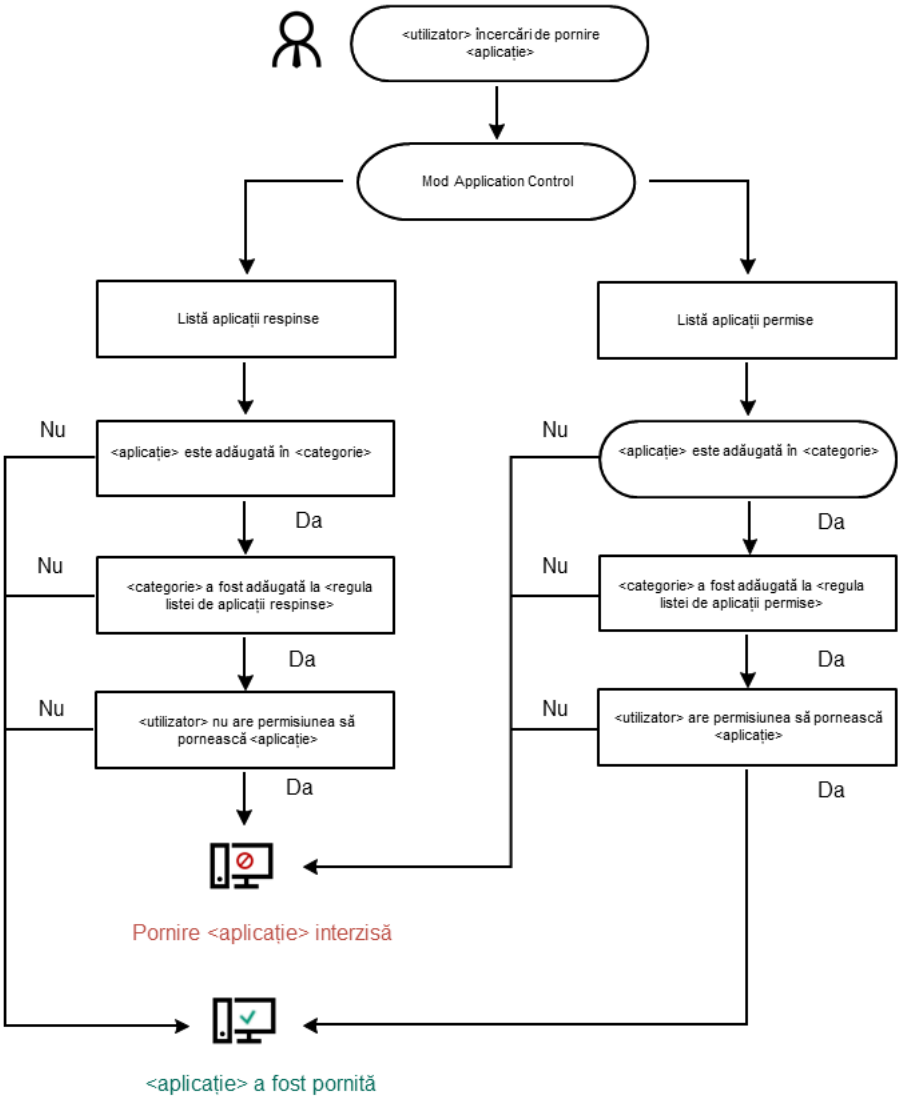
  Regulile Application Control create în Consola de administrare Kaspersky Security Center se bazează pe categorii tale particularizate de aplicații și nu pe condițiile de includere și de excludere, ca în cazul interfeței locale Kaspersky Endpoint Security.

- Primirea informațiilor despre aplicațiile instalate pe computerele din rețeaua LAN corporativă.

De aceea se recomandă utilizarea Kaspersky Security Center pentru a configura funcționarea componentei Application Control.

Algoritmul de funcționare al componentei Application Control

Kaspersky Endpoint Security folosește un algoritm pentru a lua o decizie cu privire la pornirea unei aplicații (consultați figura de mai jos).



Algoritmul de funcționare al componentei Application Control

Parametru	Descriere
Acțiune la pornirea aplicațiilor blocate de reguli	**Aplica reguli**. Kaspersky Endpoint Security gestionează pornirea aplicațiilor în funcție de modul selectat. **Testează regulile**. Kaspersky Endpoint Security permite pornirea aplicației care este blocată în modul curent pentru Application Control, dar înregistrează informațiile despre pornirea sa în raport.
Modul Control la pornirea aplicației	Poți alege una dintre următoarele opțiuni: • **Listă respinse**. Dacă este selectată această opțiune, Application Control permite tuturor utilizatorilor să pornească orice aplicație, cu excepția cazurilor care satisfac condițiile din regulile de blocare ale Application Control. • **Listă permise**. Dacă este selectată această opțiune, Application Control blochează toți utilizatorii să pornească orice aplicație, cu excepția cazurilor care satisfac condițiile din regulile de permitere ale componentei Application Control. Când este selectat modul **Listă permise**, sunt create automat două reguli Application Control: • **Imagine de aur**. • **Programe de actualizare de încredere**. Nu poți edita setările și nu poți șterge aceste reguli create automat. Poți să activezi sau să dezactivezi aceste reguli.
Monitorizează încărcarea modulelor DLL	Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security controlează încărcarea modulelor DLL atunci când utilizatorii încearcă să pornească aplicații. Informațiile despre modulul DLL și aplicația care a încărcat acest modul DLL sunt înregistrate în raport. Atunci când activați controlul asupra încărcării modulelor și driverelor DLL, asigurați-vă că în setările componentei Application Control este activată una dintre următoarele reguli: regula implicită **Imagine de aur** sau o altă regulă care conține categoria KL „**Imagine de aur\Certificate de încredere**" și care se asigură că modulele și driverele DLL de încredere sunt încărcate înainte de pornirea Kaspersky Endpoint Security. Activarea controlului încărcării modulelor și driverelor DLL când regula **Imagine de aur** este dezactivată poate duce la instabilitatea sistemului de operare. Kaspersky Endpoint Security monitorizează numai modulele și driverele DLL care au fost încărcate după bifarea casetei de selectare. După bifarea casetei de selectare, este recomandat să reporniți computerul pentru a vă asigura că aplicația monitorizează toate modulele și driverele DLL, inclusiv cele încărcate înainte de pornirea Kaspersky Endpoint Security.
Utilizează o verificare strictă a semnăturii digitale	Poți selecta un certificat drept condiție de declanșare pentru o regulă Application Control. Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security aplică reguli aplicațiilor semnate cu certificate numai din depozitul de certificate de sistem de încredere. Aplicațiile semnate cu un astfel de certificat sunt, de asemenea, considerate de încredere de către componentele de protecție, de exemplu, activitatea *Scanare malware*. Cu toate acestea, dacă specifici un certificat dintr-un alt depozit într-o regulă Application Control, Kaspersky Endpoint Security nu aplică o astfel de regulă. Dacă această casetă de selectare este debifată, Kaspersky Endpoint Security aplică reguli aplicațiilor semnate printr-un certificat din Depozitul Windows de certificate rădăcină de încredere. Astfel de aplicații nu fac parte din zona de încredere. Componentele de protecție monitorizează activitatea unor astfel de aplicații.
Șabloanele mesajelor despre blocarea aplicației	**Mesaj despre blocare**. Șablonul mesajului care se afișează atunci când este declanșată o regulă Application Control care blochează pornirea unei aplicații. **Mesaj către administrator**. Șablon al mesajului pe care un utilizator îl poate trimite administratorului rețelei LAN corporative dacă utilizatorul consideră că o aplicație a fost blocată din greșeală. După ce utilizatorul solicită accesul, Kaspersky Endpoint Security trimite un eveniment către Kaspersky Security Center: **Mesaj către administrator privind blocarea pornirii aplicației**. Descrierea evenimentului conține un mesaj către administrator cu variabile înlocuite. Puteți vizualiza aceste evenimente în consola Kaspersky Security Center, utilizând selecția de evenimente predefinită **User requests**. Dacă organizația dvs. nu are instalat Kaspersky Security Center sau nu există nicio conexiune la serverul de administrare, aplicația va trimite un mesaj administratorului la adresa de e-mail specificată.

Control adaptiv al anomaliilor

Această componentă este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Windows pentru stații de lucru. Această componentă nu este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Windows pentru servere.

Componenta Control adaptiv al anomaliilor monitorizează și blochează acțiunile care nu sunt specifice pentru computerele din rețeaua unei companii. Componenta Control adaptiv al anomaliilor utilizează un set de reguli pentru a urmări comportamentul atipic (de exemplu, regula *Pornire Microsoft PowerShell din aplicația Office*). Regulile sunt create de specialiștii Kaspersky pe baza scenariilor tipice de activitate periculoasă. Puteți configura modul în care componenta Control adaptiv al anomaliilor controlează fiecare regulă și, de exemplu, permite executarea scripturilor PowerShell care automatizează anumite activități ale fluxului de lucru. Kaspersky Endpoint Security actualizează setul de reguli împreună cu bazele de date ale aplicațiilor. Actualizările seturilor de reguli trebuie să fie confirmate manual.

Setările componentei Control adaptiv al anomaliilor

Configurarea componentei Control adaptiv al anomaliilor constă în următorii pași:

1. Instruire componentă Control adaptiv al anomaliilor.

   După ce activați componenta Control adaptiv al anomaliilor, regulile sale funcționează în *modul instruire*. În timpul instruirii, componenta Control adaptiv al anomaliilor monitorizează regulile de declanșare și trimite evenimente de declanșare către Kaspersky Security Center. Fiecare regulă are propria sa durată a modului de instruire. Durata modului de instruire este setată de către experții de la Kaspersky. În mod normal, modul de instruire este activ timp de două săptămâni.

   Dacă o regulă nu este declanșată deloc în timpul instruirii, componenta Control adaptiv al anomaliilor va considera acțiunile asociate cu această regulă ca fiind nespecifice. Kaspersky Endpoint Security va bloca toate acțiunile asociate cu acea regulă.

   Dacă o regulă a fost declanșată în timpul instruirii, Kaspersky Endpoint Security înregistrează evenimentele în jurnal în raportul de declanșare a evenimentului și în depozitul **Rule triggers in Smart Training state**.

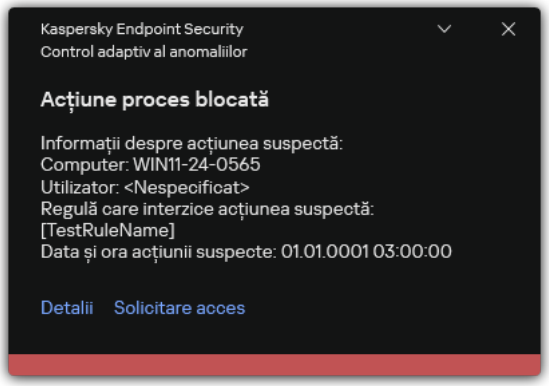
2. Analizarea raportului declanșării regulii.

   Administratorul analizează raportul de declanșare regulii sau conținutul depozitului **Rule triggers in Smart Training state**. Apoi, administratorul poate selecta comportamentul componentei Control adaptiv al anomaliilor atunci când regula este declanșată: să o blocheze sau să o accepte. De asemenea, administratorul poate continua să monitorizeze modul în care funcționează regula și să extindă durata modului de instruire. Dacă administratorul nu întreprinde nicio măsură, aplicația va continua, de asemenea, să funcționeze în modul de instruire. Termenul modului de instruire este repornit.

Componenta Control adaptiv al anomaliilor este configurată în timp real prin următoarele canale:

- Componenta Control adaptiv al anomaliilor începe automat să blocheze acțiunile asociate cu regulile care nu au fost declanșate niciodată în modul de instruire.
- Kaspersky Endpoint Security adaugă noi reguli sau le elimină pe cele învechite.
- Administratorul configurați funcționarea componentei Control adaptiv al anomaliilor după ce a examinat raportul declanșării regulii și conținutul depozitului **Rule triggers in Smart Training state**. Îți recomandăm să verifici raportul privind declanșarea regulilor și conținutul spațiului de stocare **Rule triggers in Smart Training state**.

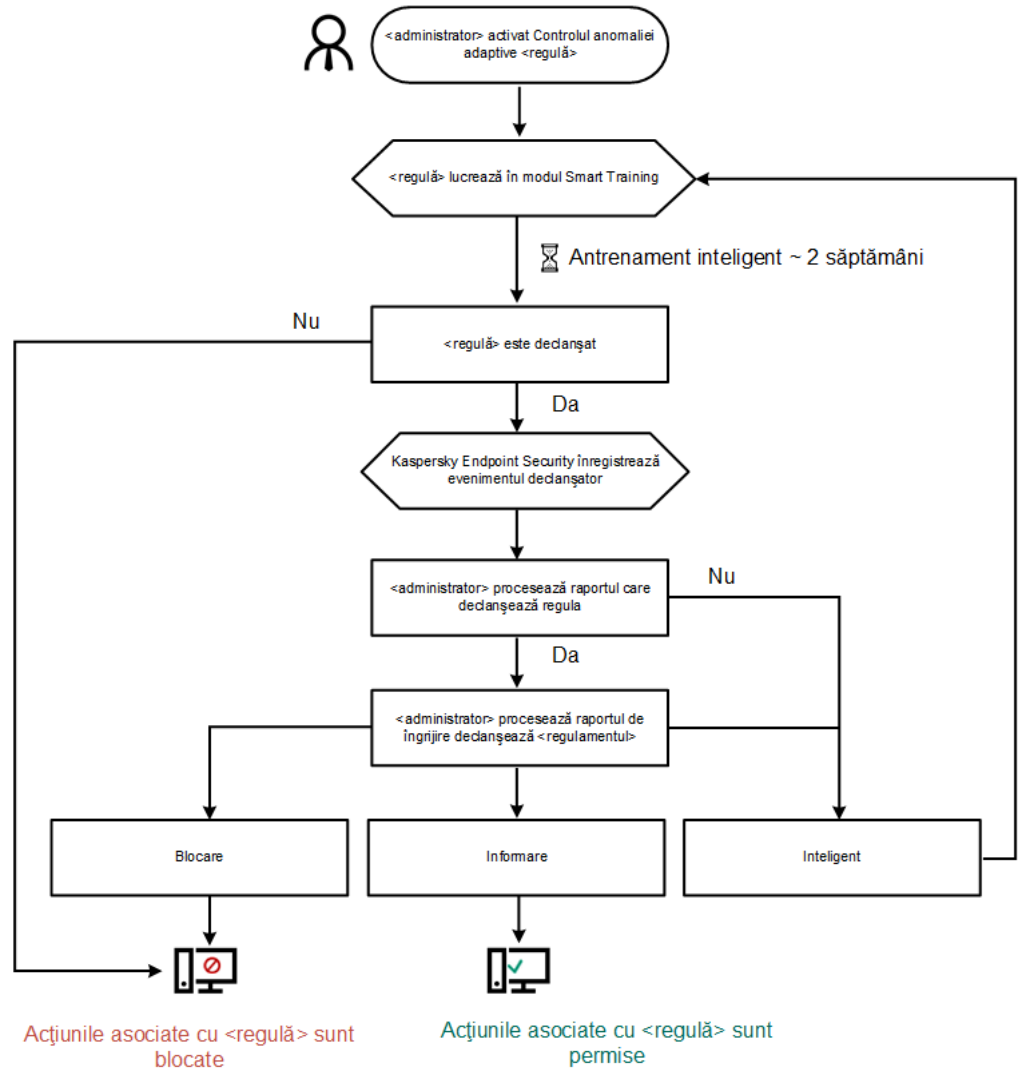
Când o aplicație periculoasă încearcă să efectueze o acțiune, Kaspersky Endpoint Security va bloca acțiunea și va afișa o notificare (consultați figura de mai jos).



Notificările componentei Control adaptiv al anomaliilor

Algoritmul de funcționare al componentei Control adaptiv al anomaliilor

Kaspersky Endpoint Security decide dacă va permite sau va bloca o acțiune asociată cu o regulă pe baza următorului algoritm (consultați figura de mai jos).



Algoritmul de funcționare al componentei Control adaptiv al anomaliilor

Setările componentei Control adaptiv al anomaliilor

Parametru	Descriere
Raport cu privire la starea regulilor funcției Control adaptiv al anomaliilor *(disponibil numai în consola Kaspersky Security Center)*	Acest raport conține informații despre starea regulilor de detectare ale componentei Control adaptiv al anomaliilor (de exemplu, *Dezactivat* sau *Blochează*). Raportul se generează pentru toate grupurile de administrare.
Raport privind regulile declanșate ale funcției Control adaptiv al anomaliilor *(disponibil numai în consola Kaspersky Security Center)*	Acest raport conține informații despre acțiunile nespecifice detectate utilizând componenta Control adaptiv al anomaliilor. Raportul se generează pentru toate grupurile de administrare.

Parametru	Descriere
Reguli	Tabel cu regulile componentei Control adaptiv al anomaliilor. Regulile sunt create de specialiștii Kaspersky pe baza scenariilor tipice de activitate periculoasă.
Șabloane	**Mesaj despre blocare**. Șablonul mesajului afișat unui utilizator atunci când este declanșată regula de Control adaptiv al anomaliilor care blochează o acțiune nespecifică. **Mesaj către administrator**. Șablonul mesajului potrivit căruia un utilizator poate fi trimis către administratorului rețelei corporative locale, dacă utilizatorul consideră că blocarea este o greșeală. După ce utilizatorul solicită accesul, Kaspersky Endpoint Security trimite un eveniment către Kaspersky Security Center: **Mesaj către administrator privind blocarea activității aplicației**. Descrierea evenimentului conține un mesaj către administrator cu variabile înlocuite. Puteți vizualiza aceste evenimente în consola Kaspersky Security Center, utilizând selecția de evenimente predefinită **User requests**. Dacă organizația dvs. nu are instalat Kaspersky Security Center sau nu există nicio conexiune la serverul de administrare, aplicația va trimite un mesaj administratorului la adresa de e-mail specificată.

Monitorizare integritate sistem

Această componentă este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Windows pentru servere. Această componentă este indisponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Windows pentru stații de lucru.

Începând cu versiunea 12.6 Kaspersky Endpoint Security or Windows include componenta Monitorizare integritate sistem în loc de componenta File Integrity Monitor. Componenta Monitorizare integritate sistem include toate funcționalitățile File Integrity Monitor și, în plus, permite monitorizarea modificărilor registry-ului și conectarea dispozitivelor externe.

Componenta Monitorizare integritate sistem monitorizează modificările din sistemul de operare care pot indica încălcări ale securității computerului. Când sunt detectate astfel de modificări, Kaspersky Endpoint Security generează evenimente corespunzătoare și alertează administratorul. Componenta Monitorizare integritate sistem poate funcționa în modul în timp real și poate efectua, de asemenea, verificări ale integrității sistemului la cerere.

Monitorizare în timp real a integrității sistemului

În modul în timp real, componenta Monitorizare integritate sistem urmărește modificările obiectelor pe care le-ai inclus în fișierul componentei (*domeniul de monitorizare*). Componenta Monitorizare integritate sistem permite, de asemenea, blocarea în timp real a accesului neautorizat la astfel de obiecte.

Componenta Verificare integritate sistem la cerere

Verificare integritate sistem la cerere este o activitate pe care o puteți executa manual sau conform unui program. Pentru a executa activitatea *Verificare integritate sistem*, trebuie să configurați domeniul de aplicare al componentei (*domeniul de monitorizare*) și creați o linie de bază. O *linie de bază* este o stare înregistrată a obiectelor din sistem, pe care aplicația o folosește ca referință atunci când o compară cu starea curentă.

Setări Monitorizare integritate sistem

Parametru	Descriere
Modul de funcționare pentru regulile de blocare	• **Blochează**. În acest mod, Monitorizare integritate sistem blochează acțiuni cu fișiere și chei de registry din domeniul de monitorizare și generează un eveniment corespunzător. • **Informează**. În acest mod, Monitorizare integritate sistem permite acțiuni cu fișiere și chei de registry din domeniul de monitorizare și generează un eveniment corespunzător.

Parametru	Descriere
Monitorizare în timp real a integrității sistemului	În modul în timp real, componenta Monitorizare integritate sistem urmărește modificările obiectelor pe care le-ai inclus în fișierul componentei (*domeniul de monitorizare*). Componenta Monitorizare integritate sistem permite, de asemenea, blocarea în timp real a accesului neautorizat la astfel de obiecte.
Monitorizează dispozitivele	Monitorizare integritate sistem monitorizează conectarea și deconectarea dispozitivelor externe.
Monitorizează fișierele și registry-ul	Monitorizare integritate sistem monitorizează modificările aduse fișierelor, directoarelor și registry-ului.
Verificare integritate sistem	Verificare integritate sistem la cerere este o activitate pe care o puteți executa manual sau conform unui program. Pentru a executa activitatea *Verificare integritate sistem*, trebuie să configurați domeniul de aplicare al componentei (*domeniul de monitorizare*) și creați o linie de bază. O *linie de bază* este o stare înregistrată a obiectelor din sistem, pe care aplicația o folosește ca referință atunci când o compară cu starea curentă.

Endpoint Sensor

Componenta Endpoint Sensor nu este inclusă în Kaspersky Endpoint Security 11.4.0.

Puteți gestiona Endpoint Sensor în Kaspersky Security Center Web Console și în Consola de administrare Kaspersky Security Center. Nu este posibil să gestionați Endpoint Sensor în Kaspersky Security Center Cloud Console.

Endpoint Sensor este conceput să interacționeze cu Kaspersky Anti Targeted Attack Platform. *Kaspersky Anti Targeted Attack Platform* este o soluție concepută pentru detectarea în timp util a amenințărilor sofisticate, cum ar fi atacuri direcționate, amenințări persistente avansate (APT), atacuri zero-day și altele. Kaspersky Anti Targeted Attack Platform include trei unități funcționale:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Poți achiziționa separat toate unitățile funcționale sau unitățile funcționale individuale. Pentru informații detaliate despre soluție, consultați Ajutor pentru Kaspersky Anti Targeted Attack Platform.

Gestionarea Endpoint Sensor are următoarele limitări:

- Puteți configura setările Endpoint Sensor într-o politică cu condiția ca Kaspersky Endpoint Security versiunea 11.0.0 până la 11.3.0 să fie instalată pe computer. Pentru mai multe informații despre configurarea setărilor componentei Endpoint Sensor utilizând politica, consultați articolele de ajutor pentru versiunile anterioare ale Kaspersky Endpoint Security.
- Dacă Kaspersky Endpoint Security versiunea 11.4.0 și o versiune ulterioară este instalat pe computer, nu puteți configura setările Endpoint Sensor in politică.

Componenta Endpoint Sensor este instalată pe computere client. Pe aceste computere, componenta monitorizează constant procesele, conexiunile la rețea active și fișierele modificate. Endpoint Sensor transmite informații către serverul KATA.

Funcționalitatea componentei este disponibilă pentru următoarele sisteme de operare:

- Windows 7 Service Pack 1 Home/Professional/Enterprise;
- Windows 8.1.1 Professional/Enterprise;
- Windows 10 RS3 Home/Professional/Education/Enterprise;
- Windows 10 RS4 Home/Professional/Education/Enterprise;
- Windows 10 RS5 Home/Professional/Education/Enterprise;
- Windows 10 RS6 Home/Professional/Education/Enterprise;
- Windows Server 2008 R2 Foundation/Standard/Enterprise (64 de biți);
- Windows Server 2012 Foundation/Standard/Enterprise (64 de biți);
- Windows Server 2012 R2 Foundation/Standard/Enterprise (64 de biți);
- Windows Server 2016 Essentials/Standard (64 de biți).

Pentru informații detaliate despre funcționarea KATA, consultați Ajutor pentru Kaspersky Anti Targeted Attack Platform.

Sandbox

Kaspersky Endpoint Security for Windows include un agent încorporat pentru integrarea cu soluția Kaspersky Sandbox. Componenta *Sandbox* detectează și blochează automat amenințările avansate de pe computere. Sandbox analizează comportamentul obiectelor pentru a detecta activitatea rău intenționată și activitatea caracteristică atacurilor țintite asupra infrastructurii IT a organizației. Sandbox analizează și scanează obiecte de pe servere speciale cu imagini virtuale implementate ale sistemelor de operare Microsoft Windows (servere Sandbox). Pentru informații detaliate despre soluție, consultați Ajutor pentru Kaspersky Sandbox și Ajutor pentru Kaspersky Anti Targeted Attack Platform.

Începând cu versiunea 12.7, Kaspersky Endpoint Security for Windows acceptă componenta Sandbox care face parte din soluția Kaspersky Anti Targeted Attack Platform. Spre deosebire de soluția Kaspersky Sandbox, componenta KATA Sandbox permite scanarea fișierelor nu doar automat, ci și manual, din meniul contextual al fișierului.

Componenta KATA Sandbox necesită implementarea Kaspersky Anti Targeted Attack Platform 7.0 sau o versiune ulterioară.

Componenta poate fi gestionată numai utilizând Kaspersky Security Center Web Console. Nu puteți gestiona această componentă utilizând Consola de administrare (MMC).

Setări componentă Sandbox

Parametru	Descriere
Integration mode	**Kaspersky Sandbox**. Integrarea cu soluția Kaspersky Sandbox. Aplicația trimite fișierele pentru a fi scanate în Kaspersky Sandbox numai în modul automat. **KATA Sandbox**. Integrarea cu componenta Sandbox a soluției Kaspersky Anti Targeted Attack Platform. Poți selecta modul de trimitere a fișierelor pentru scanare: • **Manually**. Utilizatorul trimite manual fișierul pentru scanare din meniul contextual (**Trimite către Sandbox**). • **Automatically**. Aplicația detectează automat obiectele și le trimite către Sandbox pentru scanare. • **Combined**.
Server connection settings	**Timeout (msec)**. Expirare conexiune pentru serverul Sandbox (pentru Kaspersky Sandbox) sau serverul Central Node (pentru KATA). După expirarea perioadei de expirare configurată, Kaspersky Endpoint Security trimite o solicitare către următorul server. Poți crește perioada de expirare a conexiunii pentru server dacă viteza conexiunii este mică sau dacă conexiunea este instabilă. Perioada de expirare a solicitării recomandată este de 0.5 secunde sau mai puțin. **Request queue**. Dimensiunea directorului cozii de solicitare. Când trimiți mai multe obiecte pentru scanare în Sandbox, Kaspersky Endpoint Security creează o coadă de solicitări. În mod implicit, dimensiunea directorului cozii de solicitare este limitată la 100 MO. După atingerea dimensiunii maxime, Sandbox încetează să mai adauge noi solicitări la coadă și trimite evenimentul corespunzător către Kaspersky Security Center. Puteți configura dimensiunea directorului cozii de solicitare în funcție de configurația serverului. **Server TLS certificate**. Pentru a configura o conexiune de încredere cu serverul Sandbox (pentru Kaspersky Sandbox) sau serverul Central Node (pentru KATA), trebuie să pregătești un certificat TLS. Apoi, trebuie să adaugi certificatul pe computer, folosind o politică. De asemenea, trebuie să adaugi certificatul la serverul Sandbox (pentru Kaspersky Sandbox) sau la serverul Central Node (pentru KATA). **Use two-way authentication** (doar pentru KATA Sandbox). Autentificare mutuală la stabilirea unei conexiuni securizate între Kaspersky Endpoint Security și serverul Central Node. Pentru a utiliza autentificarea mutuală, trebuie să activezi autentificarea mutuală în setările serverului Central Node, apoi să obții un container crypto și să setezi o parolă pentru a proteja containerul crypto. Un *cripto-container* este o arhivă PFX cu un certificat și o cheie privată. Puteți obține un cripto-container în consola Kaspersky Anti Targeted Attack Platform (consultați instrucțiunile din Ajutor Kaspersky Anti Targeted Attack Platform). După configurarea setărilor Central Node, trebuie să activați și autentificarea mutuală în setările Kaspersky Endpoint Security și să încărcați un container crypto protejat prin parolă.
Connection to Sandbox servers	**Kaspersky Sandbox**. Setări conexiune server Sandbox. Serverele utilizează imagini virtuale implementate ale sistemelor de operare Microsoft Windows pentru a executa obiectele care trebuie scanate. Puteți introduce o adresă IP (IPv4 sau IPv6) sau un nume de domeniu complet calificat. **KATA Sandbox**. Setări de conectare la serverul Central Node. Central Node alege setările optime pentru scanare și echilibrează încărcarea dintre serverele Sandbox.
Action on threat detection	**Move copy to Quarantine, delete object**. Dacă această opțiune este selectată, Kaspersky Endpoint Security șterge obiectul rău intenționat găsit pe computer. Înainte de a șterge obiectul, Kaspersky Endpoint Security creează o copie de rezervă în caz că obiectul trebuie restaurat ulterior. Kaspersky Endpoint Security mută copia de rezervă în Carantină. **Run Critical Areas Scan**. Dacă această opțiune este selectată, Kaspersky Endpoint Security execută activitatea *Critical Areas Scan*. În mod implicit, Kaspersky Endpoint Security scanează memoria kernel, procesele care se execută și sectoarele de boot ale discurilor. **Create IOC Scan task**. Dacă această opțiune este selectată, Kaspersky Endpoint Security creează automat o activitate de *IOC Scan (activitate de scanare IOC autonomă)*. Pentru această activitate, puteți configura modul de executare, domeniul de scanare și acțiunea la detectarea IOC (*Move copy to Quarantine, delete object* sau *Run Critical Areas Scan*). Pentru a modifica alte setări ale activității *IOC Scan*, accesați setările activității.
IOC Scan scope	**Critical file areas**. Dacă această opțiune este selectată, Kaspersky Endpoint Security efectuează o scanare IOC numai în zonele cu fișiere critice ale computerului: memoria kernel și sectoarele de boot. **File areas on system drive of the computer**. DACĂ este selectată această opțiune, Kaspersky Endpoint Security efectuează o scanare IOC pe unitatea de sistem a computerului.
Run IOC Scan task	**Manually**. Mod de executare în care poți porni manual activitatea *IOC Scan* la un moment care îți este convenabil. **Automatically**. Modul de executare în care Kaspersky Endpoint Security execută automat activitatea *IOC Scan* după ce este detectată o amenințare. **Run only when the computer is idle**. Modul de executare în care Kaspersky Endpoint Security execută activitatea *Scanare IOC* dacă economizorul de ecran este activ sau ecranul este blocat. Dacă utilizatorul deblochează computerul, Kaspersky Endpoint Security pune în pauză activitatea. Aceasta înseamnă că activitatea poate dura câteva zile până la finalizare.

Managed Detection and Response

Kaspersky Endpoint Security for Windows acceptă integrarea cu soluția Managed Detection and Response. Soluția *Kaspersky Managed Detection and Response (MDR)* detectează și analizează automat incidentele de securitate din infrastructura dvs. Pentru aceasta, MDR folosește date de telemetrie primite de la puncte finale și învățarea programată. MDR trimite datele incidentelor către experții Kaspersky. Experții pot procesa apoi incidentul și, de exemplu, pot adăuga o nouă intrare în bazele de date antivirus. Alternativ, experții pot emite recomandări privind procesarea incidentului și, de exemplu, pot sugera izolarea computerului de rețea. Pentru informații detaliate despre modul în care funcționează soluțiile, consultați pagina Ajutor Kaspersky Managed Detection and Response.

Setări Managed Detection and Response

Parametru	Descriere
Fișier de configurare MDR	Fișierul BLOB conține Id-ul clientului și informații despre licența pentru componenta Kaspersky Managed Detection and Response. Fișierul BLOB se află în arhiva ZIP a fișierului de configurare MDR. Puteți obține arhiva ZIP în Consola Kaspersky Managed Detection and Response. Pentru informații detaliate despre un fișier BLOB, consultați Ajutorul Kaspersky Managed Detection and Response.

Endpoint Detection and Response

Kaspersky Endpoint Security for Windows include un agent încorporat pentru soluția Kaspersky Endpoint Detection and Response Optimum (denumită în continuare „EDR Optimum"). Începând cu versiunea 11.8.0, Kaspersky Endpoint Security for Windows include un agent încorporat pentru soluția Kaspersky Endpoint Detection and Response Expert (denumită în continuare „EDR Expert"). *Kaspersky Endpoint Detection and Response* sunt o serie de soluții pentru protejarea infrastructurii IT corporative împotriva amenințărilor cibernetice avansate. Funcționalitatea soluțiilor combină detectarea automată a amenințărilor cu capacitatea de a reacționa la aceste amenințări pentru a contracara atacurile avansate, inclusiv exploatările, programele ransomware, atacurile fără fișiere noi, precum și metode care utilizează instrumente de sistem legitime. EDR Expert oferă o funcționalitate mai bună de monitorizare și răspuns decât EDR Optimum. Pentru detalii despre soluții, consultați Ajutor Kaspersky Endpoint Detection and Response Optimum și Ajutor Kaspersky Endpoint Detection and Response Expert.

Kaspersky Endpoint Detection and Response revizuiește și analizează dezvoltarea amenințărilor și oferă *personalului de securitate* sau *Administratorului* informații despre potențialul atac, care sunt necesare pentru un răspuns în timp util. Kaspersky Endpoint Detection and Response afișează detalii de detecție într-o fereastră separată. O *alertă* este un eveniment din infrastructura IT corporativă pe care aplicația l-a identificat ca neobișnuit sau suspect și care poate reprezenta o amenințare de securitate pentru infrastructura IT corporativă. *Detalii detecție* este un instrument pentru vizualizarea tuturor informațiilor colectate despre o amenințare detectată. Detaliile detecției includ, de exemplu, istoricul fișierelor care apar pe computer. Pentru detalii despre gestionarea detectării, consultați Ajutor Kaspersky Endpoint Detection and Response Optimum și Ajutor Kaspersky Endpoint Detection and Response Expert.

Poți configuracomponenta Endpoint Detection and Response Optimum în Web Console și Cloud Console. Setările componentei Endpoint Detection and Response Expert (cloud) sunt disponibile numai în Cloud Console.

Parametru	Descriere
Enable advanced system activity logging	Telemetria extinsă îmbunătățește precizia detectării IOC, dar utilizează mai multe resurse ale computerului. Recomandăm activarea telemetriei extinse pe computer pentru scanarea IOC retrospectivă. *Scanare IOC retrospectivă* este un mod al activității *IOC Scan* în care Kaspersky Endpoint Security scanează pentru a descoperi indicatorii de compromitere utilizând datele pentru o anumită perioadă de timp. Acest mod este destinat căutării indicatorilor de compromitere pe baza datelor de telemetrie ale computerului protejat, cum ar fi activitatea de rețea, procesele, fișierele și alte date de telemetrie. Dacă telemetria extinsă este dezactivată, Kaspersky Endpoint Security poate roti informațiile despre indicatorii de compromitere detectați.
Network Isolation	Izolarea automată a computerului de rețea, ca răspuns la amenințările detectate. Când izolarea rețelei este activată, aplicația separă toate conexiunile active și blochează toate conexiunile TCP/IP noi de pe computer. Aplicația lasă active doar următoarele conexiuni: • conexiunile listate în Excluderi izolare rețea, • conexiunile inițiate de serviciile Kaspersky Endpoint Security, • conexiunile inițiate de Agentul de rețea Kaspersky Security Center,
Automatically unlock isolated device in (hours)	Izolarea rețelei poate fi dezactivată automat după un anumit timp sau manual. În mod implicit, Kaspersky Endpoint Security dezactivează opțiunea Izolare rețea la 5 ore după începerea izolării.
Network isolation exclusions	Listă de reguli pentru excluderi de la izolarea rețelei. Conexiunile la rețea care corespund regulilor nu sunt blocate pe computere atunci când opțiunea Izolare rețea este activată. Pentru a configura Network isolation exclusions, puteți utiliza o listă de *profiluri de rețea standard*. În mod implicit, excluderile includ profiluri de rețea care conțin reguli care asigură funcționarea neîntreruptă a computerelor cu serverul DNS/DHCP și rolurile clientului DNS/DHCP. De asemenea, puteți modifica setările profilurilor standard de rețea sau puteți defini excluderile manual. Excluderile specificate în proprietățile politicii se aplică numai dacă opțiunea Izolare rețea este activată automat ca răspuns la o amenințare detectată. Excluderile specificate în proprietățile computerului se aplică numai dacă opțiunea Izolare rețea este activată manual în proprietățile computerului în consola Kaspersky Security Center sau în detaliile alertei.
Execution Prevention	Controlează executarea fișierelor și scripturilor executabile și deschiderea fișierelor în format Office. De exemplu, puteți preveni executarea aplicațiilor considerate nesigure pe computerul selectat. Suporturi pentru prevenirea executării un set de extensii de fișiere Office și un set de interpreți de scenariu. Pentru a utiliza componenta Prevenirea executării, trebuie să adăugați reguli de prevenire a executării. *Regula de prevenire a executării* este un set de criterii pe care aplicația le ia în considerare atunci când reacționează la executarea unui obiect, de exemplu când blochează executarea unui obiect. Aplicația identifică fișierele după căile sau sumele lor de verificare calculate folosind algoritmii de combinare MD5 și SHA256.
Action on execution or opening of forbidden object	**Block and add to event log**. În acest mod, aplicația blochează executarea obiectelor sau deschiderea documentelor care corespund criteriilor regulii de prevenire. Aplicația publică, de asemenea, un eveniment despre încercările de a executa obiecte sau de a deschide documente în jurnalul de evenimente Windows și în jurnalul de evenimente Kaspersky Security Center. **Add to event log**. În acest mod, Kaspersky Endpoint Security publică un eveniment despre încercările de a executa obiecte executabile sau de a deschide documente care corespund criteriilor regulii de prevenire în jurnalul de evenimente Windows și în Kaspersky Security Center, dar nu blochează încercarea de a executa sau deschide obiectul sau documentul. Acest mod este selectat în mod implicit.
Execution prevention rules	*Regula de prevenire a executării* este un set de criterii pe care aplicația le ia în considerare atunci când reacționează la executarea unui obiect, de exemplu când blochează executarea unui obiect. Aplicația identifică fișierele după căile sau sumele lor de verificare calculate folosind algoritmii de combinare MD5 și SHA256.

Parametru	Descriere
Cloud Sandbox	*Cloud Sandbox* este o tehnologie care vă permite să detectați amenințările avansate pe un computer. Kaspersky Endpoint Security redirecționează automat fișierele detectate către Cloud Sandbox pentru analiză. Cloud Sandbox execută aceste fișiere într-un mediu izolat pentru a identifica activitățile rău intenționate și a decide asupra reputației lor. Datele din aceste fișiere sunt apoi trimise către Kaspersky Security Network. Prin urmare, dacă Cloud Sandbox a detectat un fișier rău intenționat, Kaspersky Endpoint Security va efectua acțiunea corespunzătoare pentru a elimina această amenințare de pe toate computerele pe care este detectat acest fișier. Tehnologia Cloud Sandbox este activată permanent și este disponibilă pentru toți utilizatorii Kaspersky Security Network, indiferent de tipul de licență pe care îl folosesc. Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security va activa contorul pentru amenințările detectate folosind Cloud Sandbox în fereastra principală a aplicației din **Tehnologii de detectare a amenințărilor**. Kaspersky Endpoint Security va indica, de asemenea, tehnologia de detectare a amenințărilor Cloud Sandbox în evenimentele aplicației și în *Report on threats* din consola Kaspersky Security Center.

Endpoint Detection and Response Expert (on-premises)

Endpoint Detection and Response Expert (on-premises)

Kaspersky Endpoint Security for Windows acceptă integrarea cu soluția Kaspersky Endpoint Detection and Response Expert (on-premises). *Kaspersky Endpoint Detection and Response Expert (on-premises)* este o soluție de securitate cibernetică pentru companii care include aplicații Kaspersky ce permit unei organizații să se apere împotriva majorității tipurilor de riscuri cibernetice și să acopere cele mai importante scenarii de propagare a amenințărilor. Componentele EDR Expert (on-premises) sunt implementate pe Open Single Management Platform (OSMP). Această platformă execută scenarii multiplatformă într-o singură interfață și permite integrarea aplicațiilor Kaspersky cu aplicații terțe într-un sistem de securitate complet.

Unul dintre elementele centrale ale soluției este *SIEM*. SIEM urmărește evenimentele provenite de la toate componentele și corelează aceste evenimente între ele, folosind reguli definite de producător și de utilizator. EDR Expert (on-premises) analizează jurnalele și datele de telemetrie primite de la infrastructura corporativă pentru a detecta automat atacurile și permite investigarea incidentelor utilizând un grafic de investigare unificat, care combină toate evenimentele colectate în EDR Expert (on-premises), inclusiv evenimentele din aplicațiile Kaspersky și produsele de securitate a informațiilor de la terți.

Pentru a răspunde la incidente avansate, EDR Expert (on-premises) utilizează scenarii prestabilite și definite de utilizator. De asemenea, poți utiliza acțiuni de răspuns de la aplicații terțe și scenarii de răspuns care implică mai multe aplicații.

Endpoint Detection and Response (KATA)

Kaspersky Endpoint Security for Windows acceptă lucrul cu componenta Kaspersky Endpoint Detection and Response ca parte a soluției Kaspersky Anti Targeted Attack Platform (EDR (KATA)). *Kaspersky Anti Targeted Attack Platform* este o soluție concepută pentru detectarea în timp util a amenințărilor sofisticate, cum ar fi atacuri direcționate, amenințări persistente avansate (APT), atacuri zero-day și altele. Kaspersky Anti Targeted Attack Platform include trei unități funcționale:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Poți achiziționa separat toate unitățile funcționale sau unitățile funcționale individuale. Pentru informații detaliate despre soluție, consultați Ajutor pentru Kaspersky Anti Targeted Attack Platform.

Kaspersky Endpoint Security este instalat pe computere individuale din infrastructura IT corporativă și monitorizează continuu procesele, conexiunile la rețea deschise și fișierele care sunt modificate. Informațiile despre evenimentele de pe computer (date de telemetrie) sunt trimise către serverul Kaspersky Anti Targeted Attack Platform. În acest caz, aplicația Kaspersky Endpoint Security trimite, de asemenea, informații către serverul Kaspersky Anti Targeted Attack Platform despre amenințările descoperite de aplicație, precum și informații despre rezultatele procesării pentru aceste amenințări.

Integrarea EDR (KATA) și NDR (KATA) este configurată pe consola Kaspersky Security Center. Agentul încorporat este apoi gestionat utilizând consola Kaspersky Anti Targeted Attack Platform, inclusiv executarea activităților, gestionarea obiectelor aflate în carantină, vizualizarea rapoartelor și alte acțiuni.

Setări Endpoint Detection and Response Expert (on-premises)

Parametru	Descriere
Connection to telemetry collection servers	Un *server de colectare a telemetriei* este un server care face parte dintr-o soluție SIEM și care colectează, normalizează, corelează, analizează și stochează informații despre evenimentele care au loc pe computer. Configurează următoarele pentru a te conecta la serverele de colectare a datelor de telemetrie (KUMA): • **Timeout (sec)**. Expirarea timpului maxim de răspuns al serverului. Când timpul de expirare se termină, Kaspersky Endpoint Security încearcă să se conecteze la un alt server. • **Server certificate**. Certificat TLS pentru stabilirea unei conexiuni de încredere cu serverul. Poți obține un certificat TLS pe Open Single Management Platform (consultă instrucțiunile din Ajutor pentru Kaspersky Endpoint Detection and Response Expert (on-premises)). • **Use two-way authentication**. Autentificare mutuală la stabilirea unei conexiuni securizate între Kaspersky Endpoint Security și server. Pentru a utiliza autentificarea mutuală, trebuie să activezi autentificarea mutuală în setările serverului, apoi să obții un container crypto și să setezi o parolă pentru a proteja containerul crypto. Un *cripto-container* este o arhivă PFX cu un certificat și o cheie privată. Poți obține un container crypto pe Open Single Management Platform (consultă instrucțiunile din Ajutor pentru Kaspersky Endpoint Detection and Response Expert (on-premises)). După configurarea setărilor serverului, trebuie să activezi autentificarea mutuală și în setările Kaspersky Endpoint Security și să încarci un container crypto protejat prin parolă. Criptocontainerul trebuie să fie protejat prin parolă. Nu este posibil să adăugați un criptocontainer cu o parolă necompletată.
Address și **Port** (servere de colectare a datelor de telemetrie)	Setări pentru conectarea la serverele de colectare a telemetriei. Puteți introduce o adresă IP (IPv4 sau IPv6). Poți adăuga mai multe adrese de server de colectare a datelor de telemetrie. Kaspersky Endpoint Security încearcă să se conecteze la server la prima adresă IP. Dacă nu se poate stabili o conexiune, Kaspersky Endpoint Security încearcă să se conecteze la a doua adresă IP din listă și așa mai departe.
Send telemetry to telemetry collection servers	Această funcționalitate îți permite să dezactivezi complet trimiterea de telemetrie către serverul KATA. De exemplu, dacă utilizezi Kaspersky Anti Targeted Attack Platform împreună cu o altă soluție care utilizează, de asemenea, telemetria, poți dezactiva transmiterea telemetriei pentru KATA (EDR). Acest lucru vă permite să optimizați încărcarea serverului pentru aceste soluții. Dacă ai implementate soluțiile Managed Detection and Response și KATA (EDR), poți utiliza telemetria MDR și poți crea activități Răspuns la amenințare în KATA (EDR). • **Send telemetry with IOA only**. Aceasta permite optimizarea telemetriei și trimiterea doar a telemetriei cu IOA. *Indicatorul de atac (IOA)* este o regulă care conține o descriere a comportamentului suspect din sistem, care poate indica un atac țintit. Aplicația compară comportamentul curent din sistem cu aceste reguli și înregistrează în jurnal evenimentele care indică un atac țintit. Aplicația utilizează tehnologia *scanare în flux* care permite urmărirea în timp real a acestor evenimente. • **Maximum event transmission delay (sec)**. Aplicația se sincronizează cu serverul pentru a trimite evenimente după expirarea intervalului de sincronizare. Valoarea implicită este 30 de secunde. • **Limit the number of event packets per transmission**. Aplicația se sincronizează cu serverul atunci când memoria tampon este umplută cu evenimente. Valoarea implicită este de 1024 de evenimente. Această funcție permite dezactivarea utilizării ca zonă de tampon a evenimentelor înainte de sincronizarea cu serverul.
Enable request throttling	Această caracteristică ajută la optimizarea încărcării serverului. Dacă această funcționalitate este activată, aplicația restricționează transmiterea evenimentului. Dacă numărul de evenimente depășește limitele configurate, Kaspersky Endpoint Security oprește trimiterea evenimentelor. Configurează setările pentru telemetrie: • **Maximum number of events per hour**. Aplicația analizează fluxul de date de telemetrie și restricționează trimiterea evenimentelor dacă fluxul de evenimente depășește limita de evenimente pe oră configurată. Kaspersky Endpoint Security reia trimiterea evenimentelor după o oră. Valoarea implicită este de 3000 de evenimente pe oră. Dacă aplicația este instalată pe un server, fluxul de date de telemetrie este mai mare. Pentru servere, se recomandă creșterea valorii la 60.000 de evenimente pe oră. • **Percentage of event limit excess**. Aplicația sortează evenimentele după tip (de exemplu, evenimente „modificări în registry") și restricționează transmiterea evenimentelor dacă raportul dintre evenimente de același tip și numărul total de evenimente depășește limita configurată în procente. Kaspersky Endpoint Security reia trimiterea evenimentelor atunci când raportul dintre alte evenimente și numărul total de evenimente devine din nou suficient de mare. Valoarea implicită este 15%.
Send sync request to server every (min)	Frecvența solicitărilor de sincronizare trimise către serverul. În timpul sincronizării, Kaspersky Endpoint Security trimite informații despre setările și activitățile modificate ale aplicației.

Parametru	Descriere
Connection to response servers	Un *server de răspuns* este un server pentru primirea și scanarea datelor, studierea comportamentului obiectelor și publicarea rezultatelor acestor studii. Configurează următoarele detalii pentru conexiunea la serverul de răspuns: • **Timeout (sec)**. Expirarea timpului maxim de răspuns al serverului. Când timpul de expirare se termină, Kaspersky Endpoint Security încearcă să se conecteze la un alt server. • **Server certificate**. Certificat TLS pentru stabilirea unei conexiuni de încredere cu serverul. Poți obține un certificat TLS pe Open Single Management Platform (consultă instrucțiunile din Ajutor pentru Kaspersky Endpoint Detection and Response Expert (on-premises)). • **Use two-way authentication**. Autentificare mutuală la stabilirea unei conexiuni securizate între Kaspersky Endpoint Security și server. Pentru a utiliza autentificarea mutuală, trebuie să activezi autentificarea mutuală în setările serverului, apoi să obții un container crypto și să setezi o parolă pentru a proteja containerul crypto. Un *cripto-container* este o arhivă PFX cu un certificat și o cheie privată. Poți obține un container crypto pe Open Single Management Platform (consultă instrucțiunile din Ajutor pentru Kaspersky Endpoint Detection and Response Expert (on-premises)). După configurarea setărilor serverului, trebuie să activezi autentificarea mutuală și în setările Kaspersky Endpoint Security și să încarci un container crypto protejat prin parolă.
Address și **Port** (servere de răspuns)	Setări pentru conectarea la serverele de răspuns. Puteți introduce o adresă IP (IPv4 sau IPv6). Poți adăuga mai multe adrese de server de colectare a datelor de telemetrie. Kaspersky Endpoint Security încearcă să se conecteze la server la prima adresă IP. Dacă nu se poate stabili o conexiune, Kaspersky Endpoint Security încearcă să se conecteze la a doua adresă IP din listă și așa mai departe.

Setări Endpoint Detection and Response (KATA)

Parametru	Descriere
Send sync request to server every (min)	Frecvența solicitărilor de sincronizare trimise către serverul. În timpul sincronizării, Kaspersky Endpoint Security trimite informații despre setările și activitățile modificate ale aplicației.
Connection to KATA servers	Configurează următoarele detalii pentru conexiunea la serverul Central Node: • **Timeout (sec)**. Expirarea timpului maxim de răspuns al serverului Central Node. Când timpul de expirare se termină, Kaspersky Endpoint Security încearcă să se conecteze la un alt server Central Node. • **Server certificate**. Certificat TLS pentru stabilirea unei conexiuni de încredere cu serverul Central Node. Puteți obține un certificat TLS în consola Kaspersky Anti Targeted Attack Platform (consultați instrucțiunile din Ajutor Kaspersky Anti Targeted Attack Platform). • **Use two-way authentication**. Autentificare mutuală la stabilirea unei conexiuni securizate între Kaspersky Endpoint Security și serverul Central Node. Pentru a utiliza autentificarea mutuală, trebuie să activezi autentificarea mutuală în setările serverului Central Node, apoi să obții un container crypto și să setezi o parolă pentru a proteja containerul crypto. Un *cripto-container* este o arhivă PFX cu un certificat și o cheie privată. Puteți obține un cripto-container în consola Kaspersky Anti Targeted Attack Platform (consultați instrucțiunile din Ajutor Kaspersky Anti Targeted Attack Platform). După configurarea setărilor Central Node, trebuie să activați și autentificarea mutuală în setările Kaspersky Endpoint Security și să încărcați un container crypto protejat prin parolă. Criptocontainerul trebuie să fie protejat prin parolă. Nu este posibil să adăugați un criptocontainer cu o parolă necompletată.
Address și **Port** (servere KATA)	Setări pentru conectarea la serverele Kaspersky Anti Targeted Attack Platform. Introduceți adresa IP (IPv4 sau IPv6) și portul serverului Central Node pentru a vă conecta. Poți adăuga mai multe adrese de server Central Node. Kaspersky Endpoint Security încearcă să se conecteze la server la prima adresă IP. Dacă nu se poate stabili o conexiune, Kaspersky Endpoint Security încearcă să se conecteze la a doua adresă IP din listă și așa mai departe.
Send telemetry to KATA	Această funcționalitate îți permite să dezactivezi complet trimiterea de telemetrie către serverul KATA. De exemplu, dacă utilizezi Kaspersky Anti Targeted Attack Platform împreună cu o altă soluție care utilizează, de asemenea, telemetria, poți dezactiva transmiterea telemetriei pentru KATA (EDR). Acest lucru vă permite să optimizați încărcarea serverului pentru aceste soluții. Dacă ai implementate soluțiile Managed Detection and Response și KATA (EDR), poți utiliza telemetria MDR și poți crea activități Răspuns la amenințare în KATA (EDR). Configurează setările pentru telemetrie: • **Maximum event transmission delay (sec)**. Aplicația se sincronizează cu serverul pentru a trimite evenimente după expirarea intervalului de sincronizare. Valoarea implicită este 30 de secunde. • **Maximum number of event packages**. Aplicația se sincronizează cu serverul atunci când memoria tampon este umplută cu evenimente. Valoarea implicită este de 1024 de evenimente.

Parametru	Descriere
Enable request throttling	Această caracteristică ajută la optimizarea încărcării serverului. Dacă această funcționalitate este activată, aplicația restricționează transmiterea evenimentului. Dacă numărul de evenimente depășește limitele configurate, Kaspersky Endpoint Security oprește trimiterea evenimentelor. Configurează setările pentru telemetrie: • **Maximum number of events per hour**. Aplicația analizează fluxul de date de telemetrie și restricționează trimiterea evenimentelor dacă fluxul de evenimente depășește limita de evenimente pe oră configurată. Kaspersky Endpoint Security reia trimiterea evenimentelor după o oră. Valoarea implicită este de 3000 de evenimente pe oră. Dacă aplicația este instalată pe un server, fluxul de date de telemetrie este mai mare. Pentru servere, se recomandă creșterea valorii la 60.000 de evenimente pe oră. • **Percentage of event limit excess**. Aplicația sortează evenimentele după tip (de exemplu, evenimente „modificări în registry") și restricționează transmiterea evenimentelor dacă raportul dintre evenimente de același tip și numărul total de evenimente depășește limita configurată în procente. Kaspersky Endpoint Security reia trimiterea evenimentelor atunci când raportul dintre alte evenimente și numărul total de evenimente devine din nou suficient de mare. Valoarea implicită este 15%.

Network Detection and Response (KATA)

Kaspersky Endpoint Security for Windows acceptă lucrul cu componenta Kaspersky Network Detection and Response ca parte a soluției Kaspersky Anti Targeted Attack Platform (EDR (KATA)). *Kaspersky Anti Targeted Attack Platform* este o soluție concepută pentru detectarea în timp util a amenințărilor sofisticate, cum ar fi atacuri direcționate, amenințări persistente avansate (APT), atacuri zero-day și altele. Kaspersky Anti Targeted Attack Platform include trei unități funcționale:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Poți achiziționa separat toate unitățile funcționale sau unitățile funcționale individuale. Pentru informații detaliate despre soluție, consultați Ajutor pentru Kaspersky Anti Targeted Attack Platform.

Kaspersky Endpoint Security este instalat pe computere individuale din infrastructura IT corporativă și monitorizează continuu procesele, conexiunile la rețea deschise și fișierele care sunt modificate. Informațiile despre evenimentele de pe computer (date de telemetrie) sunt trimise către serverul Kaspersky Anti Targeted Attack Platform. În acest caz, aplicația Kaspersky Endpoint Security trimite, de asemenea, informații către serverul Kaspersky Anti Targeted Attack Platform despre amenințările descoperite de aplicație, precum și informații despre rezultatele procesării pentru aceste amenințări.

Integrarea EDR (KATA) și NDR (KATA) este configurată pe consola Kaspersky Security Center. Agentul încorporat este apoi gestionat utilizând consola Kaspersky Anti Targeted Attack Platform, inclusiv executarea activităților, gestionarea obiectelor aflate în carantină, vizualizarea rapoartelor și alte acțiuni.

Parametru	Descriere
Setări conectare server	**Expirare (sec)**. Expirarea timpului maxim de răspuns al serverului Central Node. Când timpul de expirare se termină, Kaspersky Endpoint Security încearcă să se conecteze la un alt server Central Node. **Certificat TLS server**. Certificat TLS pentru stabilirea unei conexiuni de încredere cu serverul Central Node. Puteți obține un certificat TLS în consola Kaspersky Anti Targeted Attack Platform (consultați instrucțiunile din Ajutor Kaspersky Anti Targeted Attack Platform). **Utilizează autentificarea mutuală**. Autentificare mutuală la stabilirea unei conexiuni securizate între Kaspersky Endpoint Security și serverul Central Node. Pentru a utiliza autentificarea mutuală, trebuie să activezi autentificarea mutuală în setările serverului Central Node, apoi să obții un container crypto și să setezi o parolă pentru a proteja containerul crypto. Un *cripto-container* este o arhivă PFX cu un certificat și o cheie privată. Puteți obține un cripto-container în consola Kaspersky Anti Targeted Attack Platform (consultați instrucțiunile din Ajutor Kaspersky Anti Targeted Attack Platform). După configurarea setărilor Central Node, trebuie să activați și autentificarea mutuală în setările Kaspersky Endpoint Security și să încărcați un container crypto protejat prin parolă. Criptocontainerul trebuie să fie protejat prin parolă. Nu este posibil să adăugați un criptocontainer cu o parolă necompletată.
Adresă și **Port**	Setări pentru conectarea la serverele Kaspersky Anti Targeted Attack Platform. Introduceți adresa IP (IPv4 sau IPv6) și portul serverului Central Node pentru a vă conecta. Poți adăuga mai multe adrese de server Central Node. Kaspersky Endpoint Security încearcă să se conecteze la server la prima adresă IP. Dacă nu se poate stabili o conexiune, Kaspersky Endpoint Security încearcă să se conecteze la a doua adresă IP din listă și așa mai departe.
Trimite solicitarea de sincronizare la serverul NDR la fiecare (min)	Frecvența solicitărilor de sincronizare trimise către serverul. În timpul sincronizării, Kaspersky Endpoint Security trimite informații despre setările și activitățile modificate ale aplicației.
Întârziere maximă între transmiterea evenimentelor (sec)	Aplicația se sincronizează cu serverul pentru a trimite evenimente după expirarea intervalului de sincronizare. Valoarea implicită este 30 de secunde.
Activează limitarea solicitărilor	Această caracteristică ajută la optimizarea încărcării serverului. Dacă această funcționalitate este activată, aplicația restricționează transmiterea evenimentului. Dacă numărul de evenimente depășește limitele configurate, Kaspersky Endpoint Security oprește trimiterea evenimentelor.
Numărul maxim de evenimente pe oră	Aplicația analizează fluxul de date de telemetrie și restricționează trimiterea evenimentelor dacă fluxul de evenimente depășește limita de evenimente pe oră configurată. Kaspersky Endpoint Security reia trimiterea evenimentelor după o oră. Valoarea implicită este de 3000 de evenimente pe oră. Dacă aplicația este instalată pe un server, fluxul de date de telemetrie este mai mare. Pentru servere, se recomandă creșterea valorii la 60.000 de evenimente pe oră.
Procentajul depășirii limitei de evenimente	Aplicația sortează evenimentele după tip (de exemplu, evenimente „modificări în registry") și restricționează transmiterea evenimentelor dacă raportul dintre evenimente de același tip și numărul total de evenimente depășește limita configurată în procente. Kaspersky Endpoint Security reia trimiterea evenimentelor atunci când raportul dintre alte evenimente și numărul total de evenimente devine din nou suficient de mare. Valoarea implicită este 15%.

Integrare cu KUMA

Kaspersky Endpoint Security for Windows acceptă soluția Kaspersky Unified Monitoring and Analysis Platform. *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* este o soluție de management al informațiilor și evenimentelor de securitate (SIEM) pentru infrastructura IT a organizațiilor. KUMA permite detectarea, analizarea și atenuarea amenințărilor de securitate înainte ca acestea să poată provoca daune.

Parametru	Descriere
Maximum delay when sending events (sec)	Aplicația se sincronizează cu serverul pentru a trimite evenimente după expirarea intervalului de sincronizare. Valoarea implicită este 30 de secunde.
Connection to KUMA servers	**Timeout (sec)**. Expirarea timpului maxim de răspuns al serverului KUMA. Când timpul de expirare se termină, Kaspersky Endpoint Security încearcă să se conecteze la un alt server KUMA. **Server certificate**. Certificatul TLS pentru stabilirea unei conexiuni de încredere cu serverul KUMA. Poți obține un certificat TLS în consola Kaspersky Unified Monitoring and Analysis Platform (consultă instrucțiunile din Kaspersky Unified Monitoring and Analysis Platform). Pentru a stabili o conexiune de încredere, în consola KUMA, în setările conectorului tcp, trebuie să selectați modul TLS **With verification** (consultați setările pentru conectorul de tip tcp în Ajutor Kaspersky Unified Monitoring and Analysis Platform). **Use two-way authentication**. Autentificare mutuală la stabilirea unei conexiuni securizate între Kaspersky Endpoint Security și KUMA. Pentru a utiliza autentificarea mutuală, în consola KUMA, în setările conectorului tcp, trebuie să selectați modul TLS **Custom PFX** (consultați setările pentru conectorul de tip tcp în Ajutor Kaspersky Unified Monitoring and Analysis Platform). Apoi trebuie să obțineți un criptocontainer și să setați o parolă pentru a proteja criptocontainerul. Un *cripto-container* este o arhivă PFX cu un certificat și o cheie privată. După configurarea setărilor KUMA, trebuie să activați și autentificarea mutuală în setările Kaspersky Endpoint Security și să încărcați un container crypto protejat prin parolă. Criptocontainerul trebuie să fie protejat prin parolă. Nu este posibil să adăugați un criptocontainer cu o parolă necompletată.
Servere KUMA	Setări conexiunii la serverele Kaspersky Unified Monitoring and Analysis Platform. Puteți introduce o adresă IP (IPv4 sau IPv6). Poți adăuga mai multe adrese de server KUMA. Kaspersky Endpoint Security încearcă să se conecteze la server la prima adresă IP. Dacă nu se poate stabili o conexiune, Kaspersky Endpoint Security încearcă să se conecteze la a doua adresă IP din listă și așa mai departe.

Full Disk Encryption

Puteți selecta o tehnologie de criptare: Kaspersky Disk Encryption sau BitLocker Drive Encryption (denumită în continuare pur și simplu „BitLocker”).

Kaspersky Disk Encryption

Kaspersky Disk Encryption nu este acceptat pe computerele bazate pe arhitectura ARM.

După ce unitățile de hard disk de sistem au fost criptate, la următoarea pornire a computerului utilizatorul trebuie să finalizeze autentificarea folosind Agentul de Autentificare pentru ca unitățile de hard disk să poată fi accesate și sistemul de operare să fie încărcat. Acest lucru necesită introducerea parolei pentru simbolul sau cardul inteligent conectat la computer sau a numelui de utilizator și a parolei pentru contul de Agent de Autentificare creat de administratorul rețelei locale folosind activitatea *Gestionare conturi Agent de Autentificare*. Aceste conturi se bazează pe conturile Microsoft Windows sub care utilizatorii se conectează la sistemul de operare. Poți utiliza, de asemenea, tehnologia Single Sign-On (SSO), care îți permite să te conectezi automat la sistemul de operare folosind numele de utilizator și parola contului Agent de Autentificare.

Autentificarea utilizatorului în Agentul de Autentificare poate fi efectuată în două moduri:

- Introdu numele de utilizator și parola pentru contul de Agent de Autentificare creat de administratorul rețelei LAN folosind instrumentele Kaspersky Security Center.
- Introdu parola pentru un simbol sau un simbol sau un card inteligent conectat la computer.

  Folosirea unui simbol sau card inteligent este disponibilă dacă unitățile de hard disk ale computerului au fost criptate utilizându-se algoritmul de criptare AES256. În cazul în care unitățile de hard disk ale computerului a fost criptate utilizându-se algoritmul de criptare AES56, adăugarea fișierului de certificat electronic la comandă va fi refuzată.

BitLocker Drive Encryption

BitLocker este o tehnologie de criptare încorporată în sistemele de operare Windows. Kaspersky Endpoint Security îți permite să controlezi și să gestionezi Bitlocker folosind infrastructura Kaspersky Next. BitLocker criptează volumele logice. BitLocker nu poate fi utilizat pentru criptarea unităților amovibile. Pentru detalii suplimentare despre BitLocker, consultați documentația Microsoft.

La criptarea discului, BitLocker plasează programul de încărcare a comenzilor de inițiere și alte fișiere auxiliare în system partition. Această partiție nu este criptată. Sistemul de operare creează automat partiția de sistem în timpul instalării programului Windows. Dacă discul este partiționat complet înainte de instalarea programului Windows, sistemul de operare nu poate crea o partiție de sistem. În acest caz, când pornești criptarea discului cu BitLocker, sistemul de operare îți solicită să partiționeze din nou discul și să creezi o partiție de sistem. După crearea unei partiții de sistem, sistemul de operare pornește criptarea BitLocker.

BitLocker asigură stocarea securizată a cheilor de acces folosind un modul de platformă de încredere. Un *Trusted Platform Module* (TPM) este un microcip dezvoltat pentru a furniza funcții de bază legate de securitate (de exemplu, pentru stocarea cheilor de criptare). Un Trusted Platform Module este de obicei instalat pe placa de bază a computerului și interacționează cu toate celelalte componente ale sistemului prin intermediul magistralei hardware. Utilizarea TPM este cea mai sigură modalitate de a stoca cheile de acces BitLocker, deoarece TPM oferă verificarea integrității sistemului înainte de pornire. Puteți cripta în continuare unitățile de pe computer fără un TPM. În acest caz, cheia de acces va fi criptată cu o parolă. BitLocker utilizează următoarele metode de autentificare:

- TPM.
- TPM și PIN.
- Parolă.

După criptarea hard disk-ului sistemului, utilizatorul trebuie să parcurgă procesul de autentificarea BitLocker pentru a porni sistemul de operare. După autentificare, BitLocker va permite utilizatorilor să se conecteze. BitLocker nu acceptă tehnologia de conectare unică (SSO).

După criptarea unei unități, BitLocker creează o cheie de recuperare. Kaspersky Endpoint Security trimite cheia de recuperare către Kaspersky Security Center astfel încât să poți restabili accesul la disc, de exemplu, dacă un utilizator și-a uitat parola.

Dacă un utilizator criptează un disc folosind BitLocker, Kaspersky Endpoint Security va trimite cheia de recuperare și informații despre criptarea discului către Kaspersky Security Center.

Dacă utilizați politicile de grup ale Windows, dezactivați gestionareaa BitLocker în setările politicii. Setările politicii Windows pot intra în conflict cu setările politicii Kaspersky Endpoint Security. Când criptați o unitate, pot apărea erori.

Setările componentei Kaspersky Disk Encryption

Parametru	Descriere
Mod criptare	**Se criptează toate unitățile de hard disk**. Dacă această opțiune este selectată, aplicația criptează toate unitățile de hard disk atunci când este aplicată politica. Dacă pe computer sunt instalate mai multe sisteme de operare, după criptare vei putea încărca doar sistemul de operare pe care este instalată aplicația. **Se decriptează toate unitățile de hard disk**. Dacă această opțiune este selectată, aplicația decriptează toate unitățile de hard disk criptate anterior atunci când este aplicată politica. **Lasă nemodificat**. Dacă este selectat acest element, aplicația lasă unitățile în starea existentă atunci când este aplicată politica. Dacă unitatea era criptată, ea va rămâne criptată. Dacă unitatea era decriptată, ea va rămâne decriptată. Acest element este selectat în mod implicit.
În timpul criptării, creează automat conturi Agent de autentificare pentru utilizatorii Windows	Dacă această casetă de selectare este bifată, aplicația creează conturi Agent de autentificare pe baza listei conturilor de utilizatori Windows din computer. În mod implicit, Kaspersky Endpoint Security folosește toate conturile locale și de domenii cu care utilizatorul s-a conectat la sistemul de operare în ultimele 30 de zile.
Setări pentru creare cont Agent de Autentificare	**Toate conturile de pe computer**. Toate conturile de pe computer care au fost active în orice moment. **Toate conturile de domeniu de pe computer**. Toate conturile de pe computer care aparțin unui domeniu și care au fost active în orice moment. **Toate conturile locale de pe computer**. Toate conturile locale de pe computer care au fost active în orice moment. **Cont serviciu cu parolă de unică folosință**. Contul serviciului este necesar pentru a obține acces la computer, de exemplu, atunci când utilizatorul uită parola. De asemenea, poți utiliza contul serviciului drept cont de rezervă. Trebuie să introduci numele contului (în mod implicit, `ServiceAccount`). Kaspersky Endpoint Security creează automat o parolă. Poți găsi parola în consola Kaspersky Security Center. **Administrator local**. Kaspersky Endpoint Security creează un cont de utilizator pentru Agentul de Autentificare pentru administratorul local al computerului. **Manager computer**. Kaspersky Endpoint Security creează un cont de utilizator pentru Agentul de Autentificare pentru contul managerului computerului. Puteți vedea ce cont are rolul de manager de computer în proprietățile computerului din Active Directory. În mod implicit, rolul de manager de computer nu este definit, adică nu corespunde niciunui cont. **Cont activ**. Kaspersky Endpoint Security creează automat un cont Agent de Autentificare pentru contul care este activ în momentul criptării discului.
Creați automat conturi Agent de autentificare pentru toți utilizatorii acestui computer după conectare	Dacă această casetă de selectare este bifată, aplicația verifică informații despre conturile utilizatorilor Windows de pe computer înainte de a porni Agentul de autentificare. Dacă Kaspersky Endpoint Security detectează un cont de utilizator Windows care nu are un cont Agent de autentificare, aplicația va crea un cont nou pentru accesarea unităților de disk criptate. Noul cont Agent de autentificare va avea următoarele setări implicite: numai conectare protejată prin parolă și modificarea parolei la prima autentificare. Prin urmare, nu trebuie să adăugați manual conturi Agent de autentificare utilizând activitatea *Gestionare conturi Agent de Autentificare* pentru computerele ale căror unități de hard disk sunt deja criptate.
Salvează nume de utilizator introdus în Agentul de Autentificare	Dacă această casetă de selectare este bifată, aplicația salvează numele contului Agent de Autentificare. Nu ți se va solicita să introduci numele contului la următoarea încercare de finalizare a autorizării în Agentul de Autentificare când folosești același cont.

Parametru	Descriere
Criptează doar spațiu de disc utilizat (reduce durata criptării)	Această casetă de selectare activează/dezactivează opțiunea care limitează zona de criptare la sectoarele ocupate de pe unitatea de hard disk. Această limită îți permite reducerea timpului necesar pentru criptare. Activarea sau dezactivarea caracteristicii **Criptează doar spațiu de disc utilizat (reduce durata criptării)** după pornirea criptării nu modifică această setare până când unitățile de hard disk nu sunt decriptate. Trebuie să bifezi sau să debifezi această casetă de selectare înainte de a începe criptarea. Dacă această casetă de selectare este bifată, sunt criptate numai poțiunile de pe unitatea de hard disk care sunt ocupate de fișiere. Kaspersky Endpoint Security criptează automat datele noi atunci când sunt adăugate. Dacă această casetă de selectare este debifată, va fi criptată întreaga unitate de hard disk, inclusiv fragmentele reziduale din fișiere șterse și modificate anterior. Această opțiune este recomandată pentru unități de hard disk noi, ale căror date nu au fost modificate sau șterse. Dacă aplici criptarea unei unități de hard disk aflate deja în uz, se recomandă să criptezi întreaga unitate de hard disk. Aceasta asigură protecția pentru toate datele, chiar și pentru datele șterse care pot fi eventual recuperate. În mod implicit, caseta de selectare este debifată.
Utilizează Legacy USB Support (nu se recomandă)	Această casetă de selectare activează sau dezactivează funcționalitatea Legacy USB Support. *Legacy USB Support* **este** o funcție BIOS/UEFI care vă permite să folosiți dispozitive USB (cum ar fi un token de securitate) în faza de pornire a computerului, înainte de a porni sistemul de operare (modul BIOS). Legacy USB Support nu afectează acceptarea dispozitivelor USB după pornirea sistemului de operare. Dacă această casetă de selectare este bifată, este activată acceptarea dispozitivelor USB la pornirea inițială a computerului. Când funcția Legacy USB Support este activată, Agentul de Autentificare în modul BIOS nu acceptă lucrul cu tokenuri prin USB. Se recomandă folosirea acestei opțiuni numai atunci când există o problemă de compatibilitate hardware și numai pentru acele computere pe care a apărut problema.
Setări parolă	Setări pentru complexitatea parolei contului Agent de Autentificare. Când utilizați tehnologia Single Sign-on, Agentul de Autentificare ignoră cerințele privind complexitatea parolei specificate în Kaspersky Security Center. Puteți seta cerințele privind complexitatea parolei în setările sistemului de operare.
Utilizare tehnologia Single Sign-On (SSO)	Tehnologia SSO face posibilă utilizarea acelorași acreditări de cont pentru a accesa unități de hard disk criptate și pentru conectare la sistemul de operare. Dacă această casetă de selectare este bifată, trebuie să introduceți acreditările contului pentru a accesa unități de hard disk criptate și pentru a vă conecta apoi automat la sistemul de operare. Dacă această casetă de selectare este debifată, pentru a accesa unități de hard disk criptate și pentru a te conecta apoi la sistemul de operare, trebuie să introduci separat acreditări pentru accesarea unităților criptate și acreditări pentru un cont de utilizator al sistemului de operare.
Încadrare furnizori acreditări terți	Kaspersky Endpoint Security acceptă furnizorul de acreditări terț ADSelfService Plus. Când lucrați cu furnizori de acreditări terți, Agentul de Autentificare interceptează parola înainte ca sistemul de operare să fie încărcat. Aceasta înseamnă că un utilizator trebuie să introducă o parolă o singură dată când se conectează la Windows. După ce se conectează la Windows, utilizatorul poate utiliza capacitățile unui furnizor de acreditări terț pentru autentificare în serviciile corporative, de exemplu. Furnizorii de acreditări terți permit utilizatorilor să-și reseteze în mod independent propria parolă. În acest caz, Kaspersky Endpoint Security va actualiza automat parola pentru Agentul de Autentificare. Dacă utilizați un furnizor de acreditări terț care nu este acceptat de aplicație, este posibil să întâmpinați anumite limitări în funcționarea tehnologiei Single Sign-On.
Ajutor	**Autentificare**. Text pentru ajutor care apare în fereastra Agent de Autentificare atunci când introduceți acreditările contului. **Modifică parola**. Text pentru ajutor care apare în fereastra Agent de Autentificare atunci când modificați parola pentru contul Agent de Autentificare. **Recuperare parolă**. Text pentru ajutor care apare în fereastra Agent de Autentificare atunci când recuperați parola pentru contul Agent de Autentificare.

Parametru	Descriere
Mod criptare	**Se criptează toate unitățile de hard disk**. Dacă această opțiune este selectată, aplicația criptează toate unitățile de hard disk atunci când este aplicată politica. Dacă pe computer sunt instalate mai multe sisteme de operare, după criptare vei putea încărca doar sistemul de operare pe care este instalată aplicația. **Se decriptează toate unitățile de hard disk**. Dacă această opțiune este selectată, aplicația decriptează toate unitățile de hard disk criptate anterior atunci când este aplicată politica. **Lasă nemodificat**. Dacă este selectat acest element, aplicația lasă unitățile în starea existentă atunci când este aplicată politica. Dacă unitatea era criptată, ea va rămâne criptată. Dacă unitatea era decriptată, ea va rămâne decriptată. Acest element este selectat în mod implicit.
Permite utilizare autentificare BitLocker, care solicită intrarea de la tastatură înaintea preîncărcării sistemului pe tablete	Utilizând o metodă de autentificare care necesită introducerea de date într-un mediu pre-bootare (înaintea încărcării sistemului), chiar dacă platforma nu acceptă introducerea înaintea încărcării sistemului (de exemplu, tastaturile de pe ecranul tactil al tabletelor). Ecranul tactil al computerelor tabletă nu este disponibil în mediul preboot. Pentru a finaliza autentificarea BitLocker pe computerele tabletă, utilizatorul trebuie să conecteze o tastatură USB, de exemplu. Dacă această casetă de selectare este bifată, este permisă utilizarea autentificării ce solicită intrarea de la tastatură înaintea încărcării sistemului. Recomandăm utilizarea acestei setări numai pentru dispozitivele care prezintă instrumente alternative pentru introducerea datelor înaintea încărcării sistemului, de exemplu o tastatură USB, în plus față de tastaturile de pe ecranul tactil. În cazul în care caseta de selectare este debifată, BitLocker Drive Encryption nu este posibilă pe tablete.
Utilizează criptare hardware (Windows 8 și versiunile ulterioare)	Dacă această casetă de selectare este bifată, aplicația folosește criptarea hardware. Acest lucru îți permite să crești viteza criptării și să folosești mai puțin resurse ale computerului.
Criptează doar spațiul de disc utilizat (Windows 8 și versiuni ulterioare)	Această casetă de selectare activează/dezactivează opțiunea care limitează zona de criptare la sectoarele ocupate de pe unitatea de hard disk. Această limită îți permite reducerea timpului necesar pentru criptare. Activarea sau dezactivarea caracteristicii **Criptează doar spațiu de disc utilizat (reduce durata criptării)** după pornirea criptării nu modifică această setare până când unitățile de hard disk nu sunt decriptate. Trebuie să bifezi sau să debifezi această casetă de selectare înainte de a începe criptarea. Dacă această casetă de selectare este bifată, sunt criptate numai poțiunile de pe unitatea de hard disk care sunt ocupate de fișiere. Kaspersky Endpoint Security criptează automat datele noi atunci când sunt adăugate. Dacă această casetă de selectare este debifată, va fi criptată întreaga unitate de hard disk, inclusiv fragmentele reziduale din fișiere șterse și modificate anterior. Această opțiune este recomandată pentru unități de hard disk noi, ale căror date nu au fost modificate sau șterse. Dacă aplici criptarea unei unități de hard disk aflate deja în uz, se recomandă să criptezi întreaga unitate de hard disk. Aceasta asigură protecția pentru toate datele, chiar și pentru datele șterse care pot fi eventual recuperate. În mod implicit, caseta de selectare este debifată.

Parametru	Descriere
Metoda de atentificare	**Doar parola (Windows 8 și versiunile ulterioare)** Dacă această opțiune este selectată, Kaspersky Endpoint Security solicită utilizatorului o parolă atunci când acesta încearcă să acceseze o unitate criptată. Această opțiune poate fi selectată atunci când nu este folosit un Trusted Platform Module (TPM). **Trusted Platform Module (TPM)** Dacă această opțiune este selectată, BitLocker folosește un Trusted Platform Module. Un *Trusted Platform Module* (TPM) este un microcip dezvoltat pentru a furniza funcții de bază legate de securitate (de exemplu, pentru stocarea cheilor de criptare). De obicei un Trusted Platform Module este instalat pe placa de bază a computerului și interacționează cu alte componente ale sistemului prin magistrala hardware. Pentru calculatoarele care execută Windows 7 sau Windows Server 2008 R2, este disponibilă numai criptarea folosind un modul TPM. Dacă nu este instalat un modul TPM, criptarea BitLocker nu este posibilă. Utilizarea unei parole pe aceste computere nu este acceptată. Un dispozitiv echipat cu un Trusted Platform Module poate crea chei de criptare care pot fi decriptate numai folosind dispozitivul respectiv. Un Trusted Platform Module criptează cheile de criptare folosind propria cheie de stocare pentru rădăcină. Cheia de stocare pentru rădăcină este stocată în Trusted Platform Module. Acest lucru oferă un nivel suplimentar de protecție împotriva încercărilor de compromitere a cheilor de criptare. Această acțiune este selectată în mod implicit. Poți seta o măsură suplimentară de protecție pentru acces la cheia de criptare și poți cripta cheia cu o parolă sau cu un PIN: • **Utilizează codul PIN pentru TPM**. Dacă această casetă de selectare este bifată, un utilizator poate utiliza un cod PIN pentru a obține acces la o cheie de criptare care este stocată pe un Trusted Platform Module (TPM). Dacă această casetă de selectare este debifată, utilizatorilor li se interzice utilizarea codurilor PIN. Pentru a accesa cheia de criptare, un utilizator trebuie să introducă parola. • **Trusted platform module (TPM) sau parola, dacă TPM este indisponibil**. Dacă este selectată această opțiune, utilizatorul poate folosi o parolă pentru a obține acces la cheile de criptare atunci când Trusted Platform Module (TPM) nu este disponibil. În cazul în care caseta de selectare este debifată și TPM nu este disponibil, criptarea completă a discului nu va începe. Metoda de autentificare selectată trebuie să fie configurată prin specificarea cerințelor privind parola sau codul PIN: • **Lungime minimă PIN (caractere)**. • **Lungime minimă parolă (caractere)**. • **Limitare perioada de valabilitate a parolei / PIN-ului pentru TPM (zile)**. • **Utilizează codul PIN îmbunătățit (litere și cifre)**. *Codul PIN îmbunătățit* permite utilizarea altor caractere în afară de cele numerice: litere latine majuscule și minuscule, caractere speciale și spații.
Recreați automat cheie de recuperare (zile)	Actualizează automat parola pentru a restabili accesul la o unitate protejată de BitLocker. Dacă este bifată caseta de selectare, specifică perioada de valabilitate a parolei cheii de recuperare. Acest lucru ajută la prevenirea reutilizării parolei cheii de recuperare.

File Level Encryption

Criptarea fișierelor nu este acceptată pe computerele bazate pe arhitectura Arm.

Această componentă este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Windows pentru stații de lucru. Această componentă nu este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Windows pentru servere.

Poți compila liste de fișiere după extensie sau după grupuri de extensii și liste de directoare stocate pe unitățile locale ale computerului și poți crea reguli pentru criptarea fișierelor care sunt create de aplicații specifice. După aplicarea unei politici, Kaspersky Endpoint Security criptează și decriptează următoarele fișiere:

- fișiere adăugate separat la liste pentru criptare și decriptare;
- fișiere stocate în directoare adăugate la liste pentru criptare și decriptare;
- Fișiere create de aplicații separate.

Criptarea fișierelor are următoarele caracteristici speciale:

- Kaspersky Endpoint Security criptează/decriptează fișiere din directoare predefinite numai pentru profiluri de utilizatori locali de pe sistemul de operare. Kaspersky Endpoint Security nu criptează sau decriptează fișierele din directoarele predefinite ale profilurilor de utilizator în roaming, profilurilor de utilizator obligatorii, profilurilor de utilizator temporare sau directoarele redirecționate.
- Kaspersky Endpoint Security nu criptează fișiere a căror modificare ar putea afecta sistemul de operare și aplicațiile instalate. De exemplu, următoarele fișiere și directoare și toate directoarele imbricate se regăsesc pe lista de excluderi de la criptare:
  - %WINDIR%;
  - %PROGRAMFILES% și %PROGRAMFILES(X86)%;
  - Fișiere Windows registry.

  Lista de excluderi de la criptare nu poate fi vizualizată sau editată. Chiar dacă se pot adăuga în lista de criptare fișiere și directoare aflate în lista de excluderi de la criptare, acestea nu vor fi criptate în timpul activității de criptare a fișierelor.

Setările componentei File Level Encryption

Parametru	Descriere
Mod criptare	**Lasă nemodificat**. Dacă este selectat acest element, Kaspersky Endpoint Security lasă fișierele și directoarele nemodificate, fără a le cripta sau a le decripta. **În conformitate cu regulile**. Dacă acest articol este selectat, Kaspersky Endpoint Security criptează fișierele și directoarele conform regulilor de criptare, decriptează fișierele și directoarele conform regulilor de decriptare și reglementează accesul aplicațiilor la fișierele criptate în conformitate cu regulile aplicației. **Decriptează tot**. Dacă este selectat acest element, Kaspersky Endpoint Security decriptează toate fișierele și directoarele criptate.
Criptare	Această filă prezintă regulile de criptare pentru fișiere stocate pe unitățile locale. Puteți adăuga fișiere după cum urmează: • **Directoare predefinite**. Kaspersky Endpoint Security vă permite să adăugați următoarele zone: **Documente**. Fișiere din directorul standard *Documente* al sistemului de operare și subdirectoarele sale. **Favorite**. Fișiere din directorul standard *Favorite* al sistemului de operare și subdirectoarele sale. **Desktop**. Fișiere din directorul standard *Desktop* al sistemului de operare și subdirectoarele sale. **Fișiere temporare**. Fișiere temporare legate de funcționarea aplicațiilor instalate pe computer. De exemplu, aplicațiile Microsoft Office creează fișiere temporare care conțin copii de rezervă ale documentelor. **Fișiere Outlook**. Fișiere legate de funcționarea clientului de e-mail Outlook: fișiere de date (PST), fișiere de date offline (OST), fișiere offline address book (OAB) și fișiere personal address book (PAB). • **Director personalizat**. Puteți introduce calea către director. Când adăugați o cale către director, respectați următoarele reguli: Utilizați o variabilă de mediu (de exemplu, `%FOLDER%\UserFolder\`). Puteți utiliza o variabilă de mediu o singură dată și numai la începutul căii. Nu folosiți căi relative. Nu folosiți caracterele `*` și `?`. Nu folosiți căi UNC. Utilizați `;` sau `,` drept caracter separator. • **Fișiere după extensie**. Puteți selecta grupuri de extensii din listă, cum ar fi grupul de extensii *Arhive*. De asemenea, puteți adăuga manual extensia fișierului.
Decriptare	Această filă prezintă regulile de decriptare pentru fișiere stocate pe unitățile locale.

Parametru	Descriere
Reguli pentru aplicații	Fila afișează un tabel care conține reguli de acces la fișierele criptate pentru aplicații și reguli de criptare pentru fișierele create sau modificate de către aplicații individuale.
Pachete criptate	Cerințe privind complexitatea parolei care trebuie îndeplinite la crearea pachetelor criptate.

Criptare unități amovibile

Criptarea unităților amovibile nu este acceptată pe computerele bazate pe arhitectura Arm.

Această componentă este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Windows pentru stații de lucru. Această componentă nu este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Windows pentru servere.

Kaspersky Endpoint Security acceptă criptare de fișiere din sisteme de fișiere FAT32 și NTFS. Dacă o unitate amovibilă cu un sistem de fișiere neacceptat este conectată la computer, activitatea de criptare pentru această unitate amovibilă se termină cu o eroare și Kaspersky Endpoint Security atribuie unității amovibile starea numai în citire.

Pentru a proteja datele de pe unitățile amovibile, puteți utiliza următoarele tipuri de criptare:

- Full Disk Encryption (FDE).

  Criptarea întregii unități amovibile, inclusiv a sistemului de fișiere.

  Nu este posibilă accesarea datelor criptate în afara rețelei corporative. De asemenea, este imposibil să accesați date criptate din rețeaua corporativă în cazul în care computerul nu este conectat la Kaspersky Security Center (de ex. pe un computer „invitat”).

- File Level Encryption (FLE).

  Criptarea numai a fișierelor de pe o unitate amovibilă. Sistemul de fișiere rămâne neschimbat.

  Criptarea fișierelor de pe unitățile amovibile oferă capacitatea de a accesa date din afara rețelei corporative folosind un mod special numit *mod portabil*.

În timpul criptării, Kaspersky Endpoint Security creează o cheie principală. Kaspersky Endpoint Security salvează cheia principală în următoarele depozite:

- Kaspersky Security Center.
- Computerul utilizatorului.

  Cheia principală este criptată cu cheia secretă a utilizatorului.

- Unitatea amovibilă.

  Cheia principală este criptată cu cheia publică a Kaspersky Security Center.

După finalizarea criptării, datele de pe unitatea amovibilă sunt accesibile în rețeaua corporativă ca și cum ați utiliza o unitate amovibilă convențională necriptată.

Accesarea datelor criptate

Când este conectată o unitate amovibilă cu date criptate, Kaspersky Endpoint Security efectuează următoarele acțiuni:

1. Verifică o cheie principală în spațiul de stocare local de pe computerul utilizatorului.

   Dacă se găsește cheia principală, utilizatorul obține acces la datele de pe unitatea amovibilă.

   Dacă nu se găsește cheia principală, Kaspersky Endpoint Security efectuează următoarele acțiuni:

   a. Trimite o solicitare către Kaspersky Security Center.

      După primirea solicitării, Kaspersky Security Center trimite un răspuns care conține cheia principală.

   b. Kaspersky Endpoint Security salvează cheia principală în stocarea locală de pe computerul utilizatorului pentru operațiunile ulterioare cu unitatea amovibilă criptată.

2. Decriptează datele.

Caracteristicile speciale ale criptării unității amovibile

Criptarea unităților amovibile are următoarele caracteristici speciale:

- Politica cu setările implicite pentru criptarea unității amovibile este concepută pentru un grup specific de computere gestionate. Prin urmare, rezultatul aplicării politicii Kaspersky Security Center configurate pentru criptarea/decriptarea unităților amovibile depinde de computerul la care este conectată unitatea amovibilă.
- Kaspersky Endpoint Security nu criptează/decriptează fișiere care au permisiunea Doar citire și care sunt stocate pe unități amovibile.
- Următoarele tipuri de dispozitive sunt acceptate ca unități amovibile:
  - Medii de date conectate prin magistrala USB
  - Unități de hard disk conectate prin magistralele USB și FireWire
  - Unități SSD conectate prin magistralele USB și FireWire

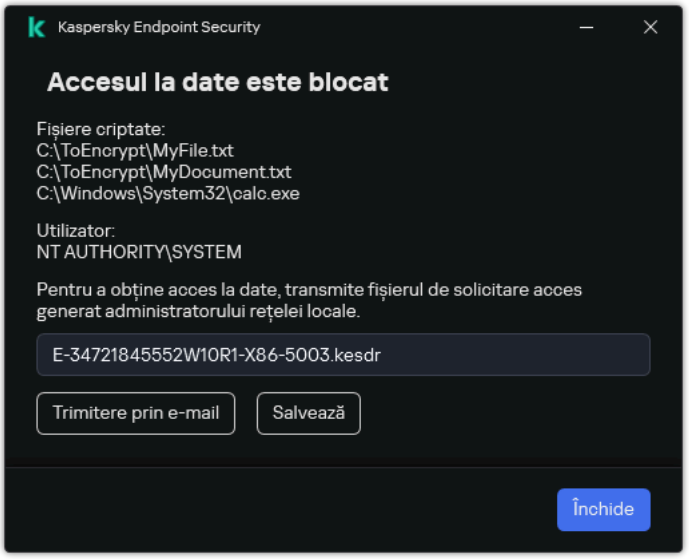
Parametru	Descriere
Mod criptare	**Criptează unitate amovibilă în întregime**. Dacă este selectat acest element, atunci când se aplică politica cu setările de criptare specificate pentru unități amovibile, Kaspersky Endpoint Security criptează unitățile amovibile sector cu sector, inclusiv sistemele lor de fișiere. **Criptează toate fișierele**. Dacă este selectat acest element, atunci când se aplică politica cu setările de criptare specificate pentru unități amovibile, Kaspersky Endpoint Security criptează toate fișierele care sunt stocate pe unitățile amovibile. Kaspersky Endpoint Security nu recriptează fișierele care sunt deja criptate. Conținutul sistemului de fișiere de pe o unitate amovibilă, inclusiv structura directoarelor și numele fișierelor criptate, nu va fi criptat și va rămâne accesibil. **Criptează numai fișiere noi**. Dacă este selectat acest element, atunci când se aplică politica cu setările de criptare specificate pentru unități amovibile, Kaspersky Endpoint Security criptează numai acele fișiere care au fost adăugate sau modificate pe unitățile amovibile după ultima aplicare a politicii aplicației Kaspersky Security Center. Acest mod de criptare este util atunci când o unitate amovibilă este folosită atât în scop personal, cât și pentru serviciu. Acest mod de criptare îți permite să lași vechile fișiere nemodificate și să le criptezi numai pe acelea pe care utilizatorul le creează pe un computer de serviciu pe care este instalat Kaspersky Endpoint Security și pentru care funcția de criptare este activată. Ca urmare, accesul la fișierele personale va fi disponibil mereu, indiferent dacă aplicația Kaspersky Endpoint Security este instalată sau nu pe computerul pe care funcția de criptare este activată. **Decriptează unitate amovibilă în întregime**. Dacă este selectat acest element, atunci când se aplică politica cu setările de criptare specificate pentru unități amovibile, Kaspersky Endpoint Security decriptează toate fișierele criptate stocate pe unitățile amovibile, precum și sistemele de fișiere ale unităților amovibile, dacă acestea au fost criptate anterior. **Lasă nemodificat**. Dacă este selectat acest element, aplicația lasă unitățile în starea existentă atunci când este aplicată politica. Dacă unitatea era criptată, ea va rămâne criptată. Dacă unitatea era decriptată, ea va rămâne decriptată. Acest element este selectat în mod implicit.
Mod portabil	Această casetă de selectare activează/dezactivează pregătirea unei unități amovibile, ceea ce face posibil accesul la fișierele stocate pe această unitate amovibilă pe computerele din afara rețelei corporative. Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security solicită utilizatorului să specifice o parolă înainte de criptarea fișierelor de pe o unitate amovibilă, atunci când se aplică politica. Parola este necesară pentru accesul la fișierele criptate pe o unitate amovibilă pe computerele din afara rețelei corporative. Puteți configura complexitatea parolei. Modul portabil este disponibil pentru modurile **Criptează toate fișierele** sau **Criptează numai fișiere noi**.
Criptează doar spațiul de disc utilizat	Această casetă de selectare activează/dezactivează modul de criptare în care sunt criptate numai sectoarele de disc ocupate. Acest mod este recomandat pentru unități noi, ale căror date nu au fost modificate sau șterse. Dacă această casetă de selectare este bifată, sunt criptate numai poțiunile din unitate care sunt ocupate de fișiere. Kaspersky Endpoint Security criptează automat datele noi atunci când sunt adăugate. Dacă această casetă de selectare este debifată, va fi criptată întreaga unitate, inclusiv fragmentele reziduale din fișiere șterse și modificate anterior. Posibilitatea de criptare numai a spațiului ocupat este disponibilă numai pentru modul **Criptează unitate amovibilă în întregime**. După începerea criptării, activarea/dezactivarea funcției **Criptează doar spațiul de disc utilizat** nu va modifica această setare. Trebuie să bifezi sau să debifezi această casetă de selectare înainte de a începe criptarea.

Reguli personalizate	Acest tabel conține dispozitivele pentru care s-au definit regulile de criptare particularizate. Puteți crea reguli de criptare pentru unități amovibile individuale în următoarele moduri:
	• Adăugați o unitate amovibilă din lista de dispozitive de încredere pentru Control dispozitive.
	• Adăugați manual o unitate amovibilă:
	  • După ID-ul dispozitivului (Hardware ID sau HWID)
	  • După modelul dispozitivului: Vendor ID (VID) și Product ID (PID)

Permiteți criptarea unităților amovibile în modul offline	Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security criptează unitățile amovibile chiar și atunci când nu există o conexiune la Kaspersky Security Center. În acest caz, datele necesare pentru decriptarea unităților amovibile sunt stocate pe unitatea de hard disk a computerului la care este conectată unitatea amovibilă și nu sunt transmise către Kaspersky Security Center. Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security nu criptează unitățile amovibile atunci când nu există o conexiune la Kaspersky Security Center.
Setări parolă de criptare / Manager de fișiere portabil	Setări privind complexitatea parolei pentru Manager de fișiere portabil.

Șabloane (criptarea datelor)

După criptarea datelor, Kaspersky Endpoint Security poate restricționa accesul la date, de exemplu, din cauza unei modificări a infrastructurii organizației și a unei modificări a Serverului de administrare Kaspersky Security Center. Dacă un utilizator nu are acces la datele criptate, acesta poate solicita administratorului accesul la date. Cu alte cuvinte, utilizatorul trebuie să trimită administratorului un fișier de solicitare a accesului. Utilizatorul trebuie apoi să încarce fișierul de răspuns primit de la administrator în Kaspersky Endpoint Security. Kaspersky Endpoint Security vă permite să solicitați acces la date de la administrator prin e-mail (consultați figura de mai jos).



Solicitarea accesului la datele criptate

Un șablon este furnizat pentru raportarea lipsei accesului la datele criptate. Pentru confortul utilizatorului, puteți completa următoarele câmpuri:

- **Către**. Introduceți adresa de e-mail a grupului de administrare cu drepturi la funcțiile de criptare a datelor.
- **Subiect**. Introduceți subiectul e-mailului cu solicitarea dvs. de acces la fișierele criptate. Puteți adăuga, de exemplu, etichete la mesajele de filtrare.
- **Mesajul utilizatorului**. Dacă este necesar, modificați conținutul mesajului. Puteți utiliza variabile pentru a obține datele necesare (de exemplu, variabila `%USER_NAME%`).

Excluderi

O *zonă de încredere* este o listă de obiecte și aplicații configurate de administratorul de sistem, pe care Kaspersky Endpoint Security nu le monitorizează când este activ.

Administratorul formează zona de încredere independent, luând în considerare caracteristicile obiectelor gestionate și aplicațiile instalate pe computer. Este posibil să fie necesară includerea obiectelor și aplicațiilor în zona de încredere când Kaspersky Endpoint Security blochează accesul la un anumit obiect sau la o anumită aplicație, dacă ești sigur că obiectul sau aplicația respectivă este inofensivă. Un administrator poate permite, de asemenea, unui utilizator să își creeze propria zonă de încredere locală pentru un anumit computer. În acest fel, utilizatorii își pot crea propriile liste locale de excluderi și aplicații de încredere, pe lângă zona generală de încredere dintr-o politică.

Începând cu Kaspersky Endpoint Security 12.5 for Windows, poți adăuga telemetrie EDR în zona de încredere. Acest lucru permite optimizarea datelor pe care aplicația le trimite către serverul de colectare a telemetriei pentru soluția Kaspersky Anti Targeted Attack Platform (EDR).

Începând cu Kaspersky Endpoint Security 12.6 for Windows, excluderile de scanare și aplicații de încredere sunt adăugate la zona de încredere. Excluderile de la scanare și aplicațiile de încredere predefinite ajută la configurarea rapidă a Kaspersky Endpoint Security pe serverele SQL, serverele Microsoft Exchange și System Center Configuration Manager. Aceasta înseamnă că nu trebuie să configurați manual o zonă de încredere pentru aplicație pe servere.

Începând cu Kaspersky Endpoint Security 12.8 for Windows, poți instala aplicația în modul Light Agent pentru a proteja mediile virtuale. Excluderile de la scanare predefinite și aplicațiile de încredere te pot ajuta să configurezi rapid Kaspersky Endpoint Security în mediile virtuale Citrix și VMware.

Excluderi de la scanare

O *excludere de la scanare* este un set de condiții care trebuie să fie îndeplinite pentru ca aplicația Kaspersky Endpoint Security să nu scaneze un anumit obiect pentru viruși și alte amenințări. Excluderile de la scanare fac posibilă utilizarea în siguranță a software-urilor legitime care pot fi exploatate de infractori pentru a aduce daune computerului sau datelor utilizatorului. Cu toate că nu au funcții rău intenționate, astfel de aplicații pot fi exploatate de intruși. Pentru detalii despre software-urile legitime care pot fi utilizate de intruși pentru a aduce daune computerului sau datelor personale, consultă site-ul web Enciclopedia IT Kaspersky.

Este posibil ca programul Kaspersky Endpoint Security să blocheze astfel de aplicații. Pentru a împiedica blocarea lor, poți configura excluderi de la scanare pentru aplicațiile în uz. În acest scop, adaugă numele sau masca de nume listată în Enciclopedia IT a Kaspersky la zona de încredere. De exemplu, utilizezi frecvent aplicația Radmin pentru administrarea de la distanță a computerelor. Kaspersky Endpoint Security privește această activitate ca suspectă și este posibil să o blocheze. Pentru a împiedica blocarea aplicației, creează o excludere de la scanare cu numele sau masca de nume listată în Enciclopedia IT a Kaspersky.

Dacă o aplicație care colectează informații și le trimite spre procesare este instalată pe computerul dvs., Kaspersky Endpoint Security poate clasifica această aplicație ca malware. Pentru a evita acest lucru, poți exclude aplicația de la scanare configurând Kaspersky Endpoint Security așa cum este descris în acest document.

Excluderile de la scanare pot fi utilizate de următoarele componente și acțiuni ale aplicației, care sunt configurate de către administratorul de sistem:

- Behavior Detection
- Exploit Prevention
- Host Intrusion Prevention
- File Threat Protection
- Web Threat Protection

- Mail Threat Protection
- Activitatea *Scanare malware*

Lista aplicațiilor de încredere

Lista de aplicații de încredere este o listă de aplicații pentru care Kaspersky Endpoint Security nu monitorizează activitatea cu fișierele și activitatea în rețea (inclusiv activitatea rău intenționată) și nici accesul la registrul de sistem. În mod implicit, Kaspersky Endpoint Security monitorizează obiectele care sunt deschise, executate sau salvate de orice proces al unei aplicații și controlează activitatea tuturor aplicațiilor și traficul în rețea generat de acestea. După ce o aplicație este adăugată la lista de aplicații de încredere, Kaspersky Endpoint Security oprește monitorizarea activității aplicației.

Diferența dintre excluderile de la scanare și aplicațiile de încredere este că, pentru excluderi, Kaspersky Endpoint Security nu scanează fișierele, în timp ce pentru aplicațiile de încredere nu controlează procesele inițiate. Dacă o aplicație de încredere creează un fișier rău intenționat într-un director care nu este inclus în excluderile de la scanare, Kaspersky Endpoint Security va detecta fișierul și va elimina amenințarea. Dacă directorul este adăugat la excluderi, Kaspersky Endpoint Security va omite acest fișier.

De exemplu, dacă presupui obiectele utilizate de aplicația Microsoft Windows Notepad standard ca fiind sigure, ceea ce înseamnă că ai încredere în această aplicație, poți adăuga Microsoft Windows Notepad în lista de aplicații de încredere, astfel încât obiectele utilizate de această aplicație nu sunt monitorizate. Acest lucru va crește performanța computerului, ceea ce este deosebit de important atunci când utilizați aplicații de pe server.

În plus, anumite acțiuni care sunt clasificate de către Kaspersky Endpoint Security ca fiind suspecte este posibil să fie sigure în contextul operațional pentru o serie de aplicații. De exemplu, interceptarea textul introdus de la tastatură este un proces de rutină pentru programele de comutare automată a structurii tastaturii (cum ar fi Punto Switcher). Pentru a ține cont de caracteristicile specifice ale unor astfel de aplicații și pentru a exclude activitatea lor din monitorizare, îți recomandăm să adaugi aceste aplicații în lista de aplicații de încredere.

Aplicațiile de încredere ajută la evitarea problemelor de compatibilitate între Kaspersky Endpoint Security și alte aplicații (de exemplu, problema scanării duble a traficului de rețea al unui computer terț de către Kaspersky Endpoint Security și de către o altă aplicație antivirus).

În același timp, fișierul executabil și procesele aplicației de încredere sunt scanate în continuare după viruși și alte programe malware. O aplicație poate fi exclusă complet de la scanarea Kaspersky Endpoint Security cu ajutorul excluderilor de la scanare.

Setări pentru excluderi

Parametru	Descriere

Tipuri de obiecte detectate

Indiferent de setările configurate pentru aplicații, Kaspersky Endpoint Security detectează și blochează întotdeauna virușii, viermii și troienii. Aceștiai pot cauza daune importante computerului.

- **Viruși și viermi**

  Subcategoria: Viruși și viermi (Viruses_and_Worms)

  Nivel de pericol: Ridicat

  Virușii și viermii clasici efectuează acțiuni care nu sunt autorizate de către utilizator. Ei pot crea copii care se pot înmulți singure.

  Virus clasic

  Când un virus clasic se infiltrează într-un computer, el infectează un fișier, se activează, efectuează acțiuni rău intenționate și adaugă copii ale sale la alte fișiere.

  Un virus clasic se multiplică numai pe resursele locale ale computerului; el nu poate pătrunde singur pe alte computere. El poate fi transferat pe un alt computer numai dacă adaugă o copie a sa la un fișier care este stocat într-un director partajat sau pe un CD inserat sau dacă utilizatorul redirecționează un mesaj de e-mail cu un fișier infectat atașat.

  Codul de virus clasic poate pătrunde în diferite zone ale computerelor, sistemelor de operare și aplicațiilor. În funcție de mediu, virușii se împart în *viruși de fișier*, *viruși de boot*, *viruși de script*, și *viruși macro*.

  Virușii pot infecta fișiere folosind o varietate de tehnici. Virușii de tip *Overwriting* își scriu codul peste o parte din codul fișierului infectat, ștergând astfel conținutul fișierului. Fișierul infectat nu mai funcționează și nu poate fi restaurat. Virușii de tip *Parasitic* modifică fișierele, lăsându-le complet sau parțial funcționale. Virușii de tip *Companion* nu modifică fișiere, dar, în schimb, creează duplicate. Atunci când un fișier infectat este deschis, este pornit un duplicat al acestuia (care este în realitate un virus). De asemenea, sunt întâlnite și următoarele tipuri de viruși: *Viruși de tip Link*, *viruși OBJ*, *viruși LIB*, viruși *cod sursă* și mulți alții.

  Viermе

  La fel ca în cazul unui virus clasic, codul unui vierme se activează și efectuează acțiuni rău intenționate după ce se infiltrează într-un computer. Virușii se numesc astfel datorită capacității lor de a se „târî" de la un computer la altul și de a răspândi copii ale lor prin numeroase canale de date, fără permisiunea utilizatorului.

  Modul în care viermii se răspândesc este principala caracteristică permițând diferențierea între diferitele tipuri de viermi. Tabelul următor conține o prezentare generală a diferitelor tipuri de viermi, clasificați după modul în care se răspândesc.

  Moduri în care se răspândesc viermii

Tip	Name	Descriere
Viermе de e-mail	Vierme e-mail	Ei se răspândesc prin e-mail. Un mesaj de e-mail infectat conține un fișier infectat cu o copie a unui vierme sau un link către un fișier care este încărcat pe un site Web care este posibil să fi fost modificat prin hacking sau creat exclusiv în acest scop. Atunci când deschizi fișierul atașat, viermele este activat. Atunci când faci clic pe link, descarci sau deschizi fișierul, viermele începe să execute acțiunile sale rău intenționate. După aceea, el continuă să răspândească alte copii ale sale, căutând alte adrese de e-mail și trimițându-le mesaje infectate.
Viermе de MI	Viermi de client MI	Se răspândesc prin intermediul clienților de mesagerie instantanee. De obicei, acești viermi trimit mesaje care conțin un link către un fișier care conține o copie a viermelui pe un site Web, utilizând listele de contact ale utilizatorului. Atunci când utilizatorul descarcă și deschide fișierul, viermele se activează.
Viermе de IRC	Viermi de chat pe Internet	Se răspândesc prin Internet Relay Chats, sisteme de servicii care permit comunicarea în timp real cu alte persoane de pe Internet. Acești viermi publică un fișier cu o copie a lor sau un link către un fișier într-un chat Internet. Atunci când utilizatorul descarcă și deschide fișierul, viermele se activează.
Viermе de rețea	Viermi de rețea	Acești viermi se răspândesc prin rețele de computere. Spre deosebire de alte tipuri de viermi, un vierme tipic de rețea se răspândește fără participarea utilizatorului. El scanează rețeaua locală pentru computere care conțin programe cu vulnerabilități. Pentru aceasta, trimite un pachet de rețea într-un format special (un „exploit") care conține codul viermelui sau o parte din acesta. Dacă în rețea se găsește un computer „vulnerabil", el primește un astfel de pachet de rețea. Atunci când viermele pătrunde complet pe computer, se activează.
Viermе P2P	Viermi pentru rețele de partajare a fișierele	Se răspândesc prin intermediul rețelelor peer-to-peer de partajare a fișierelor. Pentru a se infiltra într-o rețea P2P, viermele se copie într-un director de partajare de fișiere care este de regulă localizat pe computerul utilizatorului. Rețeaua P2P afișează informații despre acest fișier, astfel încât utilizatorul poate „găsi" fișierul infectat prin rețea, asemenea oricărui alt fișier, și îl poate apoi descărca și deschide. Viermii mai sofisticați emulează protocolul de rețea al unei rețele P2P specifice: ei returnează răspunsuri pozitive la interogări de căutare și oferă spre descărcare copii ale lor.
Viermе	Alte tipuri de viermi	Alte tipuri de viermi includ: • Viermi care se răspândesc prin resurse de rețea. Utilizând funcțiile sistemului de operare, ei scanează după directoare de rețea disponibile, se conectează la computere prin Internet și încearcă să obțină acces complet la unitățile lor de hard disk. Spre deosebire de tipurile de viermi descrise mai sus, alte tipuri de viermi nu se activează singuri, ci atunci când utilizatorul deschide un fișier care conține o copie a viermelui. • Viermi care nu folosesc niciuna dintre metodele descrise în tabelul anterior pentru a se răspândi (de exemplu, ceii care se răspândesc prin telefoanele celulare).

- **Troieni (inclusiv programe ransomware)**

  Subcategoria: Troieni

  Nivel de pericol: Ridicat

Spre deosebire de viermi și de viruși, troienii nu se multiplică singuri. De exemplu, ei penetrează un computer prin e-mail sau printr-un browser, atunci când utilizatorul vizitează o pagină Web infectată. Troienii se lansează cu participarea utilizatorului. Ei încep să execute acțiunile rău intenționate imediat după ce sunt lansați.

Diverși troieni au comportamente diferite pe computerele infectate. Principala funcție a troienilor constă în blocarea, modificarea sau distrugerea informațiilor și dezactivarea unor computere sau rețele. Troienii pot primi și trimite fișiere, le pot executa, pot afișa mesaje pe ecran, pot solicita pagini Web, pot descărca și instala programe și pot reporni computerul.

Hacker-ii folosesc adesea „seturi" de troieni diferiți.

Tipurile de comportament de troian sunt descrise în tabelul următor.

Tipuri de comportament de troian pe un computer infectat

Tip	Name	Descriere
Trojan-ArcBomb	Troieni – „bombe de arhivă"	Atunci când sunt dezarhivați, aceste arhive cresc în dimensiuni, până când funcționarea computerului este afectată. Atunci când utilizatorul încearcă să dezarhiveze o astfel de arhivă, computerul poate fi încetinit sau se poate bloca; unitatea de hard disc se umple cu date „goale". „Bombele de arhivă" sunt periculoase în special pe serverele de fișiere și de e-mail. Dacă serverul folosește un sistem automat pentru procesarea informațiilor primite, o „bombă de arhivă" poate opri serverul.
Backdoor	Troieni pentru administrare la distanță	Sunt considerați tipul cel mai periculos de troieni. Prin funcțiile lor se aseamănă cu aplicațiile de administrare la distanță care sunt instalate pe computere. Aceste programe se instalează pe computer fără a fi observate de utilizator, permițând intrusului să gestioneze computerul de la distanță.
Troian	Troieni	Includ următoarele tipuri de aplicații rău intenționate: • **Troieni clasici**. Aceștia execută doar funcții de bază ale troienilor: blochează, modifică sau distrug informații și dezactivează computere sau rețele. Ei nu au funcționalități avansate, spre deosebire de alte tipuri de troieni descrișii în tabel. • **Troieni versatili**. Aceste programe au caracteristici avansate, tipice pentru anumite tipuri de troieni.
Trojan-Ransom	Troieni de recompensă	Ei țin „ostatice" informațiile utilizatorului, modificându-le sau blocându-le sau afectând funcționarea computerului, astfel încât utilizatorul pierde capacitatea de a utiliza informațiile. Intrusul solicită o recompensă din partea utilizatorului, promițând că va trimite o aplicație pentru restaurarea performanței computerului și a datelor care au fost stocate pe acesta.
Trojan-Clicker	Troieni de tip clicker	Ei accesează pagini Web de pe computerul utilizatorului, fie prin trimiterea de comenzi către un browser, pe cont propriu, fie prin modificarea adreselor Web care sunt specificate în fișierele sistemului de operare. Prin utilizarea acestor programe, intrușii execută atacuri de rețea și sporesc numărul de vizite pe un site Web, sporind numărul de reclame banner afișate.
Trojan-Downloader	Troieni programe de descărcare	Ei accesează pagina Web a intrusului, descarcă de pe ea alte aplicații rău intenționate și le instalează pe computerul utilizatorului. Ei pot conține numele fișierului aplicației rău intenționate de descărcat sau îl pot primi de pe pagina Web accesată.
Trojan-Dropper	Troieni de tip Dropper	Ei conțin alți troieni, pe care îi pot depune și apoi instala pe unitatea de hard disc. Intrușii pot folosi programe de tipul Trojan Dropper în următoarele scopuri: • Instalarea unei aplicații rău intenționate fără a fi observat de utilizator: Programele de tipul Trojan Dropper nu afișează mesaje sau afișează mesaje false care informează, de exemplu, că există o eroare într-o arhivă sau o versiune incompatibilă a sistemului de operare. • Protejarea altei aplicații rău intenționate cunoscute de la detecție: nu toate software-urile antivirus pot detecta o aplicație rău intenționată din interiorul altei aplicații de tip Trojan Dropper.
Trojan-Notifier	Troieni de notificare	Ei informează un intrus că este accesibil computerul infectat, trimițând intrusului informații despre computer: adresa IP, numărul portului deschis sau adresa de e-mail. Ei comunică cu introdusul prin e-mail, FTP, accesând pagina Web a intrusului sau într-un alt mod. Programele de tip Trojan Notifier sunt folosite adesea în seturi care conțin mai mulți troieni. Ei îl notifică pe intrus că alți troieni s-au instalat cu succes pe computerul utilizatorului.
Trojan-Proxy	Proxyuri de troieni	Ei permit intrusului să acceseze anonim pagini Web folosind computerul utilizatorului; sunt adesea folosiți pentru a trimite spam.
Trojan-PSW	Programe dedicate sustragerii de parole	Programele care sustrag parole sunt un tip de troieni care fură conturi de utilizator, de exemplu date de înregistrare software. Acești troieni găsesc date confidențiale în fișierele de sistem și în registru și le trimit „atacatorului" prin e-mail, FTP, accesând pagina web a intrusului sau într-un alt mod. Unii dintre acești troieni sunt încadrați în tipuri separate descrise în acest tabel. Aceștia sunt Troieni care fură conturi bancare (Trojan-Banker), date de la utilizatori de clienți de mesagerie instantanee (Trojan-IM) și informații de la utilizatori de jocuri online (Trojan-GameThief).
Trojan-Spy	Spioni troieni	Ei îl spionează pe utilizator, colectând informații despre acțiunile pe efectuate de utilizator în timp ce acesta lucrează la computer. Ei pot intercepta date pe care utilizatorul le introduce de la tastatură, pot face copii de ecran sau pot colecta liste de aplicații active. După ce primesc informațiile, le transferă intrusului prin e-mail, FTP, accesând pagina Web a intrusului sau într-un alt mod.
Trojan-DDoS	Troieni atacatori de rețea	Ei trimit numeroase cereri de pe computerul utilizatorului către un server la distanță. Serverul nu dispune de resurse pentru a procesa toate cererile, astfel că nu mai funcționează (DoS sau Refuzare serviciu) Hackerii infectează adesea multe computere cu aceste programe, astfel încât pot utiliza computerele pentru a ataca simultan un singur server. Programe de tip Refuzare serviciu execută un atac de pe un singur computer, cu cunoștința utilizatorului. Programele de tip DDoS (Refuzare distribuită serviciu) execută atacuri distribuite din mai multe computere, fără a fi observate de utilizatorul computerului infectat.
Trojan-IM	Troieni care fură informații de la utilizatorii clienților de mesagerie instantanee	Fură numere de cont și parole ale utilizatorilor de clienți de mesagerie instantanee. Ei transferă datele intrusului prin e-mail, FTP, accesând pagina Web a intrusului sau într-un alt mod.
Rootkit	Rootkituri	Ei maschează alte aplicații rău intenționate și activitatea acestora, prelungind astfel persistența programelor rău intenționate în sistemul de operare. Ei pot, de asemenea, să ascundă fișiere, procese din memoria unui computer infectat sau chei de registru care execută aplicații rău intenționate. Rootkiturile pot masca schimbul de date între aplicații de pe computerul utilizatorului și alte computere din rețea.
Trojan-SMS	Troieni sub formă de mesaje SMS	Ele infectează telefoane celulare, trimițând mesaje SMS către numere de telefon cu tarif premium.
Trojan-GameThief	Troieni care fură informații de la utilizatorii de jocuri online	Ei fură acreditări de cont de la utilizatorii de jocuri online, după care trimit datele intrusului pe e-mail, prin FTP, accesând pagina Web a intrusului sau într-un alt mod.

Trojan-Banker	Troieni care furcă conturi bancare	Aceştia fură datele conturilor bancare sau datele pentru sistemele de plată electronică; trimit datele hackerului prin e-mail, FTP, accesând pagina web a hackerului sau folosind altă metodă.
Trojan-Mailfinder	Troieni care colectează adrese de e-mail	Ei colectează adrese de e-mail stocate pe iun computer şi le trimit intrusului prin e-mail, FTP, accesând pagina Web a intrusului sau într-un alt mod. Intruşii pot trimite spam către adresele pe care le-au colectat.

- **Instrumente rău intenționate**

  Subcategoria: Instrumente periculoase

  Nivel de pericol: Mediu

  Spre deosebire de alte tipuri de malware, instrumentele periculoase nu îşi execută acţiunile imediat după ce sunt pornite. Ele pot fi stocate în siguranţă şi pornite pe computerul utilizatorului. Intruşii folosesc adesea caracteristicile acestor programe pentru a crea viruşi, viermi şi troieni, să execute atacuri de reţea pe servere la distanţă, să compromită computere sau să execute alte acţiuni rău intenţionate.

  Diverse caracteristici ale instrumentelor periculoase sunt grupate după tipurile descrise în tabelul următor.

  Caracteristici ale instrumentelor periculoase

Tip	Name	Descriere
Constructor	Constructori	Permit crearea de noi viruşi, viermi şi troieni. Unele programe constructor dispun de o interfaţă bazată pe o fereastră standard în care utilizatorul poate selecta tipul aplicaţiei rău intenţionate de creat, modul de contracarare a depanatoarelor şi alte caracteristici.
Dos	Atacuri de reţea	Ei trimit numeroase cereri de pe computerul utilizatorului către un server la distanţă. Serverul nu dispune de resurse pentru a procesa toate cererile, astfel că nu mai funcţionează (DoS sau Refuzare serviciu)
Exploit	Exploituri	Un *exploit* este un set de date sau un cod de program care foloseşte vulnerabilităţile aplicaţiei în care este procesat, executând o acţiune rău intenţionată pe un computer. De exemplu, un exploit poate scrie sau citi fişiere sau poate solicita pagini Web infectate. Diferite exploituri folosesc vulnerabilităţi ale diferitelor aplicaţii sau servicii de reţea. Deghizat ca pachet de reţea, un exploit este transmis prin reţea către numeroase computere, căutând computere cu servicii de reţea vulnerabile. Un exploit într-un fişier DOC foloseşte vulnerabilităţile editorului text. Atunci când utilizatorul deschide fişierul infectat, exploitul poate începe să execute acţiuni care sunt pre-programate de către hacker Un exploit care este încorporat într-un mesaj de e-mail caută vulnerabilităţi în orice client de e-mail. El poate începe să execute o acţiune rău intenţionată imediat ce utilizatorul deschide mesajul infectat în clientul de e-mail respectiv. Viermii de reţea se răspândesc prin reţele, folosind exploituri. Exploiturile de tip Nuker sunt pachete de reţea care dezactivează computerele.
FileCryptor	Programe de criptare	Ele criptează alte aplicaţii rău intenţionate, pentru a le ascunde de aplicaţia antivirus.
Flooder	Programe pentru „contaminarea" reţelelor.	Ele trimit numeroase mesaje prin canale de reţea. Acest tip de instrumente include, de exemplu, instrumente care contaminează camerele Internet Relay Chats. Instrumentele de tip flooder nu includ programe care „contaminează" canale care sunt folosite de clienţi de e-mail, de mesagerie instantanee şi de sisteme de comunicaţii mobile. Aceste programe se disting ca tipuri separate care sunt deschise în tabel (Email-Flooder, IM-Flooder şi SMS-Flooder).
HackTool	Instrumente de hacking	Ele fac posibilă deturnarea computerului pe care sunt instalate sau atacarea altui computer (de exemplu, prin adăugarea de noi conturi de sistem fără permisiunea utilizatorului sau prin ştergerea jurnalelor de sistem pentru a ascunde urme ale prezenţei în sistemul de operare). Acest tip de instrumente include unele sniffere care prezintă funcţii rău intenţionate, cum ar fi interceptarea parolelor. Snifferele sunt programe care permit vizionarea traficului de reţea.
Hoax	Hoaxuri	Ele îl alarmează pe utilizator cu mesaje care seamănă cu cele pentru viruşi: ele pot să „detecteze un virus" într-un fişier care de fapt nu este infectat sau să îl notifice pe utilizator că discul a fost formatat, deşi acest lucru nu s-a întâmplat în realitate.
Spoofer	Instrumente de contrafacere	Ele trimit mesaje şi cereri de reţea cu o adresă a expeditorului falsă. Intruşii folosesc instrumente de tip Spoofer pentru a se deghiza în expeditori reali de mesaje, de exemplu.
VirTool	Instrumente care modifică aplicaţii rău intenţionate	Ele permit modificarea altor programe malware, ascunzându-le de aplicaţiile antivirus.
Email-Flooder	Programe care „contaminează" adrese de e-mail	Ele trimit numeroase mesaje către diferite adrese de e-mail, „contaminându-le" astfel. Un volum mare de mesaje primite îi împiedică pe utilizatori să vizualizeze mesaje utile din inboxurile lor.
IM-Flooder	Programe care „contaminează" traficul clienţilor de mesagerie instantanee	Ele îi inundă cu mesaje pe clienţii aplicaţiilor de mesagerie instantanee. Un volum mare de mesaje îi împiedică pe utilizatori să vizualizeze mesaje utile.
SMS-Flooder	Programe care „contaminează" traficul cu mesaje SMS	Ele trimit numeroase mesaje SMS către telefoane celulare.

- **Adware**

  Subcategoria: Software de advertising (Adware)

  Nivel de pericol: Mediu

  Programele adware afişează informaţii publicitare utilizatorului. Programele adware afişează reclame banner în interfeţele altor programe şi redirecţionează interogările de căutare către pagini Web de publicitate. Unele dintre ele colectează informaţii de marketing despre utilizator şi le trimit dezvoltatorului. Aceste informaţii pot include numele site-urilor Web care sunt vizitate de utilizator sau conţinutul interogărilor de căutare ale utilizatorului. Spre deosebire de programele de tip Trojan-Spy, programele adware trimit aceste informaţii dezvoltatorului, cu permisiunea utilizatorului.

- **Programe de apelare automată**

Subcategoria: software legitim care poate fi utilizat de intruși pentru a aduce daune computerului sau datelor personale.

Nivel de pericol: Mediu

Majoritatea acestor aplicații sunt utile, astfel că mulți utilizatori le execută. Aceste aplicații includ clienți IRC, programe de apelare automată, programe de descărcare a fișierelor, programe de monitorizare a activității sistemului, utilitare de parolă și servere de Internet pentru FTP, HTTP și Telnet.

Cu toate acestea, dacă intruși obțin acces la aceste programe sau dacă le instalează pe computerul utilizatorului, unele dintre caracteristicile aplicației pot fi utilizate pentru a încălca securitatea.

Aceste aplicații diferă după funcția lor; tipurile lor sunt descrise în tabelul următor.

Tip	Name	Descriere
Client-IRC	Clienți de chat Internet	Utilizatorii instalează aceste programe pentru a vorbi cu alte persoane în camere Internet Relay Chats. Intruși îi folosesc pentru a răspândi malware.
Downloader	Programe pentru descărcare	Ele pot descărca fișiere din pagini Web în mod ascuns.
Monitor	Programe pentru monitorizare	Ele permit monitorizarea activității pe computerul pe care sunt instalate (urmărind ce aplicații sunt active și modul în care se modifică date cu aplicațiile care sunt instalate pe alte computere).
PSWTool	Programe de restaurare a parolelor	Ele permit vizualizarea și restaurarea parolelor uitate. Intruși le instalează în mod secret pe computerele utilizatorilor, în același scop.
RemoteAdmin	Programe de administrare la distanță	Sunt folosite pe scară largă de administratorii de sistem. Aceste programe permit obținerea accesului la interfața unui computer la distanță pentru a o monitoriza și a o gestiona. Intruși le instalează în mod secret pe computerele utilizatorilor, în același scop: acela de a monitoriza și a gestiona computere la distanță. Programele legitime de administrare la distanță diferă de troienii de tip Backdoor pentru administrare la distanță. Troienii au capacitatea de a penetra în sistemul de operare independent și de a se instala; programele legale nu pot face acest lucru.
Server-FTP	Servere FTP	Ele funcționează ca servere FTP. Intruși le instalează pe computerul utilizatorului pentru a deschide accesul la distanță prin FTP.
Server-Proxy	Proxy server	Ele funcționează ca servere proxy. Intruși le instalează pe computerul utilizatorului pentru a trimite spam în numele utilizatorului.
Server-Telnet	Servere Telnet	Ele funcționează ca servere Telnet. Intruși le instalează pe computerul utilizatorului pentru a deschide accesul la distanță prin Telnet.
Server-Web	Servere Web	Ele funcționează ca servere Web. Intruși le instalează pe computerul utilizatorului pentru a deschide accesul la distanță prin HTTP.
RiskTool	Instrumente pentru a lucra pe un computer local	Ele oferă utilizatorului opțiuni suplimentare atunci când lucrează pe propriul computer. Instrumentele permit utilizatorului să ascundă fișiere sau ferestre ale aplicațiilor active și să termine procese active.
NetTool	Instrumente de rețea	Ele oferă utilizatorului opțiuni suplimentare atunci când lucrează cu alte computere din rețea. Aceste instrumente permit repornirea computerelor, detectarea porturilor deschise și pornirea aplicațiilor instalate pe computere.
Client-P2P	Clienți de rețea P2P	Ei permit lucrul în rețele peer-to-peer. Ei pot fi folosite de intruși pentru a răspândi malware.
Client-SMTP	Clienți SMTP	Trimite mesaje e-mail fără știrea utilizatorului. Intruși le instalează pe computerul utilizatorului pentru a trimite spam în numele utilizatorului.
WebToolbar	Bare de instrumente Web	Ele adaugă bare de instrumente la interfețele altor aplicații pentru a utiliza motoare de căutare.
FraudTool	Pseudo-programe	Ele se deghizează în alte tipuri de programe. De exemplu, există programe pseudo-antivirus care afișează mesaje despre detectarea de malware. Cu toate acestea, în realitate ele nu găsesc și nu dezinfectează nimic.

- **Software legitim care poate fi utilizat de intruși pentru a aduce daune computerului sau datelor personale**

  Subcategoria: software legitim care poate fi utilizat de intruși pentru a aduce daune computerului sau datelor personale.

  Nivel de pericol: Mediu

  Majoritatea acestor aplicații sunt utile, astfel că mulți utilizatori le execută. Aceste aplicații includ clienți IRC, programe de apelare automată, programe de descărcare a fișierelor, programe de monitorizare a activității sistemului, utilitare de parolă și servere de Internet pentru FTP, HTTP și Telnet.

  Cu toate acestea, dacă intruși obțin acces la aceste programe sau dacă le instalează pe computerul utilizatorului, unele dintre caracteristicile aplicației pot fi utilizate pentru a încălca securitatea.

  Aceste aplicații diferă după funcția lor; tipurile lor sunt descrise în tabelul următor.

Tip	Name	Descriere
Client-IRC	Clienți de chat Internet	Utilizatorii instalează aceste programe pentru a vorbi cu alte persoane în camere Internet Relay Chats. Intruși îi folosesc pentru a răspândi malware.
Downloader	Programe pentru descărcare	Ele pot descărca fișiere din pagini Web în mod ascuns.
Monitor	Programe pentru monitorizare	Ele permit monitorizarea activității pe computerul pe care sunt instalate (urmărind ce aplicații sunt active și modul în care se modifică date cu aplicațiile care sunt instalate pe alte computere).
PSWTool	Programe de restaurare a parolelor	Ele permit vizualizarea și restaurarea parolelor uitate. Intruși le instalează în mod secret pe computerele utilizatorilor, în același scop.

RemoteAdmin	Programe de administrare la distanță	Sunt folosite pe scară largă de administratorii de sistem. Aceste programe permit obținerea accesului la interfața unui computer la distanță pentru a o monitoriza și a o gestiona. Intrușii le instalează în mod secret pe computerele utilizatorilor, în același scop: acela de a monitoriza și a gestiona computere la distanță. Programele legitime de administrare la distanță diferă de troienii de tip Backdoor pentru administrare la distanță. Troienii au capacitatea de a penetra în sistemul de operare independent și de a se instala; programele legale nu pot face acest lucru.
Server-FTP	Servere FTP	Ele funcționează ca servere FTP. Intrușii le instalează pe computerul utilizatorului pentru a deschide accesul la distanță prin FTP.
Server-Proxy	Proxy server	Ele funcționează ca servere proxy. Intrușii le instalează pe computerul utilizatorului pentru a trimite spam în numele utilizatorului.
Server-Telnet	Servere Telnet	Ele funcționează ca servere Telnet. Intrușii le instalează pe computerul utilizatorului pentru a deschide accesul la distanță prin Telnet.
Server-Web	Servere Web	Ele funcționează ca servere Web. Intrușii le instalează pe computerul utilizatorului pentru a deschide accesul la distanță prin HTTP.
RiskTool	Instrumente pentru a lucra pe un computer local	Ele oferă utilizatorului opțiuni suplimentare atunci când lucrează pe propriul computer. Instrumentele permit utilizatorului să ascundă fișiere sau ferestre ale aplicațiilor active și să termine procese active.
NetTool	Instrumente de rețea	Ele oferă utilizatorului opțiuni suplimentare atunci când lucrează cu alte computere din rețea. Aceste instrumente permit repornirea computerelor, detectarea porturilor deschise și pornirea aplicațiilor instalate pe computere.
Client-P2P	Clienți de rețea P2P	Ei permit lucrul în rețele peer-to-peer. Ei pot fi folosite de intruși pentru a răspândi malware.
Client-SMTP	Clienți SMTP	Trimite mesaje e-mail fără știrea utilizatorului. Intrușii le instalează pe computerul utilizatorului pentru a trimite spam în numele utilizatorului.
WebToolbar	Bare de instrumente Web	Ele adaugă bare de instrumente la interfețele altor aplicații pentru a utiliza motoare de căutare.
FraudTool	Pseudo-programe	Ele se deghizează în alte tipuri de programe. De exemplu, există programe pseudo-antivirus care afișează mesaje despre detectarea de malware. Cu toate acestea, în realitate ele nu găsesc și nu dezinfectează nimic.

- **Obiecte arhivate a căror arhivare poate fi utilizată pentru a proteja un cod rău intenționat**

  Subcategoria: Fișiere arhivate care pot provoca daune.

  Nivel de pericol: Mediu.

  Fișierul este împachetat folosind un program de arhivare special, care este utilizat pentru arhivarea programelor malware: viruși, viermi, troieni. Kaspersky Endpoint Security scanează modulul de dezarhivare din arhive SFX (cu autoextragere).

  Pentru a ascunde malware-ul de la detectarea de către un antivirus, hackerii îl arhivează folosind programe de arhivare speciale. Experții Kaspersky au identificat programele de arhivare care sunt cele mai populare în rândul hackerilor.

- **Obiecte arhivate multiplu**

  Subcategoria: Fișiere arhivate care pot provoca daune.

  Nivel de pericol: Mediu.

  Fișierul este împachetat folosind un program de arhivare special, care este utilizat pentru arhivarea programelor malware: viruși, viermi, troieni. Kaspersky Endpoint Security scanează modulul de dezarhivare din arhive SFX (cu autoextragere).

  Pentru a ascunde malware-ul de la detectarea de către un antivirus, hackerii îl arhivează folosind programe de arhivare speciale. Experții Kaspersky au identificat programele de arhivare care sunt cele mai populare în rândul hackerilor.

Excluderi

Acest tabel conține informații despre excluderile de la scanare.

Recomandăm specificarea unor căi relative în locul unor căi absolute. Acest lucru permite excluderea nu doar a obiectelor sistemului de fișiere, ci și a obiectelor fără fișiere. De exemplu, `*\Program Files (x86)\Folder\Subfolder`.

Puteți exclude obiecte din scanări folosind următoarele metode:

- Introduceți calea către fișier sau director.
- Introduceți codul hash al obiectului.
- Folosiți măști:
  - Caracterul `*` (asterisc) ține locul oricărui set de caractere, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\*\*.txt` va include toate căile către fișierele cu extensia TXT din directoarele de pe unitatea C:, dar nu și din subdirectoare.
  - Două caractere `*` consecutive țin locul oricărui set de caractere (inclusiv un set gol) din numele de fișier sau director, inclusiv caracterele `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\**\*.txt` va include toate căile către fișierele cu extensia TXT localizată în directoarele imbricate în `Folder`, cu excepția `Folder` în sine. Masca trebuie să includă cel puțin un nivel de imbricare. Masca `C:\**\*.txt` nu este o mască validă.

- `?` (semn de întrebare) ține locul oricărui caracter individual, cu excepția caracterelor `\` și `/` (delimitatori pentru numele de fișiere și directoare din căile către fișiere și directoare). De exemplu, masca `C:\Folder\???.txt` va include căi pentru toate fișierele din directorul denumit `Folder` care au extensia TXT și un nume format din trei caractere.

  Puteți utiliza măști oriunde într-o cale de fișier sau director. De exemplu, dacă doriți ca domeniul de scanare să includă directorul Descărcări pentru toate conturile de utilizator de pe computer, introduceți masca `C:\Users\*\Downloads\`.

  Kaspersky Endpoint Security acceptă variabile de mediu

  > Kaspersky Endpoint Security nu acceptă variabila de mediu `%userprofile%` atunci când se generează o listă de excluderi în consola Kaspersky Security Center. Pentru a aplica intrarea tuturor conturilor de utilizatori, puteți utiliza caracterul * (de exemplu, `C:\Users\*\Documents\File.exe`). Ori de câte ori adăugați o variabilă de mediu, trebuie să reporniți aplicația.

- Introduceți numele tipului obiectului conform clasificării din Enciclopedia Kaspersky (de exemplu, `Email-Worm`, `Rootkit` sau `RemoteAdmin`). Puteți folosi măști cu caracterul `?` (înlocuiește orice caracter unic) și caracterul `*` (înlocuiește orice număr de caractere). De exemplu, dacă este specificată masca `Client*`, aplicația exclude obiectele `Client-IRC`, `Client-P2P` și `Client-SMTP` de la scanări.

> Kaspersky Endpoint Security ascunde lista excluderilor de la scanare în interfața de utilizator a aplicației dacă configurarea excluderilor de la scanare este blocată de administrator în consolă (simbolul „lacăt închis") și excluderile de la scanare locale sunt interzise (caseta de selectare **Permite utilizarea excluderilor locale** este debifată).

Aplicații de încredere

Acest tabel listează aplicațiile de încredere a căror activitate nu este monitorizată de Kaspersky Endpoint Security în cursul funcționării sale.

Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști.

> Kaspersky Endpoint Security nu acceptă variabila de mediu `%userprofile%` atunci când se generează o listă de aplicații de încredere în consola Kaspersky Security Center. Pentru a aplica intrarea tuturor conturilor de utilizatori, puteți utiliza caracterul * (de exemplu, `C:\Users\*\Documents\File.exe`). Ori de câte ori adăugați o variabilă de mediu, trebuie să reporniți aplicația.

Componenta Application Control monitorizează pornirea fiecărei aplicații, indiferent dacă aplicația este inclusă sau nu în tabelul de aplicații de încredere.

> Kaspersky Endpoint Security ascunde lista consolidată a aplicațiilor de încredere în interfața de utilizator a aplicației dacă configurarea aplicațiilor de încredere este blocată de administrator în consolă (simbolul „lacăt închis") și aplicațiile locale de încredere sunt interzise (caseta de selectare **Permite utilizarea aplicațiilor de încredere locale** este debifată).

Îmbină valorile în momentul moștenirii

(disponibil numai în consola Kaspersky Security Center)

Aceasta combină lista excluderilor de la scanare și a aplicațiilor de încredere în politicile părinte și copil din Kaspersky Security Center. Pentru a îmbina listele, politica copil trebuie să fie configurată pentru a moșteni setările politicii părinte a Kaspersky Security Center.

Dacă este bifată caseta de selectare, elementele de listă din politica părinte Kaspersky Security Center sunt afișate în politicile copil. În acest fel, puteți crea, de exemplu, o listă consolidată de aplicații de încredere pentru întreaga organizație.

Elementele de listă moștenite dintr-o politică copil nu pot fi șterse sau editate. Elementele de pe lista de excluderi de la scanare și lista de aplicații de încredere care sunt îmbinate în timpul moștenirii pot fi șterse și editate numai în politica părinte. Puteți adăuga, edita sau șterge elemente de listă în politicile de nivel inferior.

Dacă elementele din listele politicii copil și părinte se potrivesc, aceste elemente sunt afișate ca același element al politicii părinte.

Dacă nu este bifată caseta de selectare, elementele listei nu sunt îmbinate la moștenirea setărilor politicilor Kaspersky Security Center.

Această funcționalitate permite, de asemenea, îmbinarea listelor în profilurile de politici. Pentru a îmbina liste, în profilul cu cea mai mare prioritate, activează moștenirea setărilor dintr-un profil cu prioritate mai mică. Pentru mai multe detalii despre prioritățile profilului politicii, vezi secțiunea Ajutor pentru Kaspersky Security Center.

Permite utilizarea excluderilor locale / Permite utilizarea aplicațiilor de încredere locale *(disponibil numai în consola Kaspersky Security Center)*	*Excluderi locale și aplicații locale de încredere (zonă de încredere locală)* – listă definită de utilizator a obiectelor și aplicațiilor din Kaspersky Endpoint Security pentru un anumit computer. Kaspersky Endpoint Security nu monitorizează obiectele și aplicațiile din zona de încredere locală. În acest fel, utilizatorii își pot crea propriile liste locale de excluderi și aplicații de încredere, pe lângă zona generală de încredere dintr-o politică. Dacă este bifată caseta de selectare, un utilizator poate crea o listă locală de excluderi de la scanare și o listă locală de aplicații de încredere. Un administrator poate utiliza Kaspersky Security Center pentru a vizualiza, adăuga, edita sau șterge elemente de listă din proprietățile computerului. Dacă este debifată caseta de selectare, un utilizator poate accesa numai listele generale de excluderi de la scanare și de aplicații de încredere generate în politică.
Telemetrie EDR (KATA) / NDR (KATA) *(disponibil numai în consola Kaspersky Security Center)*	Acest tabel conține informații despre excluderile de telemetrie EDR.
Telemetrie KUMA *(disponibil numai în consola Kaspersky Security Center)*	Lista evenimentelor care urmează să fie trimise către Kaspersky Unified Monitoring and Analysis Platform (KUMA). Kaspersky Endpoint Security funcționează în următoarele moduri: • **Trimite toate evenimentele**. În acest mod, aplicația trimite toate evenimentele din jurnalul Windows, cu excepția evenimentelor adăugate la regulile de excludere. • **Trimite numai evenimentele selectate**. În acest mod, aplicația trimite numai evenimentele adăugate în regulile de includere.
Depozit certificate de sistem de încredere	Dacă este selectat unul dintre depozitele de certificate de sistem de încredere, Kaspersky Endpoint Security exclude de la scanare aplicațiile semnate cu o semnătură digitală de încredere. Kaspersky Endpoint Security atribuie automat astfel de aplicații grupului **De încredere**. Dacă este selectat **Nu se utilizează**, Kaspersky Endpoint Security scanează aplicațiile indiferent dacă au sau nu o semnătură digitală. Kaspersky Endpoint Security plasează o aplicație într-un grup de încredere în funcție de nivelul de pericol pe care îl poate prezenta această aplicație pentru computer.

Setări aplicație

Poți configura următoarele setări generale ale aplicației:

- Mod de funcționare
- Autoprotecție
- Performanță
- Informații depanare
- Starea computerului când se aplică setările

Parametru	Descriere
Pornește aplicația la pornirea computerului (recomandat)	Atunci când este selectată această opțiune, Kaspersky Endpoint Security este pornit după încărcarea sistemului de operare, protejând computerul pe parcursul întregii sesiuni. Atunci când această opțiune este debifată, Kaspersky Endpoint Security nu se lansează după încărcarea sistemului de operare, până când utilizatorul îl pornește manual. Protecția computerului este dezactivată și datele utilizatorilor pot fi expuse unor amenințări.
Utilizează tehnologia Dezinfectare avansată (necesită resurse considerabile ale computerului)	De obicei, Kaspersky Endpoint Security oprește programele malware detectate înainte ca computerul să fie infectat. Tehnologia Dezinfectare avansată protejează computerul de programele malware deja active (infecții active), reducând astfel la minimum riscul de pierdere a datelor și de răspândire a amenințării. Dacă această tehnologie este activată, atunci când se detectează o activitate rău intenționată, Kaspersky Endpoint Security afișează o notificare pop-up. În această notificare, Kaspersky Endpoint Security oferă utilizatorului posibilitatea să efectueze o Dezinfectare avansată a computerului. După ce utilizatorul aprobă această procedură, Kaspersky Endpoint Security neutralizează amenințarea și apoi repornește computerul. Tehnologia de dezinfectare avansată folosește resurse de calcul considerabile, care port încetini alte aplicații. Când aplicația este în proces de detectare a unei infecții active, unele funcționalități ale sistemului de operare pot fi indisponibile. Disponibilitatea sistemului de operare este restabilită când Dezinfectarea avansată este finalizată și computerul este repornit. Dacă Kaspersky Endpoint Security este instalat pe un computer care rulează Windows Server, Kaspersky Endpoint Security nu va afișa notificarea. Prin urmare, nu poți selecta o acțiune pentru a dezinfecta o amenințare activă. Pentru a neutraliza o amenințare, este necesar să activați tehnologia Dezinfectare avansată în setările aplicației și să activați imediat Dezinfectarea avansată din proprietățile activității *Scanare malware*. Apoi, este necesar să porniți activitatea *Scanare malware*.
Utilizează Kaspersky Security Center ca server proxy pentru activare *(disponibil numai în consola Kaspersky Security Center)*	Dacă această casetă de selectare este bifată, aplicația folosește serverul de administrare Kaspersky Security Center ca server proxy pentru conectarea la serverele de activare. Acest lucru este necesar atunci când utilizezi un cod de activare pentru a activa aplicația într-un segment de rețea izolat, fără acces la internet. Dacă activezi aplicația cu a fișier cheie, accesul la internet nu este necesar.
Activează Autoprotecție	Când această funcționalitate este activată, Kaspersky Endpoint Security previne alterarea sau ștergerea fișierelor aplicației de pe unitatea de hard disk, a proceselor de memorie și a înregistrărilor din registry-ul de sistem.
Blochează gestionarea externă a serviciilor aplicației	Dacă această funcționalitate este activată, Kaspersky Endpoint Security nu permite gestionarea serviciilor aplicației folosind aplicații terțe (cum ar fi CMD). Atunci când apare o încercare de a gestiona serviciile aplicației utilizând aplicații terțe, în bara de activități Microsoft Windows apare o notificare, deasupra pictogramei aplicației (cu excepția cazului în care serviciul de notificare a fost dezactivat de către utilizator). Poți permite gestionarea externă a serviciilor aplicației numai pe computere care nu acceptă tehnologia AM-PPL sau pe computere care au tehnologia dezactivată.
Amână activități planificate în timpul funcționării cu alimentare de la baterie	Dacă această casetă de selectare este bifată, modul de economisire a energiei este activat atunci când computerul funcționează pe baterie. Kaspersky Endpoint Security amână activitățile planificate. Dacă este necesar, poți porni manual activitățile de scanare și de actualizare. Atunci când modul de economisire a energiei este activat și computerul funcționează cu alimentare de la baterie, următoarele activități nu sunt executate, chiar dacă sunt planificate: • *Scanare completă* • *Scanare zone critice* • *Scanare personalizată* • *Verificare integritate aplicație* • *Scanare IOC* • *Actualizarea modulelor bazelor de date și ale aplicațiilor* (doar corecțiile) Aplicația omite actualizările planificate ale bazei de date doar atunci când laptopul funcționează pe baterie și nivelul bateriei este sub 30%. În toate celelalte cazuri, Kaspersky Endpoint Security actualizează bazele de date conform planificării, indiferent dacă laptopul este conectat la priză sau funcționează pe baterie sau dacă aplicația este în modul Economisire energie.

Parametru	Descriere
Cedează resurse pentru alte aplicații	Consumul de resurse ale computerului de către Kaspersky Endpoint Security atunci când scanează un computer poate crește gradul de încărcare a subsistemelor CPU și ale unității de hard disk. Acest lucru poate încetini alte aplicații. Pentru a optimiza performanța, Kaspersky Endpoint Security oferă un *mod de transfer al resurselor către alte aplicații*. În acest mod, sistemul de operare poate scădea prioritatea firelor de execuție a activităților de scanare ale Kaspersky Endpoint Security atunci când încărcarea CPU este mare. Acest lucru permite redistribuirea resurselor sistemului de operare către alte aplicații. Astfel, activitățile de scanare vor beneficia de mai puțin timp de procesare. Ca urmare, Kaspersky Endpoint Security va avea nevoie de mai mult timp pentru a scana computerul. În mod implicit, aplicația este configurată să cedeze resurse pentru alte aplicații.
Limitează utilizarea CPU pentru activitățile de scanare	Pentru a optimiza performanța Kaspersky Endpoint Security, poți limita utilizarea procesorului cu ajutorul activității *Scanare malware*. Dacă este bifată caseta de selectare, sarcina medie pe toate nucleele procesorului de la activitatea *Scanare malware* nu trebuie se apropie valoarea specificată. În mod implicit, caseta de selectare este debifată.
Activează scrierea imaginii memoriei	Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security scrie imagini atunci când se blochează. În cazul în care caseta de selectare este nebifată, Kaspersky Endpoint Security nu scrie imagini. În plus, aplicația șterge fișierele imagine existente de pe unitatea de hard disk a computerului.
Activează protecția fișierelor imagine memorie și de urmărire	Dacă această casetă de selectare este bifată, accesul la fișierele imagine este permis administratorului de sistem și celui local, precum și utilizatorului care a activat scrierea fișierelor imagine. Doar administratorii de sistem și cei locali pot accesa fișierele de urmărire. Dacă această casetă de selectare este debifată, orice utilizator poate accesa fișierele de imagine memorie și de urmărire.
Starea computerului când se aplică setările *(disponibil numai în consola Kaspersky Security Center)*	Setări pentru afișarea stărilor computerelor client cu aplicația Kaspersky Endpoint Security instalată în Consola Web atunci când apar erori la aplicarea unei politici sau executarea unei activități. Sunt disponibile următoarele stări: *OK*, *Avertisment* și *Critică*.
Instalează actualizările fără să repornești computerul	Efectuarea upgrade-ului aplicației fără repornirea computerului îți permite să asiguri funcționarea neîntreruptă a serverelor. Poți efectua upgrade-ul aplicației fără repornire începând cu versiunea 11.10.0. Pentru a efectua upgrade-ul unei versiuni anterioare a aplicației, trebuie să repornești computerul. Începând cu versiunea 11.11.0 puteți efectua următoarele acțiuni fără să reporniți computerul: • instalarea corecțiilor • modificarea setului de componente al aplicației • instalarea Kaspersky Endpoint Security peste Kaspersky Security for Windows Server Valoarea implicită a parametrului variază în funcție de tipul sistemului de operare. Dacă aplicația este instalată pe o stație de lucru, efectuarea upgrade-ului aplicației fără opțiunea de repornire este dezactivată. Dacă aplicația este instalată pe un server, efectuarea upgrade-ului aplicației fără opțiunea de repornire este activată.
Compatibilitate cu software-ul de administrare la distanță *(disponibil numai în consola Kaspersky Security Center)*	Dacă folosirea Kaspersky Endpoint Security împreună cu Instrumentele de administrare la distanță (RAT) cauzează probleme, puteți activa modul compatibilitate. Problemele pot fi legate de incompatibilitatea RAT-urilor cu funcționalitatea Secure Desktop a aplicației. Scopul acestei funcționalități este de a confirma acțiunile care pot reduce nivelul de securitate al computerului. Această funcționalitate permite unei aplicații să afișeze o casetă de dialog de confirmare care este izolată de alte procese. Această funcționalitate folosește drepturi avansate pentru a securiza solicitarea. În acest fel, doar utilizatorul poate confirma acțiunea și nu malware-ul. Dacă această opțiune este selectată, modul Compatibilitate RAT este activat. Aplicația afișează o casetă de dialog de confirmare fără această funcționalitate. Acest lucru poate reduce nivelul de securitate al computerului. Nu vă recomandăm să activați modul compatibilitate dacă Kaspersky Endpoint Security nu cauzează probleme cu RAT. Dacă această opțiune este deselectată, modul Compatibilitate RAT este dezactivat. În mod implicit, caseta de selectare este debifată. Exemplu: Când utilizați browserul în modul RemoteApp, este posibil ca Kaspersky Endpoint Security să nu afișeze o fereastră de confirmare când accesați un site web cu un certificat care nu este de încredere deoarece RemoteApp nu acceptă funcționalitatea Secure Desktop a aplicației. Acest lucru poate face ca browserul să nu mai răspundă. Pentru ca browserul să funcționeze corect în modul RemoteApp, trebuie să activați modul compatibilitate. De asemenea, puteți încerca să activați modul compatibilitate dacă întâmpinați probleme cu funcționalitatea Secure Desktop atunci când utilizați alt software terț.

Rapoarte și spații de stocare

Rapoarte

Informațiile despre funcționarea fiecărei componente Kaspersky Endpoint Security, evenimentele de criptare de date, performanțele fiecărei activități de scanare, de actualizare și de verificare a integrității, precum și funcționarea generală a aplicației sunt înregistrate în rapoarte.

Rapoartele sunt stocate în directorul `C:\ProgramData\Kaspersky Lab\KES.14.1\Report`.

Copie de rezervă

Opțiunea *Copiere de rezervă* stochează copii de rezervă ale fișierelor care au fost șterse sau modificate în timpul dezinfectării. O *copie de rezervă* este copia unui fișier creată înainte ca fișierul să fie dezinfectat sau șters. Copiile de rezervă ale fișierelor sunt stocate într-un format special și nu reprezintă o amenințare.

Copiile de rezervă ale fișierelor sunt stocate în directorul `C:\ProgramData\Kaspersky Lab\KES.14.1\QB`.

Utilizatorii din grupul Administratori au permisiuni complete de a accesa acest director. Utilizatorul al cărui cont a fost utilizat pentru a instala Kaspersky Endpoint Security primește drepturi de acces limitate la acest director.

Kaspersky Endpoint Security nu permite configurarea permisiunilor de acces al utilizatorului la copiile de rezervă ale fișierelor.

Carantină

Carantină este un spațiu de stocare locală special de pe computer. Utilizatorul poate pune în carantină fișierele pe care le consideră periculoase pentru computer. Fișierele introduse în carantină sunt stocate într-o stare criptată și nu amenință securitatea dispozitivului. Kaspersky Endpoint Security utilizează Carantina numai atunci când este integrată cu soluțiile Kaspersky Detection and Response. În alte cazuri, Kaspersky Endpoint Security plasează fișierul relevant în Copie de rezervă. Pentru detalii privind gestionarea funcției Carantină ca parte a soluțiilor, consultă Kaspersky Sandbox Help, Kaspersky Endpoint Detection and Response Optimum Help, Kaspersky Endpoint Detection and Response Expert Help, Kaspersky Anti Targeted Attack Platform Help, and Kaspersky Endpoint Detection and Response Expert (on-premises) Help.

Carantina poate fi configurată numai utilizând funcția Web Console. De asemenea, puteți utiliza Web Console pentru a gestiona obiecte aflate în carantină (restaurare, ștergere, adăugare etc.). Puteți restaura obiectele local pe computer folosind linia de comandă.

Kaspersky Endpoint Security utilizează contul de sistem (SYSTEM) pentru a pune în carantină fișierele.

Parametru	Descriere
Delete reports after (days)	În cazul în care caseta de selectare este bifată, termenul maxim de stocare a raportului este limitat la intervalul de timp definit. Durata maximă implicită de stocare pentru rapoarte este de 30 de zile. După această perioadă de timp, Kaspersky Endpoint Security șterge automat înregistrările cele mai vechi din fișierul de raport.
Limit the size of report file to (MB)	În cazul în care caseta de selectare este bifată, dimensiunea maximă a raportului este limitată la valoarea definită. În mod implicit, dimensiunea maximă a fișierului este de 1.024 MO. Pentru a evita depășirea dimensiunii maxime a fișierului raport, Kaspersky Endpoint Security șterge automat înregistrările cele mai vechi din fișierul de raport atunci când este atinsă dimensiunea maximă a acestuia.
Delete objects after (days)	În cazul în care caseta de selectare este bifată, termenul maxim de stocare a fișierului este limitat la intervalul de timp definit. Durata maximă implicită de stocare pentru fișiere este de 30 de zile. După expirarea duratei maxime de stocare, Kaspersky Endpoint Security șterge fișierele cele mai vechi din Copie de rezervă.
Limit the size of Backup to (MB)	În cazul în care caseta de selectare este bifată, dimensiunea maximă de stocare este limitată la valoarea definită. În mod implicit, dimensiunea maximă este de 1024 MO. Pentru a evita depășirea dimensiunii maxime a de stocare, Kaspersky Endpoint Security șterge automat fișierele cele mai vechi din stocare atunci când este atinsă dimensiunea maximă de stocare.
Limit the size of Quarantine	În cazul în care caseta de selectare este bifată, dimensiunea maximă a directorului Carantină este limitată la valoarea definită. În mod implicit, dimensiunea maximă este de 1024 MO. Când directorul Carantină atinge dimensiunea maximă, Kaspersky Endpoint Security trimite evenimentul *Spațiu insuficient în spațiul de stocare Carantină* către Kaspersky Security Center și publică evenimentul în Jurnalul de evenimente Windows. Între timp, aplicația nu mai pune în carantină obiecte noi. Trebuie să goliți directorul Carantină manual.
Notify when the Quarantine storage reaches (%)	Valoarea pragului pentru Carantină. De exemplu, puteți seta pragul pentru Carantină la 50%. Când directorul Carantină atinge pragul, Kaspersky Endpoint Security trimite evenimentul corespunzător către Kaspersky Security Center și publică evenimentul în Jurnalul de evenimente Windows. Între timp, aplicația continuă să pună în carantină obiecte noi.
Transfer de date pe serverul de administrare *(disponibil numai în Kaspersky Security Center)*	Categoriile de evenimente de pe computerele client ale căror informații trebuie transmise către Serverul de administrare. Poți dezactiva transferul anumitor date pentru a optimiza spațiul pe disc pe Serverul de administrare. Aplicația trimite evenimente din următoarele categorii: • **About Quarantine files**. Poți vizualiza lista fișierelor carantinate din consola Kaspersky Security Center în directorul **Advanced** → **Repositories** → **Quarantine**. Kaspersky Endpoint Security utilizează Carantina numai atunci când este integrată cu soluțiile Kaspersky Detection and Response. • **About files in Backup**. Poți vizualiza lista fișierelor din consola Kaspersky Security Center în directorul **Advanced** → **Repositories** → **Backup**. • **About unprocessed files**. Poți vizualiza lista fișierelor neprocesate în consola Kaspersky Security Center în directorul **Advanced** → **Repositories** → **Active threats**. • **About installed devices**. Poți vizualiza lista dispozitivelor conectate din consola Kaspersky Security Center în directorul **Advanced** → **Repositories** → **Hardware**. Lista de dispozitive este disponibilă și în proprietățile computerului și în politica Kaspersky Endpoint Security for Windows (secțiunea **Control dispozitive**). • **About started applications**. Poți vizualiza lista fișierelor executabile din consola Kaspersky Security Center în directorul **Advanced** → **Application management** → **Executable files**. Lista fișierelor executabile este disponibilă și în proprietățile computerului. • **About file encryption errors**. Poți vizualiza lista erorilor de criptare a fișierelor din consola Kaspersky Security Center în directorul **Advanced** → **Data encryption and protection** → **Encryption events**. Lista de erori este disponibilă și în proprietățile computerului. • **Report on Adaptive Anomaly Control rules state**. Poți vizualizați raportul din consola Kaspersky Security Center în nodul **Administration Server** din fila **Reports**. Acest raport este disponibil și în proprietățile politicii Kaspersky Endpoint Security for Windows (secțiunea **Control adaptiv al anomaliilor**). • **Report on triggered Adaptive Anomaly Control rules**. Poți vizualizați raportul din consola Kaspersky Security Center în nodul **Administration Server** din fila **Reports**. Acest raport este disponibil și în proprietățile politicii Kaspersky Endpoint Security for Windows (secțiunea **Control adaptiv al anomaliilor**). • **About a threat development chain**. Poți vizualiza detaliile detecției din Kaspersky Security Center Web Console în secțiunea **Monitoring** → **Alerts**. Informațiile despre lanțul de dezvoltare a amenințărilor sunt utilizate de soluțiile Kaspersky Endpoint Detection and Response.

Setări de rețea

Poți să configurezi serverul proxy utilizat pentru conectarea la Internet și actualizarea bazelor de date antivirus, să selectezi modul de monitorizare a portului de rețea și să configurezi o scanare a conexiunilor criptate.

Parametru	Descriere
Limitează traficul pentru conexiunile contorizate	Dacă ați bifat această casetă de selectare, aplicația își limitează propriul trafic de rețea dacă se limitează conexiunea la internet. Kaspersky Endpoint Security identifică o conexiune la internet de mare viteză pentru telefonie mobilă ca fiind o conexiune limitată și identifică o conexiune Wi-Fi ca fiind o conexiune nelimitată. Funcția Comunicații în rețea sensibile la costuri funcționează pe computere care rulează Windows 8 sau o versiune ulterioară.
Injectează segmente de script în traficul web pentru a interacționa cu paginile web	Dacă această casetă este selectată, Kaspersky Endpoint Security va injecta în traficul web un script de interacțiune cu paginile web. Acest script asigură faptul că componenta Control Web poate funcționa corect. Scriptul permite înregistrarea evenimentelor Control Web. Fără acest script, nu puteți activa monitorizarea activității pe Internet a utilizatorului. Experții Kaspersky recomandă injectarea acestui script de interacțiune a paginii web în trafic pentru a asigura funcționarea corectă a Control Web.
Setări server proxy	Setările serverului proxy utilizat pentru accesul la Internet al utilizatorilor de computere client. Kaspersky Endpoint Security utilizează aceste setări pentru anumite componente de protecție, inclusiv pentru actualizarea bazelor de date și modulelor de aplicații. Pentru configurarea automată a unui server proxy, Kaspersky Endpoint Security utilizează protocolul WPAD (Proxy Auto-Discovery Protocol). Dacă adresa IP a serverului proxy nu poate fi determinată cu ajutorul acestui protocol, aplicația utilizează adresa serverului proxy specificată în setările browserului Microsoft Internet Explorer.
Ocolește serverul proxy pentru adrese locale	Dacă este bifată caseta de selectare, Kaspersky Endpoint Security nu utilizează un server proxy la efectuarea unei actualizări dintr-un director partajat.
Setări autentificare server proxy	Pentru a autentifica aplicația pe serverul proxy pentru acces la internet, trebuie să introduci acreditările utilizatorului. Kaspersky Endpoint Security acceptă autentificarea automată pe serverul proxy. Dacă autentificarea automată a eșuat, aplicația îți solicită să introduci acreditările. **Nu utiliza autentificarea**. **Autentificare NTLM**. Autentificare NTLM folosind contul de utilizator curent (implicit). **Autentificare NTLM cu nume de utilizator și parolă**. Autentificare NTLM folosind acreditări specificate manual. **Numele de utilizator și parola**. Autentificare cu acreditări specificate manual. **Autentificare automată**. **Autentificare Kerberos**. Autentificare Kerberos folosind contul de utilizator curent. Pentru a vă asigura că autentificarea Kerberos funcționează corect atunci când utilizați înregistrări CNAME pentru adresa serverului proxy, trebuie să înregistrați un nume principal de serviciu (SPN) pentru fiecare înregistrare CNAME. **Autentificare Kerberos cu nume de utilizator și parolă**. Autentificare Kerberos folosind acreditări specificate manual. Dacă este selectată autentificarea Kerberos, Kaspersky Endpoint Security poate, în funcție de setările serverului proxy, să efectueze autentificarea utilizând protocolul Kerberos sau NTLM.
Porturi monitorizate	**Monitorizează toate porturile de rețea**. În acest mod de monitorizare a porturilor de rețea, componentele de protecție (File Threat Protection, Web Threat Protection și Mail Threat Protection) monitorizează fluxurile de date transmise prin orice porturi de rețea deschise ale computerului. **Monitorizează numai porturile de rețea selectate**. Iîn acest mod de monitorizare a portului de rețea, componentele de protecție monitorizează porturile selectate ale computerului și activitatea în rețea a aplicațiilor selectate. Lista porturilor de rețea folosite în mod normal pentru transmiterea e-mailurilor și a traficului de rețea este configurată în conformitate cu recomandările experților Kaspersky. **Monitorizează toate porturile pentru aplicațiile din lista recomandată de Kaspersky**. În acest caz este utilizată o listă predefinită de aplicații ale căror porturi de rețea sunt monitorizate de Kaspersky Endpoint Security. De exemplu, printre acestea se numără Google Chrome, Adobe Reader, Java și alte aplicații. **Monitorizează toate porturile pentru aplicațiile specificate**. În acest caz este utilizată o listă de aplicații ale căror porturi de rețea sunt monitorizate de Kaspersky Endpoint Security.

Parametru	Descriere
Scanare conexiuni criptate	Kaspersky Endpoint Security scanează traficul de rețea criptat transmis prin următoarele protocoale: • SSL 3.0. • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. Kaspersky Endpoint Security acceptă următoarele moduri de scanare a conexiunilor criptate: • **Nu scana conexiunile criptate**. Kaspersky Endpoint Security nu va avea acces la conținutul site-urilor web ale căror adrese încep cu `https://`. • **Scanează conexiunile criptate la cererea componentelor de protecție**. Kaspersky Endpoint Security va scana traficul criptat numai la solicitarea componentelor Web Threat Protection, Mail Threat Protection și Control Web. • **Scanează întotdeauna conexiunile criptate**. Kaspersky Endpoint Security va scana traficul de rețea criptat chiar dacă componentele de protecție sunt dezactivate. Kaspersky Endpoint Security nu scanează conexiunile criptate care au fost stabilite de aplicații de încredere pentru care scanarea traficului este dezactivată. Kaspersky Endpoint Security nu scanează conexiunile criptate din lista predefinită de site-uri web de încredere. Lista predefinită de site-uri web de încredere este creată de experții Kaspersky. Această listă este actualizată cu bazele de date antivirus ale aplicației. Puteți vizualiza lista predefinită de site-uri web de încredere numai în interfața Kaspersky Endpoint Security. Nu puteți vizualiza lista în consola Kaspersky Security Center.
Certificate rădăcină de încredere	Lista cu certificatele rădăcină de încredere. Kaspersky Endpoint Security vă permite să instalați certificate rădăcină de încredere pe computerele utilizatorilor dacă, de exemplu, trebuie să implementați un nou centru de certificare. Aplicația vă permite să adăugați un certificat într-un magazin special de certificate Kaspersky Endpoint Security. În acest caz, certificatul este considerat de încredere numai pentru aplicația Kaspersky Endpoint Security. Cu alte cuvinte, utilizatorul poate obține acces la un site web cu certificatul nou în browser. Dacă aplicația încearcă să obțină acces la site-ul web, poate să apară o eroare de conexiune din cauza unei probleme delate de certificat. Pentru a adăuga la magazinul de certificate de sistem, puteți utiliza politicile de grup Director activ.
Vizitarea unui domeniu cu un certificat care nu este de încredere	• **Permite**. La vizitarea unui domeniu cu un certificat care nu este de încredere, Kaspersky Endpoint Security permite conectarea la rețea. Atunci când se deschide un domeniu cu un certificat neautorizat într-un browser, Kaspersky Endpoint Security afișează o pagină HTML cu un avertisment prin care nu se recomandă vizitarea domeniului respectiv. Un utilizator poate face clic pe linkul din pagina de avertizare HTML pentru a obține accesul la resursa web solicitată. Dacă o aplicație terță sau un serviciu terț stabilește o conexiune cu un domeniu cu un certificat care nu este de încredere, Kaspersky Endpoint Security își creează propriul certificat pentru a scana traficul. Noul certificat are starea *Nu este de încredere*. Acest lucru este necesar pentru a avertiza aplicația terță despre conexiunea care nu este de încredere, deoarece pagina HTML nu poate fi afișată în acest caz și conexiunea poate fi stabilită în modul în fundal. • **Blochează**. La vizitarea unui domeniu cu un certificat care nu este de încredere, Kaspersky Endpoint Security blochează conexiunea la rețea. Atunci când se deschide un domeniu cu un certificat neautorizat într-un browser, Kaspersky Endpoint Security afișează o pagină HTML cu informații privind motivul pentru care domeniul respectiv este blocat.
Vizitarea unui domeniu cu o eroare de scanare a conexiunilor criptate	• **Blochează**. Dacă apare o eroare la scanarea conexiunii criptate, Kaspersky Endpoint Security blochează conexiunea la rețea. • **Permite și adaugă domeniul la excluderi**. Dacă apare o eroare la scanarea conexiunii criptate, Kaspersky Endpoint Security adaugă domeniul care a generat eroarea în lista domeniilor cu erori la scanare și nu monitorizează traficul de rețea criptat atunci când acest domeniu este vizitat. Puteți vizualiza o listă de domenii cu erori de scanare a conexiunilor sigure numai în interfața locală a aplicației. Pentru a șterge conținutul listei, trebuie să selectați **Blochează**. Kaspersky Endpoint Security generează, de asemenea, un eveniment pentru eroarea de scanare a conexiunii criptate.
Blochează conexiunile SSL 2.0	Dacă această casetă de selectare este bifată, aplicația monitorizează și blochează conexiunile la rețea stabilite prin protocolul SSL 2.0. Dacă caseta de selectare este debifată, aplicația nu blochează conexiunile de rețea stabilite prin protocolul SSL 2.0. Cu toate acestea, aplicația nu monitorizează traficul de rețea prin acest protocol.
Blochează conexiunile SSL 3.0	Dacă această casetă de selectare este bifată, aplicația blochează conexiunile la rețea stabilite prin protocolul SSL 3.0. Dacă caseta de selectare este debifată, aplicația nu blochează conexiunile de rețea stabilite prin protocolul SSL 3.0. Aplicația monitorizează traficul de rețea prin acest protocol. Toate componentele aplicației funcționează fără restricții.
Blochează conexiunile TLS 1.0	Dacă această casetă de selectare este bifată, aplicația blochează conexiunile la rețea stabilite prin protocolul TLS 1.0. Dacă caseta de selectare este debifată, aplicația nu blochează conexiunile de rețea stabilite prin protocolul TLS 1.0. Aplicația monitorizează traficul de rețea prin acest protocol. Toate componentele aplicației funcționează fără restricții.

Parametru	Descriere
Decriptează o conexiune criptată cu site-ul web care utilizează certificatul EV	Certificatele EV (Extended Validation Certificate) confirmă autenticitatea site-urilor web și îmbunătățesc securitatea conexiunii. Browserele folosesc o pictogramă cu un lacăt în bara de adrese pentru a indica faptul că un site web are un certificat EV. De asemenea, browserele pot colora complet sau parțial bara de adrese în verde. În cazul în care caseta de selectare este bifată, aplicația decriptează și monitorizează conexiunile criptate cu site-uri web care utilizează un certificat EV. În cazul în care caseta de selectare este debifată, aplicația nu are acces la conținutul traficului HTTPS. Din acest motiv, aplicația monitorizează traficul HTTPS doar pe baza adresei site-ului web, de exemplu, `https://bing.com`. Dacă deschideți pentru prima dată un site web cu certificat EV, conexiunea criptată va fi decriptată indiferent dacă este bifată sau nu caseta de selectare.
Configurează adresele de încredere	În acest caz este utilizată o listă de adrese web pentru care Kaspersky Endpoint Security nu scanează conexiunile la rețea. În acest caz, Kaspersky Endpoint Security nu scanează traficul HTTPS al adreselor web de încredere atunci când componentele Web Threat Protection, Mail Threat Protection și Control Web își fac treaba. Puteți introduce numele unui domeniu sau o adresă IP. Kaspersky Endpoint Security acceptă caracterul `*` pentru introducerea unei măști în numele domeniului. Kaspersky Endpoint Security nu acceptă simbolul `*` pentru adresele IP. Puteți selecta un interval de adrese IP folosind o mască de subrețea (de exemplu, 198.51.100.0/24). Exemple: • `domain.com` – dosarul include următoarele adrese: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Înregistrarea este exclusiv pentru subdomenii (de exemplu, `subdomain.domain.com`). • `subdomain.domain.com` – dosarul include următoarele adrese: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Înregistrarea este exclusiv pentru domeniul `domain.com`. • `*.domain.com` – dosarul include următoarele adrese: `https://movies.domain.com`, `https://images.domain.com/page123`. Înregistrarea este exclusiv pentru domeniul `domain.com`.
Configurează aplicațiile de încredere	Lista de aplicații de încredere a căror activitate nu este monitorizată de Kaspersky Endpoint Security în cursul funcționării sale. Puteți selecta tipurile activității aplicației pe care Kaspersky Endpoint Security nu le va monitoriza (de exemplu, nu scanați traficul de rețea). Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști.
Pentru a scana conexiunile criptate în aplicații cu propriul depozit de certificate, folosește *(disponibil numai în interfața Kaspersky Endpoint Security)*	Dacă această casetă de selectare este bifată, aplicația scanează traficul criptat din browserul Mozilla Firefox și clientul de e-mail Thunderbird. Poate fi blocat accesul la unele site-uri web prin protocolul HTTPS. Pentru a scana traficul în browserul Mozilla Firefox și în clientul de e-mail Thunderbird, trebuie să activați opțiunea Scanare conexiune criptată. Dacă Scanare conexiune criptată este dezactivată, aplicația nu scanează traficul din browserul Mozilla Firefox și clientul de e-mail Thunderbird. Aplicația folosește certificatul rădăcină Kaspersky pentru a decripta și analiza traficul criptat. Puteți selecta depozitul de certificate care va conține certificatul rădăcină Kaspersky. • **Depozitul de certificate Windows (recomandat)**. Certificatul rădăcină Kaspersky este adăugat la acest depozit în timpul instalării Kaspersky Endpoint Security. • **Depozitul de certificate propriu**. Mozilla Firefox și Thunderbird folosesc propriile depozite de certificate. Dacă este selectat depozitul de certificate Mozilla, trebuie să adăugați manual certificatul rădăcină Kaspersky la acest depozit prin proprietățile browserului.

Interfață

Poți configura setările pentru interfața aplicației.

Parametru	Descriere
Interacțiune cu utilizatorul *(disponibil numai în consola Kaspersky Security Center)*	**Afișare interfață simplificată**. Pe un computer client, fereastra principală a aplicației este inaccesibilă și numai pictograma din zona de notificare Windows este disponibilă. În meniul contextual al pictogramei, utilizatorul poate efectua un număr limitat de operații cu Kaspersky Endpoint Security. Kaspersky Endpoint Security afișează, de asemenea, doar notificările care necesită acțiunea utilizatorului deasupra pictogramei aplicației. **Afișare interfață utilizator**. Pe un computer client, fereastra principală a Kaspersky Endpoint Security și pictograma din zona de notificare Windows sunt disponibile. În meniul contextual al pictogramei, utilizatorul poate efectua operații cu Kaspersky Endpoint Security. Kaspersky Endpoint Security afișează, de asemenea, notificări deasupra pictogramei aplicației. **Ascundeți secțiunea Monitorizare activitate aplicație**. Pe computerul client, în fereastra principală a Kaspersky Endpoint Security, butonul **Monitorizare activitate aplicație** nu este disponibil. *Monitorizare activitate aplicație* este un instrument destinat vizualizării în timp real a informațiilor despre activitatea aplicațiilor de pe computerul unui utilizator. **Nu afișați interfața cu utilizatorul**. Pe un computer client, nu sunt afișate semne de funcționare a Kaspersky Endpoint Security. Pictograma din zona de notificare Windows și notificările sunt disponibile.
Configurează notificările	Un tabel cu setările de notificare pentru evenimente cu diferite niveluri de importanță care pot apărea în timpul funcționării unei componente, a unei activități sau a întregii aplicații. Kaspersky Endpoint Security prezintă notificări despre evenimente pe ecran, le trimite prin e-mail sau le înregistrează în jurnal.
Configurează notificările prin e-mail	Setări ale serverului SMTP pentru livrarea notificărilor despre evenimentele înregistrate în timpul funcționării aplicației. În mod implicit, Kaspersky Endpoint Security utilizează setările notificărilor prin e-mail de la Kaspersky Security Center. Pentru mai multe detalii despre setările notificărilor prin e-mail, consultați Ajutor pentru Kaspersky Security Center. Dacă trebuie să configurați notificările individuale prin e-mail, puteți edita următoarele setări: • **Adresă expeditor**. Adresa de e-mail a expeditorului. Utilizarea unei adrese inexistente nu este recomandată. • **Server SMTP**. Una sau mai multe adrese ale serverelor de e-mail ale organizației dvs. (de exemplu, `mail.company.com`). Puteți introduce o adresă IP (IPv4 sau IPv6). Pentru a autentifica utilizatorul pe serverul SMTP, introduceți acreditările expeditorului în câmpurile corespunzătoare. Pentru a testa notificările prin e-mail, puteți trimite un mesaj de testare. • **Adresă destinatar**. Adresele de e-mail ale destinatarilor cărora aplicația le va trimite notificări. • **Mod trimitere**. Modul de trimitere a notificărilor prin e-mail. Kaspersky Endpoint Security poate trimite mesaje imediat când are loc un eveniment; alternativ, poate urma o planificare preconfigurată.
Afișează starea aplicației în zona de notificări	Categorii de evenimente ale aplicației care cauzează schimbarea pictogramei Kaspersky Endpoint Security în zona de notificări din bara de activități Microsoft Windows (sau) și determină apariția unei notificări pop-up.
Notificări privind starea bazei de date antivirus locală	Setările pentru notificări despre baze de date antivirus învechite și utilizate de către aplicație.
Protecție prin parolă	Dacă butonul de comutare este activat, Kaspersky Endpoint Security solicită utilizatorului o parolă atunci când acesta încearcă să efectueze o operațiune care se încadrează în domeniul funcției Protecție prin parolă. Domeniul funcției Protecție prin parolă include operațiunile interzise (cum ar fi dezactivarea componentelor de protecție) și conturile de utilizator cărora li se aplică domeniul funcției Protecție prin parolă. După activarea funcției Protecție prin parolă, Kaspersky Endpoint Security îți solicită să setezi o parolă pentru contul KLAdmin.
Asistență utilizator / Link către resurse web *(disponibil numai în consola Kaspersky Security Center)*	Lista de linkuri către resurse Web care conțin informații despre asistența tehnică pentru Kaspersky Endpoint Security. Linkurile adăugate se afișează în fereastra **Suport** a interfeței locale a aplicației Kaspersky Endpoint Security în locul linkurilor standard.
Asistență utilizator / Descriere *(disponibil numai în consola Kaspersky Security Center)*	Mesaj care este afișat în fereastra **Suport** a interfeței locale a Kaspersky Endpoint Security.

Gestionare setări

Puteți salva setările curente ale Kaspersky Endpoint Security într-un fișier și le puteți utiliza pentru a configura rapid aplicația pe un alt computer. De asemenea, puteți utiliza un fișier de configurare atunci când implementați aplicația prin Kaspersky Security Center cu un pachet de instalare. Puteți restabili setările implicite în orice moment.

Setările de gestionare a configurației aplicației sunt disponibile numai în interfața Kaspersky Endpoint Security.

Setări de gestionare a configurației aplicației

Setări	Descriere
Importă	Extrageți setările aplicației dintr-un fișier în format CFG și le aplicați.
Exportă	Salvați setările curente ale aplicației într-un fișier în format CFG.
Restaurează	Puteți restaura oricând setările aplicației recomandate de Kaspersky. Când setările sunt restabilite, nivelul de securitate **Recomandat** este setat pentru toate componentele de protecție.

Actualizarea bazelor de date și modulelor aplicației

Actualizarea bazelor de date și modulelor aplicației Kaspersky Endpoint Security asigură o protecție actualizată pe computer. Zilnic apar în întreaga lume viruși și alte tipuri de programe malware noi. Bazele de date Kaspersky Endpoint Security conțin informații despre amenințări și despre modurile de neutralizare a acestora. Pentru a detecta rapid amenințările, este esențial să actualizezi în mod regulat bazele de date și modulele aplicației.

Este posibil ca funcționalitatea Actualizări (inclusiv furnizarea de actualizări ale semnăturii antivirus și actualizări ale bazei de cod) să nu fie disponibile în software în SUA.

Actualizările regulate necesită o licență activă. Dacă nu există nicio licență curentă, vei avea posibilitatea să efectuezi doar o singură actualizare.

Computerul trebuie să fie conectat la Internet pentru a descărca cu succes pachetul de actualizare de pe serverele de actualizare Kaspersky. În mod implicit, setările de conectare la Internet sunt stabilite automat. Dacă utilizați un server proxy, trebuie să configurați setările serverului proxy.

Actualizările se descarcă prin protocolul HTTPS. Acestea pot fi descărcate, de asemenea, prin protocolul HTTP atunci când este imposibilă descărcarea actualizărilor prin protocolul HTTPS.

La efectuarea unei actualizări, pe computer sunt descărcate și instalate următoarele obiecte:

- Baze de date Kaspersky Endpoint Security. Protecția computerului este furnizată folosind baze de date care conțin semnături de viruși și alte amenințări și informații despre modalitățile pentru neutralizarea acestora. Componentele protecției utilizează aceste informații la căutarea de fișiere infectate pe computer și la neutralizarea acestora. Bazele de date sunt actualizate constant cu înregistrări de amenințări noi și metode pentru contracararea lor. Prin urmare, îți recomandăm să actualizezi bazele de date regulat.

  Pe lângă bazele de date Kaspersky Endpoint Security, sunt actualizate și driverele de rețea care le permit componentelor aplicației să intercepteze traficul de rețea.

- Modulele aplicației. Pe lângă bazele de date Kaspersky Endpoint Security, poți actualiza și modulele aplicației. Actualizarea modulelor aplicației remediază vulnerabilitățile din Kaspersky Endpoint Security, adaugă funcții noi și îmbunătățește funcțiile existente.

În timpul actualizării, modulele și bazele de date ale aplicației de pe computer sunt comparate cu versiunile lor actualizate din sursa de actualizare. Dacă bazele de date și modulele actuale ale aplicației diferă de versiunile lor actualizate, porțiunea lipsă care să regăsește în actualizări este instalată pe computer.

Dacă bazele de date sunt neactuale, este posibil ca dimensiunea pachetului de actualizare să fie mare (până la câteva zeci de MB), fapt care poate cauza sporirea traficului din Internet.

Informațiile despre starea curentă a bazelor de date Kaspersky Endpoint Security sunt afișate în fereastra principală a aplicației sau în sfatul pe ecran pe care îl vedeți când deplasați cursorul peste pictograma aplicației din zona de notificare.

Informațiile despre rezultatele actualizărilor și despre toate evenimentele care apar în timpul funcționării activității de actualizare sunt înregistrate în Raportul Kaspersky Endpoint Security.

Dacă aplicația funcționează în modul Light Agent, consideratii speciale sunt implicate în actualizarea bazelor de date și a modulelor aplicațiilor.

Modulul aplicației și setările de actualizare a bazei de date

Parametru	Descriere
Planificare actualizare baze de date	**Automat**. În acest mod, aplicația verifică sursa de actualizare pentru disponibilitatea pachetelor de actualizare noi cu o anumită frecvență. Frecvența verificării disponibilității pachetelor de actualizare noi crește în timpul epidemiilor de viruși și scade în absența acestora. După detectarea unui nou pachet de actualizări, Kaspersky Endpoint Security îl descarcă și instalează actualizările pe computer. **Manually**. Acest mod de executare a activității de actualizare vă permite să porniți manual activitatea de actualizare. **By schedule**. În acest mod de executare a activității de actualizare, Kaspersky Endpoint Security rulează activitatea de actualizare în conformitate cu programul specificat de dvs. Dacă este selectat acest mod de executare a activității de actualizare, puteți porni manual și activitatea de actualizare Kaspersky Endpoint Security.
Run missed tasks	Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security pornește activitatea omisă imediat ce acest lucru devine posibil. Activitatea poate fi omisă, de exemplu, dacă computerul a fost oprit la ora programată pentru începerea activității. Când aplicația are ocazia să execute activitățile omise, aceasta le execută aleatoriu într-un anumit interval de timp pentru a distribui încărcarea pe computer. Dacă această casetă de selectare este debifată, Kaspersky Endpoint Security nu execută activitățile omise. În schimb, aplicația execută următoarea activitate în conformitate cu planificarea curentă.

Parametru	Descriere
Surse actualizare	O *sursă de actualizare* este o resursă care conține actualizări pentru bazele de date și modulele aplicației Kaspersky Endpoint Security. Sursele de actualizare includ serverul Kaspersky Security Center, serverele de actualizare ale Kaspersky și directoare de rețea sau locale. În cazul în care serverele de actualizare Kaspersky nu sunt disponibile, Kaspersky Endpoint Security poate utiliza domenii alternative pentru a-și actualiza bazele de date și modulele software ale aplicației. Pentru informații detaliate, consultați Baza de cunoștințe pentru suport tehnic. Lista implicită de surse de actualizare include Kaspersky Security Center și servere de actualizare ale Kaspersky. Poți adăuga la listă alte surse de actualizare. Poţţ specifica drept surse de actualizare servere HTTP/FTP și directoare partajate. Kaspersky Endpoint Security nu acceptă actualizări de la servere HTTPS decât dacă sunt servere de actualizare ale Kaspersky. Dacă mai multe resurse sunt selectate drept surse de actualizare, Kaspersky Endpoint Security încearcă să se conecteze la ele pe rând, începând cu prima din listă și efectuează acțiunea de actualizare preluând pachetul de actualizare de la prima sursă disponibilă. În mod implicit, Kaspersky Endpoint Security utilizează serverul Kaspersky Security Center ca primă sursă de actualizare. Acest lucru ajută la conservarea traficului]n timpul actualizării. Dacă o politică nu este aplicată computerului, serverele Kaspersky sunt selectate ca primă sursă de actualizare în setările activității locale *Actualizarea modulelor bazelor de date și ale aplicațiilor*, deoarece este posibil ca aplicația să nu aibă acces la serverul Kaspersky Security Center. Dacă aplicația se execută în modul Light Agent, un director pe SVM este selectat ca sursă de actualizare.
Execută actualizările bazei de date ca	În mod implicit, activitatea de actualizare a aplicației Kaspersky Endpoint Security este pornită din partea utilizatorului al cărui cont l-ai utilizat pentru a face Log in la sistemul de operare. Totuși, aplicația Kaspersky Endpoint Security poate fi actualizată și dintr-o sursă de actualizare la care utilizatorul nu are acces din cauza lipsei drepturilor necesare (de exemplu, dintr-un director partajat care conține un pachet de actualizare) sau dintr-o sursă de actualizare pentru care autentificarea serverului proxy nu este configurată. În setările aplicației, poți specifica un utilizator care are astfel de drepturi și poți porni activitatea de actualizare a aplicației Kaspersky Endpoint Security din contul utilizatorului respectiv.
Descarcă actualizările modulelor aplicației	Descărcarea actualizărilor modulelor aplicației cu actualizări ale bazei de date a aplicației. Dacă este bifată caseta de selectare, Kaspersky Endpoint Security notifică utilizatorul despre actualizările disponibile ale modulului de aplicație și include actualizări ale modulului de aplicație în pachetul de actualizare în timp ce rulează activitatea de actualizare. Modul în care sunt aplicate actualizările modulelor aplicației este stabilit prin următoarele setări: • **Instalează actualizările critice și aprobate**. Dacă este selectată această opțiune, atunci când sunt disponibile actualizări ale modulelor aplicației, Kaspersky Endpoint Security instalează automat actualizările critice și orice altă actualizare a modulelor aplicației numai după ce instalarea lor este aprobată local prin interfața aplicației sau în Kaspersky Security Center. • **Instalează numai actualizările aprobate**. Dacă este selectată această opțiune, atunci când sunt disponibile actualizări ale modulelor aplicației, Kaspersky Endpoint Security le instalează numai după ce instalarea lor este aprobată local prin interfața aplicației sau în Kaspersky Security Center. Această opțiune este selectată în mod implicit. Dacă nu este bifată caseta de selectare, Kaspersky Endpoint Security nu notifică utilizatorul despre actualizările disponibile ale modulului de aplicație și nu include actualizări ale modulului de aplicație în pachetul de actualizare în timp ce rulează activitatea de actualizare. Dacă actualizările modulelor aplicației necesită revizuirea și acceptarea Acordului de licență pentru utilizatorul final, aplicația instalează actualizările numai după acceptarea termenilor Acordului de licență pentru utilizatorul final. Această casetă de selectare este bifată în mod implicit.
Copiază actualizările în director	Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security copiază pachetul de actualizare în directorul partajat specificat sub caseta de selectare. După aceea, alte computere din rețeaua LAN pot primi pachetul de actualizare din acest director partajat. Acest lucru reduce traficul de Internet, deoarece pachetul de actualizare este descărcat o singură dată. Următorul director este specificat în mod implicit: `C:\ProgramData\Kaspersky Lab\KES.14.1\Update distribution\`.

Parametru	Descriere
Server proxy pentru actualizări *(disponibil numai în interfața Kaspersky Endpoint Security)*	Setările serverului proxy pentru accesul la Internet al utilizatorilor computerelor client pentru a actualiza modulele aplicației și bazele de date. Pentru configurarea automată a unui server proxy, Kaspersky Endpoint Security utilizează protocolul WPAD (Web Proxy Auto-Discovery Protocol). Dacă adresa IP a serverului proxy nu poate fi determinată cu ajutorul acestui protocol, Kaspersky Endpoint Security utilizează adresa serverului proxy specificată în setările browserului Microsoft Internet Explorer.
Ocolește serverul proxy pentru adrese locale *(disponibil numai în interfața Kaspersky Endpoint Security)*	Dacă este bifată caseta de selectare, Kaspersky Endpoint Security nu utilizează un server proxy la efectuarea unei actualizări dintr-un director partajat.

Anexa 2. Grupurile de încredere pentru aplicații

Kaspersky Endpoint Security clasifică în grupuri de încredere toate aplicațiile lansate pe computer. Aplicațiile sunt clasificate în grupuri de încredere în funcție de nivelul de amenințare pe care aplicațiile îl au pentru sistemul de operare.

Grupurile de încredere sunt următoarele:

- **De încredere**. Acest grup include aplicații pentru care sunt îndeplinite una sau mai multe dintre condițiile următoare:
  - Aplicațiile sunt semnate digital de către distribuitori de încredere.
  - Aplicațiile sunt înregistrate în bazele de date de aplicații de încredere din Kaspersky Security Network.
  - Utilizatorul a plasat aplicația în grupul *De încredere*.

  Nicio operațiune nu este interzisă pentru aceste aplicații.
- **Restricționat la nivel inferior**. Acest grup include aplicații pentru care sunt îndeplinite condițiile următoare:
  - Aplicațiile nu sunt semnate digital de către distribuitori de încredere.
  - Aplicațiile nu sunt înregistrate în bazele de date de aplicații de încredere din Kaspersky Security Network.
  - Utilizatorul a plasat aplicația în grupul *Restricționat la nivel inferior*.

  Aceste aplicații fac obiectul unor restricții minime în privința accesului la resursele sistemului de operare.
- **Restricționat la nivel superior**. Acest grup include aplicații pentru care sunt îndeplinite condițiile următoare:
  - Aplicațiile nu sunt semnate digital de către distribuitori de încredere.
  - Aplicațiile nu sunt înregistrate în bazele de date de aplicații de încredere din Kaspersky Security Network.
  - Utilizatorul a plasat aplicația în grupul *Restricționat la nivel superior*.

  Aceste aplicații fac obiectul unor restricții severe în privința accesului la resursele sistemului de operare.

- **Nu este de încredere**. Acest grup include aplicații pentru care sunt îndeplinite condițiile următoare:
  - Aplicațiile nu sunt semnate digital de către distribuitori de încredere.
  - Aplicațiile nu sunt înregistrate în bazele de date de aplicații de încredere din Kaspersky Security Network.
  - Utilizatorul a plasat aplicația în grupul *Nu este de încredere*.

  Pentru astfel de aplicații, toate operațiile sunt blocate.

Anexa 3. Extensii de fișiere pentru scanarea rapidă a unităților amovibile

com – fișier executabil pentru o aplicație cu o dimensiune de maxim 64 KB

exe – fișier executabil sau arhivă cu dezarhivare automată

sys – fișier de sistem Microsoft Windows

prg – text de program pentru dBase™, Clipper sau Microsoft Visual FoxPro® sau pentru un program din suita WAVmaker

bin – fișier binar

bat – fișier de comenzi

cmd – fișier de comenzi pentru Microsoft Windows NT (similar unui fișier de comenzi pentru DOS), OS/2

dpl – bibliotecă Borland Delphi comprimată

dll – fișier bibliotecă cu legături dinamice

scr – ecran de pornire Microsoft Windows

cpl – modul panou de control Microsoft Windows

ocx – obiect Microsoft OLE (Object Linking and Embedding - Control legare și îmbinare obiect)

tsp – program care se execută în mod secvențial

drv – driver de dispozitiv

vxd – driver de dispozitiv virtual Microsoft Windows

pif – fișier de informații despre programe

lnk – fișier de link Microsoft Windows

reg – fișier cheie de registru de sistem Microsoft Windows

ini – fișier de configurare care conține date de configurare pentru Microsoft Windows, Windows NT și unele aplicații

cla – clasă Java

vbs – script Visual Basic®

vbe – extensie video BIOS

js, jse – text sursă JavaScript

htm – document hipertext

htt – antet hipertext Microsoft Windows

hta – program hipertext pentru Microsoft Internet Explorer®

asp – script Active Server Pages

chm – fișier HTML compilat

pht – fișier HTML cu scripturi PHP integrate

php – script integrat în fișiere HTML

wsh – fișier Microsoft Windows Script Host

wsf – script Microsoft Windows

the – fișier de tapet de fundal pentru desktop Microsoft Windows 95

hlp – fișier Ajutor Windows

msg – mesaj de e-mail Microsoft Mail

plg – mesaj de e-mail

mbx – mesaj de e-mail Microsoft Office salvat

doc* – documente Microsoft Office Word, cum ar fi doc pentru documente Microsoft Office Word, docx pentru documente Microsoft Office Word 2007 cu suport XML și docm pentru documente Microsoft Office Word 2007 cu suport pentru macrocomenzi.

dot* – șabloane pentru documente Microsoft Office Word, cum ar fi: dot pentru șabloane de documente Microsoft Office Word, dotx pentru șabloane de documente Microsoft Office Word 2007, dotm pentru șabloane de documente Microsoft Office Word 2007 cu suport pentru macrocomenzi.

fpm – program de baze de date, fișier de pornire Microsoft Visual FoxPro

rtf – document Rich Text Format

shs – fragment Windows Shell Scrap Object Handler

dwg – bază de date de desene AutoCAD®

msi – pachet Microsoft Windows Installer

otm – proiect VBA pentru Microsoft Office Outlook

pdf – document Adobe Acrobat

swf – obiect pachet Shockwave® Flash

jpg, jpeg – format de elemente grafice comprimate

emf – fișier de format Metafișier extins;

ico – fișier pictogramă obiect

ov? – fișiere executabile Microsoft Office Word

xl* – documente și fișiere Microsoft Office Excel, cum ar fi: xla, extensia pentru Microsoft Office Excel, xlc pentru diagrame, xlt pentru șabloane de documente, xlsx pentru registre de lucru Microsoft Office Excel 2007, xltm pentru registre de lucru Microsoft Office Excel 2007 cu suport pentru macrocomenzi, xlsb pentru registre de lucru Microsoft Office Excel 2007 în format binar (exceptând XML), xltx pentru șabloane Microsoft Office Excel 2007, xlsm pentru șabloane Microsoft Office Excel 2007 cu suport pentru macrocomenzi și xlam pentru plug-inuri Microsoft Office Excel 2007 cu suport pentru macrocomenzi

pp* – documente și fișierele Microsoft Office PowerPoint®, cum ar fi: pps pentru diapozitive Microsoft Office PowerPoint, ppt pentru prezentări, pptx pentru prezentări Microsoft Office PowerPoint 2007, pptm pentru prezentări Microsoft Office PowerPoint 2007 cu suport pentru macrocomenzi, potx pentru șabloane de prezentări Microsoft Office PowerPoint 2007, potm pentru șabloane de prezentări Microsoft Office PowerPoint 2007 cu suport pentru macrocomenzi, ppsx pentru prezentări de diapozitive Microsoft Office PowerPoint 2007, ppsm pentru prezentări de diapozitive Microsoft Office PowerPoint 2007 cu suport pentru macrocomenzi și ppam pentru plug-inuri Microsoft Office PowerPoint 2007 cu suport pentru macrocomenzi.

md* – documente și fișierele Microsoft Office Access®, cum ar fi: mda pentru grupurile de lucru Microsoft Office Access și mdb pentru bazele de date

sldx – un diapozitiv Microsoft PowerPoint 2007

sldm – un diapozitiv Microsoft PowerPoint 2007 cu suport pentru macrocomenzi

thmx – o temă Microsoft Office 2007

Anexa 4. Tipuri de fișiere pentru filtrarea atașărilor Mail Threat Protection

Reține că este posibil ca formatul real al unui fișier să nu corespundă cu extensia de nume a acestuia.

Dacă ai activat filtrarea atașărilor la mesaje de e-mail, componenta Mail Threat Protection poate să redenumească sau să șteargă fișiere cu următoarele extensii:

com – fișier executabil pentru o aplicație cu o dimensiune de maxim 64 KB

exe – fișier executabil sau arhivă cu dezarhivare automată

sys – fișier de sistem Microsoft Windows

prg – text de program pentru dBase™, Clipper sau Microsoft Visual FoxPro® sau pentru un program din suita WAVmaker

bin – fișier binar

bat – fișier de comenzi

cmd – fișier de comenzi pentru Microsoft Windows NT (similar unui fișier de comenzi pentru DOS), OS/2

dpl – bibliotecă Borland Delphi comprimată

dll – fișier bibliotecă cu legături dinamice

scr – ecran de pornire Microsoft Windows

cpl – modul panou de control Microsoft Windows

ocx – obiect Microsoft OLE (Object Linking and Embedding - Control legare și îmbinare obiect)

tsp – program care se execută în mod secvențial

drv – driver de dispozitiv

vxd – driver de dispozitiv virtual Microsoft Windows

pif – fișier de informații despre programe

lnk – fișier de link Microsoft Windows

reg – fișier cheie de registru de sistem Microsoft Windows

ini – fișier de configurare care conține date de configurare pentru Microsoft Windows, Windows NT și unele aplicații

cla – clasă Java

vbs – script Visual Basic®

vbe – extensie video BIOS

js, jse – text sursă JavaScript

htm – document hipertext

htt – antet hipertext Microsoft Windows

hta – program hipertext pentru Microsoft Internet Explorer®

asp – script Active Server Pages

chm – fișier HTML compilat

pht – fișier HTML cu scripturi PHP integrate

php – script integrat în fișiere HTML

wsh – fișier Microsoft Windows Script Host

wsf – script Microsoft Windows

the – fișier de tapet de fundal pentru desktop Microsoft Windows 95

hlp – fișier Ajutor Windows

msg – mesaj de e-mail Microsoft Mail

plg – mesaj de e-mail

mbx – mesaj de e-mail Microsoft Office salvat

doc* – documente Microsoft Office Word, cum ar fi doc pentru documente Microsoft Office Word, docx pentru documente Microsoft Office Word 2007 cu suport XML și docm pentru documente Microsoft Office Word 2007 cu suport pentru macrocomenzi.

dot* – șabloane pentru documente Microsoft Office Word, cum ar fi: dot pentru șabloane de documente Microsoft Office Word, dotx pentru șabloane de documente Microsoft Office Word 2007, dotm pentru șabloane de documente Microsoft Office Word 2007 cu suport pentru macrocomenzi.

fpm – program de baze de date, fișier de pornire Microsoft Visual FoxPro

rtf – document Rich Text Format

shs – fragment Windows Shell Scrap Object Handler

dwg – bază de date de desene AutoCAD®

msi – pachet Microsoft Windows Installer

otm – proiect VBA pentru Microsoft Office Outlook

pdf – document Adobe Acrobat

swf – obiect pachet Shockwave® Flash

jpg, jpeg – format de elemente grafice comprimate

emf – fișier de format Metafișier extins;

ico – fișier pictogramă obiect

ov? – fișiere executabile Microsoft Office Word

xl* – documente și fișiere Microsoft Office Excel, cum ar fi: xla, extensia pentru Microsoft Office Excel, xlc pentru diagrame, xlt pentru șabloane de documente, xlsx pentru registre de lucru Microsoft Office Excel 2007, xltm pentru registre de lucru Microsoft Office Excel 2007 cu suport pentru macrocomenzi, xlsb pentru registre de lucru Microsoft Office Excel 2007 în format binar (exceptând XML), xltx pentru șabloane Microsoft Office Excel 2007, xlsm pentru șabloane Microsoft Office Excel 2007 cu suport pentru macrocomenzi și xlam pentru plug-inuri Microsoft Office Excel 2007 cu suport pentru macrocomenzi

pp* – documente și fișierele Microsoft Office PowerPoint®, cum ar fi: pps pentru diapozitive Microsoft Office PowerPoint, ppt pentru prezentări, pptx pentru prezentări Microsoft Office PowerPoint 2007, pptm pentru prezentări Microsoft Office PowerPoint 2007 cu suport pentru macrocomenzi, potx pentru șabloane de prezentări Microsoft Office PowerPoint 2007, potm pentru șabloane de prezentări Microsoft Office PowerPoint 2007 cu suport pentru macrocomenzi, ppsx pentru prezentări de diapozitive Microsoft Office PowerPoint 2007, ppsm pentru prezentări de diapozitive Microsoft Office PowerPoint 2007 cu suport pentru macrocomenzi și ppam pentru plug-inuri Microsoft Office PowerPoint 2007 cu suport pentru macrocomenzi.

md* – documente și fișierele Microsoft Office Access®, cum ar fi: mda pentru grupurile de lucru Microsoft Office Access și mdb pentru bazele de date

sldx – un diapozitiv Microsoft PowerPoint 2007

sldm – un diapozitiv Microsoft PowerPoint 2007 cu suport pentru macrocomenzi

thmx – o temă Microsoft Office 2007

Anexa 5. Setări de rețea pentru interacțiunea cu servicii externe

Kaspersky Endpoint Security și Kaspersky Security Center utilizează un canal de comunicație criptat cu TLS (Transport Layer Security) pentru a lucra cu serviciile externe ale Kaspersky.

Kaspersky Endpoint Security utilizează următoarele setări de rețea pentru interacțiunea cu servicii externe.

Setări de rețea

Adresă	Descriere
`activation-v2.kaspersky.com/activationservice/activationservice.svc` Protocolul: `HTTPS` Port: `443`	Activarea aplicației.

Adresă	Descriere

`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`
Protocolul: `HTTPS`
Port: `443`
	Actualizarea bazelor de date și modulelor aplicației.

`downloads.upd.kaspersky.com` Protocolul: `HTTPS` Port: `443`	• Actualizarea bazelor de date și modulelor aplicației. • Verificarea accesului la serverele Kaspersky. Dacă accesul la servere utilizând DNS-ul sistemului nu este posibil, aplicația utilizează DNS-ul public. Acest lucru este necesar pentru a ne asigura că bazele de date antivirus sunt actualizate și că este păstrat nivelul de securitate pentru computer. Kaspersky Endpoint Security utilizează următoarea listă de servere DNS publice, în ordinea următoare: 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). Solicitările emise de aplicație pot conține adrese ale domeniilor și adresa IP publică a utilizatorului, deoarece aplicația stabilește o conexiune TCP/UDP cu serverul DNS. Această informație este necesară, de exemplu, pentru validarea certificatului unei resurse web, atunci când se utilizează HTTPS. Dacă Kaspersky Endpoint Security utilizează un server DNS public, procesarea datelor este guvernată de politica de confidențialitate a serviciului relevant. Dacă vrei să împiedici Kaspersky Endpoint Security să folosească un server DNS public, contactează Suportul tehnic pentru o corecție privată.
`touch.kaspersky.com` Protocolul: `HTTP`	• Primirea timpului de încredere pentru verificarea perioade de valabilitate a certificatului (conexiune TLS). • Avertisment cu privire la accesul refuzat la o resursă web în browser atunci când Web Threat Protection se execută.

Adresă	Descriere
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 Protocolul: HTTP Port: 80	Actualizarea bazelor de date și modulelor aplicației.
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 Protocolul: HTTPS Port: 443	Utilizarea 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 Protocolul: KSN Port: 443, 1443	Utilizarea Kaspersky Security Network.
click.kaspersky.com redirect.kaspersky.com Protocolul: HTTPS Port: 443	Urmați linkurile din interfață.

Setări, utilizate pentru criptare

Adresă	Descriere
crl.kaspersky.com ocsp.kaspersky.com Protocolul: HTTP Port: 80	Infrastructură cu cheie publică (PKI).

Anexa 6. Evenimente aplicație

Informațiile despre funcționarea fiecărei componente Kaspersky Endpoint Security, evenimentele de criptare a datelor, finalizarea fiecărei activități de scanare malware, activitatea de actualizare și activitatea de verificare a integrității, precum și despre funcționarea generală a aplicației sunt înregistrate în Jurnalul de evenimente Kaspersky Security Center și în Jurnalul de evenimente Windows.

Kaspersky Endpoint Security generează evenimente de tipurile următoare: evenimente generale și evenimente specifice. Evenimentele specifice sunt create de Kaspersky Endpoint Security for Windows. Evenimentele specifice au un ID simplu, de exemplu, `000000cb`. Evenimentele specifice conțin următorii parametri necesari:

- `GNRL_EA_DESCRIPTION` reprezintă conținutul evenimentului.
- `GNRL_EA_ID` reprezintă ID-ul serviciului evenimentului.
- `GNRL_EA_SEVERITY` reprezintă starea evenimentului. `1` – *Info*, `2` – *Warning*, `3` – *Functional failure*, `4` – *Critical*.
- `EVENT_TYPE_DISPLAY_NAME` reprezintă titlul evenimentului.
- `TASK_DISPLAY_NAME` reprezintă numele componentei aplicației care a inițiat evenimentul.

Evenimentele generale pot fi create de Kaspersky Endpoint Security for Windows, precum și de alte aplicații Kaspersky (de exemplu, Kaspersky Security for Windows Server). Evenimentele generale au un ID mai complex, de exemplu, `GNRL_EV_VIRUS_FOUND`. Pe lângă setările necesare, elementele generale conțin setări avansate.

Cât timp sunt stocate evenimentele pe server

Critică

License expired

Stare	!
Componentă	Auditare sistem
ID eveniment Windows	`201`
ID eveniment Kaspersky Security Center	`GNRL_EV_LICENSE_EXPIRATION`
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

License has almost expired

Stare	!
Componentă	Auditare sistem
ID eveniment Windows	`203`
ID eveniment Kaspersky Security Center	`000000cb`

Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Databases are missing or corrupted

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	206
ID eveniment Kaspersky Security Center	000000ce
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Databases are extremely out of date

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	207
ID eveniment Kaspersky Security Center	000000cf
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Application autorun is disabled

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	209
ID eveniment Kaspersky Security Center	000000d1
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Activation error

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	229
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Active threat detected. Advanced Disinfection should be started

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	231
ID eveniment Kaspersky Security Center	000000e7

Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

KSN servers unavailable

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	2023
ID eveniment Kaspersky Security Center	000007e7
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Not enough space in Quarantine storage

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	343
ID eveniment Kaspersky Security Center	00000157
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Object not restored from Quarantine

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	346
ID eveniment Kaspersky Security Center	0000015a
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Object not deleted from Quarantine

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	348
ID eveniment Kaspersky Security Center	0000015c
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

The application established a connection to a website with an untrusted certificate

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	57
ID eveniment Kaspersky Security Center	00000039

Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Failed to verify an encrypted connection. The domain is added to the list of exclusions

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	`60`
ID eveniment Kaspersky Security Center	`0000003c`
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Malicious object detected (local bases)

Stare	ⓘ
Componentă	File Threat Protection Web Threat Protection Mail Threat Protection Protecție AMSI Host Intrusion Prevention Behavior Detection Anti-Cryptor Exploit Prevention Scanare malware
ID eveniment Windows	`302`
ID eveniment Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND`
Parametri eveniment	• `GNRL_EA_PARAM_1` este codul hash al obiectului (SHA256). • `GNRL_EA_PARAM_2` este numele obiectului. Când este detectată o criptare externă a fișierelor partajate, aplicația afișează calea către fișierul țintă. • `GNRL_EA_PARAM_5` este numele amenințării, în conformitate cu clasificarea Kaspersky, de exemplu, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` este numele utilizatorului sesiunii. • `GNRL_EA_PARAM_8` este tipul de amenințare (`type`). • `GNRL_EA_PARAM_9` sunt informații suplimentare despre obiectul detectat: Componenta aplicației (`engine`). Tehnologii de detectare a amenințărilor (`method`). Amenințare detectată de Kaspersky Private Security Network (`blacklist`): `true` sau `false`. Versiunea EDR. Identificator amenințare în EDR. Codul hash MD5 al obiectului.
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Malicious object detected (KSN)

Stare	ⓘ
Componentă	File Threat Protection Web Threat Protection Mail Threat Protection Protecție AMSI Host Intrusion Prevention Behavior Detection Anti-Cryptor Exploit Prevention Scanare malware
ID eveniment Windows	`302`
ID eveniment Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND_BY_KSN`
Parametri eveniment	• `GNRL_EA_PARAM_1` este codul hash al obiectului (SHA256). • `GNRL_EA_PARAM_2` este numele obiectului. • `GNRL_EA_PARAM_5` este numele amenințării, în conformitate cu clasificarea Kaspersky, de exemplu, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` este numele utilizatorului sesiunii. • `GNRL_EA_PARAM_8` este tipul de amenințare (`type`). • `GNRL_EA_PARAM_9` sunt informații suplimentare despre obiectul detectat: Componenta aplicației (`engine`). Tehnologii de detectare a amenințărilor (`method`). Amenințare detectată de Kaspersky Private Security Network (`blacklist`): `true` sau `false`. Versiunea EDR. Identificator amenințare în EDR. Codul hash MD5 al obiectului.
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Disinfection impossible

Stare	ⓘ
Componentă	File Threat Protection Mail Threat Protection Host Intrusion Prevention Behavior Detection Anti-Cryptor Scanare malware
ID eveniment Windows	`312`
ID eveniment Kaspersky Security Center	`GNRL_EV_OBJECT_NOTCURED`
Parametri eveniment	• `GNRL_EA_PARAM_1` este codul hash al obiectului (SHA256). • `GNRL_EA_PARAM_2` este numele obiectului. • `GNRL_EA_PARAM_5` este numele amenințării, în conformitate cu clasificarea Kaspersky, de exemplu, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` este numele utilizatorului sesiunii. • `GNRL_EA_PARAM_8` este tipul de amenințare (`type`). • `GNRL_EA_PARAM_9` sunt informații suplimentare despre obiectul detectat: Componenta aplicației (`engine`). Tehnologii de detectare a amenințărilor (`method`). Amenințare detectată de Kaspersky Private Security Network (`blacklist`): `true` sau `false`. Versiunea EDR. Identificator amenințare în EDR. Codul hash MD5 al obiectului.
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Cannot be deleted

Stare	ⓘ
Componentă	File Threat Protection Host Intrusion Prevention Behavior Detection Anti-Cryptor Scanare malware
ID eveniment Windows	313
ID eveniment Kaspersky Security Center	00000139
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Processing error

Stare	ⓘ
Componentă	File Threat Protection Web Threat Protection Mail Threat Protection Host Intrusion Prevention Protecție AMSI Scanare malware
ID eveniment Windows	317
ID eveniment Kaspersky Security Center	0000013d
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Process terminated

Stare	ⓘ
Componentă	File Threat Protection Host Intrusion Prevention Behavior Detection Scanare malware
ID eveniment Windows	452
ID eveniment Kaspersky Security Center	000001c4
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Unable to terminate process

Stare	ⓘ
Componentă	File Threat Protection Host Intrusion Prevention Behavior Detection Scanare malware
ID eveniment Windows	453
ID eveniment Kaspersky Security Center	000001c5
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Dangerous link blocked

Stare	⚠
Componentă	Web Threat Protection
ID eveniment Windows	362
ID eveniment Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_BLOCKED
Parametri eveniment	• GNRL_EA_PARAM_2 este calea către obiect. • GNRL_EA_PARAM_5 este numele obiectului conform clasificării Kaspersky. • GNRL_EA_PARAM_7 este numele utilizatorului sesiunii. • GNRL_EA_PARAM_8 este tipul de amenințare (type). • GNRL_EA_PARAM_9 sunt informații suplimentare despre obiectul detectat: Componenta aplicației (engine). Tehnologii de detectare a amenințărilor (method). Amenințare detectată de Private KSN (blacklist): true sau false.
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Dangerous link opened

Stare	⚠
Componentă	Web Threat Protection
ID eveniment Windows	363
ID eveniment Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_REPORTED
Parametri eveniment	• GNRL_EA_PARAM_2 este calea către obiect. • GNRL_EA_PARAM_5 este numele obiectului conform clasificării Kaspersky. • GNRL_EA_PARAM_7 este numele utilizatorului sesiunii. • GNRL_EA_PARAM_8 este tipul de amenințare (type). • GNRL_EA_PARAM_9 sunt informații suplimentare despre obiectul detectat: Componenta aplicației (engine). Tehnologii de detectare a amenințărilor (method). Amenințare detectată de Private KSN (blacklist): true sau false.
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Previously opened dangerous link detected

Stare	⚠
Componentă	Web Threat Protection
ID eveniment Windows	1201
ID eveniment Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_PASSED
Parametri eveniment	• GNRL_EA_PARAM_2 este calea către obiect. • GNRL_EA_PARAM_5 este numele obiectului conform clasificării Kaspersky. • GNRL_EA_PARAM_7 este numele utilizatorului sesiunii. • GNRL_EA_PARAM_8 este tipul de amenințare (type). • GNRL_EA_PARAM_9 sunt informații suplimentare despre obiectul detectat: Componenta aplicației (engine). Tehnologii de detectare a amenințărilor (method). Amenințare detectată de Private KSN (blacklist): true sau false.
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Process action blocked

Stare	⚠
Componentă	Control adaptiv al anomaliilor
ID eveniment Windows	`2200`
ID eveniment Kaspersky Security Center	`GNRL_EV_ADSEC_DETECT`
Parametri eveniment	• `GNRL_EA_PARAM_1` este numele regulii Control adaptiv al anomaliilor. • `GNRL_EA_PARAM_2` este ID-ul regulii euristice. • `GNRL_EA_PARAM_3` este numele utilizatorului sesiunii. • `GNRL_EA_PARAM_4` este procesul sursă. • `GNRL_EA_PARAM_5` este obiectul sursă. • `GNRL_EA_PARAM_6` este procesul țintă. • `GNRL_EA_PARAM_7` este obiectul țintă. • `GNRL_EA_PARAM_8` sunt informații suplimentare despre obiectul detectat: Sume de control ale procesului/obiectului sursă și ale procesului/obiectului țintă. Proces blocat (`verdict_type`): `true` sau `false`. ID securitate utilizator (SID).
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Keyboard not authorized

Stare	⚠
Componentă	BadUSB Attack Prevention
ID eveniment Windows	`2051`
ID eveniment Kaspersky Security Center	`00000803`
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

AMSI request was blocked

Stare	⚠
Componentă	Protecție AMSI
ID eveniment Windows	`2200`
ID eveniment Kaspersky Security Center	`00000898`
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Network activity blocked

Stare	⚠
Componentă	Firewall
ID eveniment Windows	`602`
ID eveniment Kaspersky Security Center	`00000329`
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Network attack detected

Stare	⚠
Componentă	Network Threat Protection
ID eveniment Windows	651
ID eveniment Kaspersky Security Center	GNRL_EV_ATTACK_DETECTED
Parametri eveniment	• GNRL_EA_PARAM_1 este numele atacului. • GNRL_EA_PARAM_2 este protocolul. • GNRL_EA_PARAM_3 este adresa IP a computerului care acționează ca sursă a atacului de rețea. Adresa IP este indicată în ordinea octeților gazdei. De exemplu, 2886729929 pentru 172.16.0.201. • GNRL_EA_PARAM_4 este numărul portului. • GNRL_EA_PARAM_5 este o adresă IPv6, de exemplu, 12B012B012B012B012B012B012B012B0. • GNRL_EA_PARAM_6 este adresa IP a computerului vizat de atacul de rețea. Adresa IP este indicată în ordinea octeților gazdei. De exemplu, 2886729929 pentru 172.16.0.201.
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Application startup prohibited

Stare	⚠
Componentă	Application Control
ID eveniment Windows	702
ID eveniment Kaspersky Security Center	GNRL_EV_APPLICATION_LAUNCH_DENIED
Parametri eveniment	• GNRL_EA_PARAM_2 este numele utilizatorului sesiunii. • GNRL_EA_PARAM_3 este identificatorul categoriei creat manual. • GNRL_EA_PARAM_4 este ID-ul categoriei aplicației. • GNRL_EA_PARAM_5 sunt informații despre semnătura digitală a aplicației. • GNRL_EA_PARAM_6 este numele fișierului executabil al aplicației (de exemplu, chrome.exe). • GNRL_EA_PARAM_7 este calea către fișierul executabil. • GNRL_EA_PARAM_8 este codul hash al obiectului (SHA256). • GNRL_EA_PARAM_9 este versiunea aplicației pe care utilizatorul încearcă să o execute.
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Prohibited process was started before Kaspersky Endpoint Security startup

Stare	⚠
Componentă	Application Control
ID eveniment Windows	710
ID eveniment Kaspersky Security Center	000002c6
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Access denied (local bases)

Stare	⚠
Componentă	Control Web

ID eveniment Windows	752
ID eveniment Kaspersky Security Center	GNRL_EV_WEB_URL_BLOCKED
Parametri eveniment	• GNRL_EA_PARAM_1 este adresa URL. • GNRL_EA_PARAM_2 este numele utilizatorului sesiunii. • GNRL_EA_PARAM_3 este numele regulii Web Control.
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Access denied (KSN)

Stare	ⓘ
Componentă	Control Web
ID eveniment Windows	752
ID eveniment Kaspersky Security Center	GNRL_EV_WEB_URL_BLOCKED_BY_KSN
Parametri eveniment	• GNRL_EA_PARAM_1 este adresa URL. • GNRL_EA_PARAM_2 este numele utilizatorului sesiunii. • GNRL_EA_PARAM_3 este numele regulii Web Control.
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Operation with the device prohibited

Stare	ⓘ
Componentă	Control dispozitive
ID eveniment Windows	802
ID eveniment Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
Parametri eveniment	• GNRL_EA_PARAM_1 este ID-ul hardware (HWID). • GNRL_EA_PARAM_2 este numele utilizatorului sesiunii.
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Network connection blocked

Stare	ⓘ
Componentă	Control dispozitive
ID eveniment Windows	809
ID eveniment Kaspersky Security Center	00000329
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Error updating component

Stare	ⓘ
Componentă	Actualizează
ID eveniment Windows	1011
ID eveniment Kaspersky Security Center	000003f3

Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Error distributing component updates

Stare	ⓘ
Componentă	Actualizează
ID eveniment Windows	1012
ID eveniment Kaspersky Security Center	000003f4
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Local update error

Stare	ⓘ
Componentă	Actualizează
ID eveniment Windows	1014
ID eveniment Kaspersky Security Center	000003f6
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Network update error

Stare	ⓘ
Componentă	Actualizează
ID eveniment Windows	1015
ID eveniment Kaspersky Security Center	000003f7
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Cannot start two tasks at the same time

Stare	ⓘ
Componentă	Actualizează
ID eveniment Windows	1017
ID eveniment Kaspersky Security Center	000003f9
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Error verifying application databases and modules

Stare	ⓘ
Componentă	Actualizează
ID eveniment Windows	1018
ID eveniment Kaspersky Security Center	000003fa

Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Error in interaction with Kaspersky Security Center

Stare	ⓘ
Componentă	Actualizează
ID eveniment Windows	1019
ID eveniment Kaspersky Security Center	000003fb
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Not all components were updated

Stare	ⓘ
Componentă	Actualizează
ID eveniment Windows	1021
ID eveniment Kaspersky Security Center	000003fd
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Update completed successfully, update distribution failed

Stare	ⓘ
Componentă	Actualizează
ID eveniment Windows	1023
ID eveniment Kaspersky Security Center	000003ff
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Internal task error

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	101
ID eveniment Kaspersky Security Center	00000065
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Patch installation failed

Stare	ⓘ
Componentă	Actualizează
ID eveniment Windows	2153
ID eveniment Kaspersky Security Center	00000869

Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Patch rollback failed

Stare	⚠
Componentă	Actualizează
ID eveniment Windows	2156
ID eveniment Kaspersky Security Center	0000086c
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Error applying file encryption / decryption rules

Stare	⚠
Componentă	Criptare date
ID eveniment Windows	904
ID eveniment Kaspersky Security Center	00000388
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

File encryption / decryption error

Stare	⚠
Componentă	Criptare date
ID eveniment Windows	912
ID eveniment Kaspersky Security Center	GNRL_EV_ENCRYPTION_ERROR
Parametri eveniment	• GNRL_EA_PARAM_1 este calea către fișier. • GNRL_EA_PARAM_2 este cauza erorii. • GNRL_EA_PARAM_3 este tipul dispozitivului.
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

File access blocked

Stare	⚠
Componentă	Criptare date
ID eveniment Windows	940
ID eveniment Kaspersky Security Center	GNRL_EV_ENCRYPTION_DATAACCESS_VIOLATION
Parametri eveniment	• GNRL_EA_PARAM_1 este obiectul țintă. • GNRL_EA_PARAM_2 este numele utilizatorului sesiunii. • GNRL_EA_PARAM_3 este numele fișierului executabil al aplicației (de exemplu, chrome.exe), care încearcă să obțină acces la fișier.
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Error enabling portable mode

Stare	⚠
Componentă	Criptare date
ID eveniment Windows	951
ID eveniment Kaspersky Security Center	000003b7
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Error disabling portable mode

Stare	⚠
Componentă	Criptare date
ID eveniment Windows	953
ID eveniment Kaspersky Security Center	000003b9
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Error creating encrypted package

Stare	⚠
Componentă	Criptare date
ID eveniment Windows	931
ID eveniment Kaspersky Security Center	000003a3
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Error encrypting / decrypting device

Stare	⚠
Componentă	Criptare date
ID eveniment Windows	1305
ID eveniment Kaspersky Security Center	00000519
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Could not load encryption module

Stare	⚠
Componentă	Criptare date
ID eveniment Windows	1311
ID eveniment Kaspersky Security Center	0000051f
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

The task for managing Authentication Agent accounts ended with an error

Stare	ⓘ
Componentă	Criptare date
ID eveniment Windows	1340
ID eveniment Kaspersky Security Center	0000053c
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Policy cannot be applied

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	1312
ID eveniment Kaspersky Security Center	00000520
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

FDE upgrade failed

Stare	ⓘ
Componentă	Criptare date
ID eveniment Windows	1342
ID eveniment Kaspersky Security Center	0000053e
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

FDE upgrade rollback failed (for more information, please refer to the Kaspersky Endpoint Security for Windows Online Help)

Stare	ⓘ
Componentă	Criptare date
ID eveniment Windows	1344
ID eveniment Kaspersky Security Center	00000540
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Kaspersky Anti Targeted Attack Platform server unavailable

Stare	ⓘ
Componentă	Endpoint Sensor
ID eveniment Windows	2100
ID eveniment Kaspersky Security Center	00000834
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Failed to delete object

Stare	⚠
Componentă	Sandbox
ID eveniment Windows	2252
ID eveniment Kaspersky Security Center	000008cc
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Object not quarantined (Sandbox)

Stare	⚠
Componentă	Sandbox
ID eveniment Windows	2603
ID eveniment Kaspersky Security Center	00000a2b
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

An internal error occurred

Stare	⚠
Componentă	Sandbox
ID eveniment Windows	2607
ID eveniment Kaspersky Security Center	00000a2f
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Invalid Sandbox server certificate

Stare	⚠
Componentă	Sandbox
ID eveniment Windows	2613
ID eveniment Kaspersky Security Center	00000a35
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

The Sandbox node is unavailable

Stare	⚠
Componentă	Sandbox
ID eveniment Windows	2614
ID eveniment Kaspersky Security Center	00000a36
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Failed to process the object in Sandbox

Stare	⚠
Componentă	Sandbox
ID eveniment Windows	2617
ID eveniment Kaspersky Security Center	00000a39
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Maximum load to Sandbox is exceeded

Stare	⚠
Componentă	Sandbox
ID eveniment Windows	2618
ID eveniment Kaspersky Security Center	00000a3a
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

IOC found

Stare	⚠
Componentă	Endpoint Detection and Response
ID eveniment Windows	2651
ID eveniment Kaspersky Security Center	00000a5b
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Sandbox license verification failed

Stare	⚠
Componentă	Sandbox
ID eveniment Windows	2620
ID eveniment Kaspersky Security Center	00000a3c
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Eroare la trimiterea activității de scanare către Sandbox de către un utilizator

Stare	⚠
Componentă	Sandbox
ID eveniment Windows	2623
ID eveniment Kaspersky Security Center	00000a3e
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Eroare la crearea activității Sandbox

Stare	ⓘ
Componentă	Sandbox
ID eveniment Windows	2621
ID eveniment Kaspersky Security Center	00000a3d
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Object startup blocked

Stare	ⓘ
Componentă	Endpoint Detection and Response
ID eveniment Windows	2553
ID eveniment Kaspersky Security Center	000009f9
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Process startup blocked

Stare	ⓘ
Componentă	Endpoint Detection and Response
ID eveniment Windows	2551
ID eveniment Kaspersky Security Center	000009f7
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Script execution blocked

Stare	ⓘ
Componentă	Endpoint Detection and Response
ID eveniment Windows	2559
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Object not quarantined (Endpoint Detection and Response)

Stare	ⓘ
Componentă	Endpoint Detection and Response
ID eveniment Windows	2556
ID eveniment Kaspersky Security Center	000009fc
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Process startup is not blocked

Stare	ⓘ
Componentă	Endpoint Detection and Response
ID eveniment Windows	2561
ID eveniment Kaspersky Security Center	00000a01
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Object is not blocked

Stare	ⓘ
Componentă	Endpoint Detection and Response
ID eveniment Windows	2562
ID eveniment Kaspersky Security Center	00000a02
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Script execution is not blocked

Stare	ⓘ
Componentă	Endpoint Detection and Response
ID eveniment Windows	2563
ID eveniment Kaspersky Security Center	00000a03
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Error changing application components

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	1401
ID eveniment Kaspersky Security Center	00000579
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

There are patterns of a possible brute-force attack in the system

Stare	ⓘ
Componentă	Inspecție jurnal
ID eveniment Windows	2800
ID eveniment Kaspersky Security Center	00000af0
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

There are patterns of a possible Windows Event Log abuse

Stare	ⓘ
Componentă	Inspecție jurnal
ID eveniment Windows	2801
ID eveniment Kaspersky Security Center	00000af1
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Atypical actions detected on behalf of a new service installed

Stare	ⓘ
Componentă	Inspecție jurnal
ID eveniment Windows	2802
ID eveniment Kaspersky Security Center	00000af2
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Atypical logon that uses explicit credentials detected

Stare	ⓘ
Componentă	Inspecție jurnal
ID eveniment Windows	2803
ID eveniment Kaspersky Security Center	00000af3
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

There are patterns of a possible Kerberos forged PAC (MS14-068) attack in the system

Stare	ⓘ
Componentă	Inspecție jurnal
ID eveniment Windows	2804
ID eveniment Kaspersky Security Center	00000af4
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Suspicious changes detected in the privileged built-in Administrators group

Stare	ⓘ
Componentă	Inspecție jurnal
ID eveniment Windows	2805
ID eveniment Kaspersky Security Center	00000af5
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

There is an atypical activity detected during a network logon session

Stare	!
Componentă	Inspecție jurnal
ID eveniment Windows	2806
ID eveniment Kaspersky Security Center	00000af6
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Log Inspection rule triggered

Stare	!
Componentă	Inspecție jurnal
ID eveniment Windows	2807
ID eveniment Kaspersky Security Center	00000af7
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Atypical event occurs too often. Event aggregation started

Stare	!
Componentă	Inspecție jurnal
ID eveniment Windows	2808
ID eveniment Kaspersky Security Center	00000af8
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Report on an atypical event for the aggregation period

Stare	!
Componentă	Inspecție jurnal
ID eveniment Windows	2809
ID eveniment Kaspersky Security Center	00000af9
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Error connecting to the EDR Expert server

Stare	!
Componentă	Endpoint Detection and Response Expert (on-premises)
ID eveniment Windows	2850
ID eveniment Kaspersky Security Center	00000b22
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Invalid certificate of the EDR Expert server

Stare	!
Componentă	Endpoint Detection and Response Expert (on-premises)
ID eveniment Windows	2851
ID eveniment Kaspersky Security Center	00000b23
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Invalid certificate of the agent on the EDR Expert server

Stare	!
Componentă	Endpoint Detection and Response Expert (on-premises)
ID eveniment Windows	2852
ID eveniment Kaspersky Security Center	00000b24
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Eroare la conectarea la serverul de răspuns EDR Expert

Stare	!
Componentă	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID eveniment Windows	2858
ID eveniment Kaspersky Security Center	00000b22
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Certificat nevalid al serverului de răspuns EDR Expert

Stare	!
Componentă	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID eveniment Windows	2859
ID eveniment Kaspersky Security Center	00000b23
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Certificat nevalid al agentului de pe serverul de răspuns EDR Expert

Stare	!
Componentă	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID eveniment Windows	2860
ID eveniment Kaspersky Security Center	00000b24

Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Eroare de conectare la serverul de colectare a telemetriei EDR Expert

Stare	ⓘ
Componentă	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID eveniment Windows	2854
ID eveniment Kaspersky Security Center	00000b22
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Certificat nevalid al serverului de colectare a telemetriei EDR Expert

Stare	ⓘ
Componentă	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID eveniment Windows	2855
ID eveniment Kaspersky Security Center	00000b23
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Certificat nevalid al agentului de pe serverul de colectare a telemetriei EDR Expert

Stare	ⓘ
Componentă	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID eveniment Windows	2856
ID eveniment Kaspersky Security Center	00000b24
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Eroare la conectarea la serverul NDR

Stare	ⓘ
Componentă	Network Detection and Response (KATA)
ID eveniment Windows	3080
ID eveniment Kaspersky Security Center	00000c08
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Certificat nevalid al serverului NDR

Stare	ⓘ
Componentă	Network Detection and Response (KATA)
ID eveniment Windows	3081

ID eveniment Kaspersky Security Center	00000c09
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Certificat nevalid al agentului de pe serverul NDR

Stare	ⓘ
Componentă	Network Detection and Response (KATA)
ID eveniment Windows	3082
ID eveniment Kaspersky Security Center	00000c0a
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Dispozitivul tău este conectat la un Server de administrare care nu este de încredere. Contactează administratorul

Stare	ⓘ
Componentă	Protecție conexiune Server de administrare
ID eveniment Windows	3301
ID eveniment Kaspersky Security Center	00000ce5
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

File or folder change was detected

Stare	ⓘ / ⚠ / ⓘ
Componentă	Monitorizare integritate sistem
ID eveniment Windows	2950
ID eveniment Kaspersky Security Center	00000b86
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Pentru a configura perioada de păstrare pentru acest eveniment, accesează secțiunea **Event configuration** a politicii și setează perioada de păstrare pentru evenimentul Monitorizare integritate sistem general – *File or folder change was detected*.

Object changes too often. Event aggregation started

Stare	ⓘ / ⚠ / ⓘ
Componentă	Monitorizare integritate sistem
ID eveniment Windows	2955
ID eveniment Kaspersky Security Center	00000b8b
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Report on object modification for the aggregation period

Stare	ⓘ / ⚠ / ⓘ
Componentă	Monitorizare integritate sistem
ID eveniment Windows	2956
ID eveniment Kaspersky Security Center	00000b8c
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Pentru a configura perioada de păstrare pentru acest eveniment, accesează secțiunea **Event configuration** a politicii și setează perioada de păstrare pentru evenimentul Monitorizare integritate sistem general – *File or folder change was detected*.

Monitoring scope includes incorrect objects

Stare	ⓘ
Componentă	Monitorizare integritate sistem
ID eveniment Windows	2953
ID eveniment Kaspersky Security Center	00000b89
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Registry change was detected

Stare	ⓘ / ⚠ / ⓘ
Componentă	Monitorizare integritate sistem
ID eveniment Windows	2951
ID eveniment Kaspersky Security Center	00000b87
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Pentru a configura perioada de păstrare pentru acest eveniment, accesează secțiunea **Event configuration** a politicii și setează perioada de păstrare pentru evenimentul Monitorizare integritate sistem general – *File or folder change was detected*.

Device connection / disconnection is detected

Stare	ⓘ / ⚠ / ⓘ
Componentă	Monitorizare integritate sistem
ID eveniment Windows	2952
ID eveniment Kaspersky Security Center	00000b88
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Pentru a configura perioada de păstrare pentru acest eveniment, accesează secțiunea **Event configuration** a politicii și setează perioada de păstrare pentru evenimentul Monitorizare integritate sistem general – *File or folder change was detected*.

Domeniul de monitorizare include obiecte incorecte

Stare	ⓘ / ⚠ / ⓘ
Componentă	Monitorizare integritate sistem
ID eveniment Windows	2903
ID eveniment Kaspersky Security Center	00000b89
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Pentru a configura perioada de păstrare pentru acest eveniment, accesează secțiunea **Event configuration** a politicii și setează perioada de păstrare pentru evenimentul Monitorizare integritate sistem general – *File or folder change was detected*.

Attempts to perform the restricted operations with the object is too many. Event aggregation started

Stare	ⓘ
Componentă	Monitorizare integritate sistem
ID eveniment Windows	2963
ID eveniment Kaspersky Security Center	00000b93
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

An operation with the files of the monitoring scope was blocked

Stare	ⓘ
Componentă	Monitorizare integritate sistem
ID eveniment Windows	2959
ID eveniment Kaspersky Security Center	00000b8f
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Pentru a configura perioada de păstrare pentru acest eveniment, accesează secțiunea **Event configuration** a politicii și setează perioada de păstrare pentru evenimentul Monitorizare integritate sistem general – *File or folder change was detected*.

Registry modification blocked

Stare	ⓘ
Componentă	Monitorizare integritate sistem
ID eveniment Windows	2960
ID eveniment Kaspersky Security Center	00000b90
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Pentru a configura perioada de păstrare pentru acest eveniment, accesează secțiunea **Event configuration** a politicii și setează perioada de păstrare pentru evenimentul Monitorizare integritate sistem general – *File or folder change was detected*.

Processing error

Stare	ⓘ
Componentă	Monitorizare integritate sistem
ID eveniment Windows	2954
ID eveniment Kaspersky Security Center	00000b8a
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

System Integrity Monitoring: rule triggering disabled for user accounts without matching security identifier (SID)

Stare	ⓘ
Componentă	Monitorizare integritate sistem
ID eveniment Windows	2964
ID eveniment Kaspersky Security Center	00000b94
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Application Control: rule triggering disabled for user accounts without matching security identifier (SID)

Stare	ⓘ
Componentă	Application Control
ID eveniment Windows	711
ID eveniment Kaspersky Security Center	000002c7
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Device Control: rule triggering disabled for user accounts without matching security identifier (SID)

Stare	ⓘ
Componentă	Control dispozitive
ID eveniment Windows	810
ID eveniment Kaspersky Security Center	0000032a
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Web Control: rule triggering disabled for user accounts without matching security identifier (SID)

Stare	ⓘ
Componentă	Control Web
ID eveniment Windows	757
ID eveniment Kaspersky Security Center	000002f5
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Adaptive Anomaly Control: rule triggering disabled for user accounts without matching security identifier (SID)

Stare	⚠
Componentă	Control adaptiv al anomaliilor
ID eveniment Windows	504
ID eveniment Kaspersky Security Center	000001f8
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Log Inspection: rule triggering disabled for user accounts without matching security identifier (SID)

Stare	⚠
Componentă	Inspecție jurnal
ID eveniment Windows	2810
ID eveniment Kaspersky Security Center	00000afa
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Unable to connect to the Integration Server for more than 6 hours. Check Integration Server status and network settings

Stare	⚠
Componentă	Light Agent
ID eveniment Windows	3103
ID eveniment Kaspersky Security Center	00000c1f
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

SVM is unavailable

Stare	⚠
Componentă	Light Agent
ID eveniment Windows	3151
ID eveniment Kaspersky Security Center	00000c4f
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Malicious object detected. Advanced Disinfection should be started on a virtual machine template

Stare	⚠
Componentă	Light Agent
ID eveniment Windows	3182
ID eveniment Kaspersky Security Center	00000c6e
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Conexiunea la rețea stabilită prin protocolul depreciat a fost blocată

Stare	ⓘ
Componentă	Protecție
ID eveniment Windows	75
ID eveniment Kaspersky Security Center	0000004b
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Eroare conexiune server KUMA

Stare	ⓘ
Componentă	Integrare KUMA
ID eveniment Windows	2854
ID eveniment Kaspersky Security Center	00000b26
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Certificat nevalid al serverului KUMA

Stare	ⓘ
Componentă	Integrare KUMA
ID eveniment Windows	2855
ID eveniment Kaspersky Security Center	00000b27
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Certificat nevalid al agentului de pe serverul KUMA

Stare	ⓘ
Componentă	Integrare KUMA
ID eveniment Windows	2856
ID eveniment Kaspersky Security Center	00000b28
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Eroare funcțională

Task cannot be performed

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	212
ID eveniment Kaspersky Security Center	000000d4

Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Invalid task settings. Settings not applied

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	707
ID eveniment Kaspersky Security Center	000002c3
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Avertisment

Application crashed during previous session

Stare	⚠
Componentă	Auditare sistem
ID eveniment Windows	237
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

License expires soon

Stare	⚠
Componentă	Auditare sistem
ID eveniment Windows	204
ID eveniment Kaspersky Security Center	000000cc
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Databases are out of date

Stare	⚠
Componentă	Auditare sistem
ID eveniment Windows	208
ID eveniment Kaspersky Security Center	000000d0
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Automatic updates are disabled

Stare	⚠
Componentă	Auditare sistem
ID eveniment Windows	210
ID eveniment Kaspersky Security Center	000000d2
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Self-Defense is disabled

Stare	⚠
Componentă	Auditare sistem
ID eveniment Windows	211
ID eveniment Kaspersky Security Center	000000d3
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Protection components are disabled

Stare	⚠
Componentă	Auditare sistem
ID eveniment Windows	214
ID eveniment Kaspersky Security Center	000000d6
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Computer is running in safe mode

Stare	⚠
Componentă	Auditare sistem
ID eveniment Windows	215
ID eveniment Kaspersky Security Center	000000d7
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

There are unprocessed files

Stare	⚠
Componentă	Auditare sistem
ID eveniment Windows	216
ID eveniment Kaspersky Security Center	000000d8
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Group policy applied

Stare	⚠
Componentă	Auditare sistem
ID eveniment Windows	219
ID eveniment Kaspersky Security Center	000000db
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Task stopped

Stare	⚠
Componentă	Auditare sistem
ID eveniment Windows	222
ID eveniment Kaspersky Security Center	000000de
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Quit and reopen the application to complete updating

Stare	⚠
Componentă	Auditare sistem
ID eveniment Windows	224
ID eveniment Kaspersky Security Center	0000057b
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Computer restart required

Stare	⚠
Componentă	Auditare sistem
ID eveniment Windows	225
ID eveniment Kaspersky Security Center	000000e1
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

The license allows the use of components that have not been installed

Stare	⚠
Componentă	Auditare sistem
ID eveniment Windows	226
ID eveniment Kaspersky Security Center	000000e2
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Advanced Disinfection started

Stare	⚠
Componentă	Auditare sistem
ID eveniment Windows	232
ID eveniment Kaspersky Security Center	000000e8
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Advanced Disinfection completed

Stare	⚠
Componentă	Auditare sistem
ID eveniment Windows	233
ID eveniment Kaspersky Security Center	000000e9
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Incorrect reserve key

Stare	⚠
Componentă	Auditare sistem
ID eveniment Windows	230
ID eveniment Kaspersky Security Center	000000e6
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Subscription expires soon

Stare	⚠
Componentă	Auditare sistem
ID eveniment Windows	240
ID eveniment Kaspersky Security Center	000000f0
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Blocat

Stare	⚠
Componentă	Behavior Detection Anti-Cryptor Exploit Prevention Web Threat Protection
ID eveniment Windows	331

ID eveniment Kaspersky Security Center	GNRL_EV_OBJECT_BLOCKED
Parametri eveniment	• GNRL_EA_PARAM_1 este codul hash al obiectului (SHA256). • GNRL_EA_PARAM_2 este numele obiectului. Când este detectată o criptare externă a fișierelor partajate, aplicația afișează calea către fișierul țintă. • GNRL_EA_PARAM_5 este numele amenințării, în conformitate cu clasificarea Kaspersky, de exemplu, EICAR-Test-File. • GNRL_EA_PARAM_7 este numele utilizatorului sesiunii. • GNRL_EA_PARAM_8 este tipul de amenințare (type). • GNRL_EA_PARAM_9 sunt informații suplimentare despre obiectul detectat: Componenta aplicației (engine). Tehnologii de detectare a amenințărilor (method). Amenințare detectată de Kaspersky Private Security Network (blacklist): true sau false. Versiunea EDR. Identificator amenințare în EDR. Codul hash MD5 al obiectului.
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

The operating system settings do not allow to control access to Wi-Fi networks

Stare	⚠
Componentă	Control dispozitive
ID eveniment Windows	249
ID eveniment Kaspersky Security Center	000000f9
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Object not restored from Backup

Stare	⚠
Componentă	Auditare sistem
ID eveniment Windows	336
ID eveniment Kaspersky Security Center	00000150
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Suspicious network activity detected

Stare	⚠
Componentă	Auditare sistem
ID eveniment Windows	2001
ID eveniment Kaspersky Security Center	000007d1
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Encrypted connection terminated

Stare	⚠
Componentă	Auditare sistem
ID eveniment Windows	250
ID eveniment Kaspersky Security Center	000007d3
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Participation in KSN disabled

Stare	⚠
Componentă	Auditare sistem
ID eveniment Windows	2021
ID eveniment Kaspersky Security Center	000007e5
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Processing of some OS functions is disabled

Stare	⚠
Componentă	Auditare sistem
ID eveniment Windows	245
ID eveniment Kaspersky Security Center	000000f5
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Quarantine storage is almost out of space

Stare	⚠
Componentă	Auditare sistem
ID eveniment Windows	344
ID eveniment Kaspersky Security Center	00000158
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Network connection blocked

Stare	⚠
Componentă	Auditare sistem
ID eveniment Windows	809
ID eveniment Kaspersky Security Center	00000abe
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Cannot create a backup copy

Stare	⚠
Componentă	File Threat Protection Mail Threat Protection Host Intrusion Prevention Protecție AMSI Scanare malware
ID eveniment Windows	`314`
ID eveniment Kaspersky Security Center	`GNRL_EV_OBJECT_REPORTED`
Parametri eveniment	• `GNRL_EA_PARAM_1` este codul hash al obiectului (SHA256). • `GNRL_EA_PARAM_2` este numele obiectului. • `GNRL_EA_PARAM_5` este numele amenințării, în conformitate cu clasificarea Kaspersky, de exemplu, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` este numele utilizatorului sesiunii. • `GNRL_EA_PARAM_8` este tipul de amenințare (`type`). • `GNRL_EA_PARAM_9` sunt informații suplimentare despre obiectul detectat: Componenta aplicației (`engine`). Tehnologii de detectare a amenințărilor (`method`). Amenințare detectată de Kaspersky Private Security Network (`blacklist`): `true` sau `false`. Versiunea EDR. Identificator amenințare în EDR. Codul hash MD5 al obiectului.
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Stare	⚠
Componentă	File Threat Protection Behavior Detection Anti-Cryptor Host Intrusion Prevention Scanare malware
ID eveniment Windows	`310`
ID eveniment Kaspersky Security Center	`00000136`
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Object encrypted

Stare	⚠
Componentă	Host Intrusion Prevention
ID eveniment Windows	`320`
ID eveniment Kaspersky Security Center	`00000140`
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Object corrupted

Stare	⚠
Componentă	File Threat Protection Web Threat Protection Mail Threat Protection Protecție AMSI Host Intrusion Prevention Scanare malware
ID eveniment Windows	`321`
ID eveniment Kaspersky Security Center	`00000141`
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Legitimate software that can be used by intruders to damage your computer or personal data was detected (local bases)

Stare	⚠
Componentă	File Threat Protection Web Threat Protection Mail Threat Protection Host Intrusion Prevention Protecție AMSI Behavior Detection Anti-Cryptor Anti-Cryptor Scanare malware
ID eveniment Windows	`303`
ID eveniment Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND`
Parametri eveniment	• `GNRL_EA_PARAM_1` este codul hash al obiectului (SHA256). • `GNRL_EA_PARAM_2` este numele obiectului. • `GNRL_EA_PARAM_5` este numele amenințării, în conformitate cu clasificarea Kaspersky, de exemplu, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` este numele utilizatorului sesiunii. • `GNRL_EA_PARAM_8` este tipul de amenințare (`type`).
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Legitimate software that can be used by intruders to damage your computer or personal data was detected (KSN)

Stare	⚠
Componentă	File Threat Protection Web Threat Protection Mail Threat Protection Host Intrusion Prevention Protecție AMSI Behavior Detection Anti-Cryptor Anti-Cryptor Scanare malware
ID eveniment Windows	`303`

ID eveniment Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_BY_KSN
Parametri eveniment	• GNRL_EA_PARAM_1 este codul hash al obiectului (SHA256). • GNRL_EA_PARAM_2 este numele obiectului. • GNRL_EA_PARAM_5 este numele amenințării, în conformitate cu clasificarea Kaspersky, de exemplu, EICAR-Test-File. • GNRL_EA_PARAM_7 este numele utilizatorului sesiunii. • GNRL_EA_PARAM_8 este tipul de amenințare (type).
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Object deleted

Stare	⚠
Componentă	File Threat Protection Mail Threat Protection Host Intrusion Prevention Exploit Prevention Behavior Detection Anti-Cryptor Scanare malware
ID eveniment Windows	307
ID eveniment Kaspersky Security Center	GNRL_EV_OBJECT_DELETED
Parametri eveniment	• GNRL_EA_PARAM_1 este codul hash al obiectului (SHA256). • GNRL_EA_PARAM_2 este numele obiectului. • GNRL_EA_PARAM_5 este numele amenințării, în conformitate cu clasificarea Kaspersky, de exemplu, EICAR-Test-File. • GNRL_EA_PARAM_7 este numele utilizatorului sesiunii. • GNRL_EA_PARAM_8 este tipul de amenințare (type). • GNRL_EA_PARAM_9 sunt informații suplimentare despre obiectul detectat: Componenta aplicației (engine). Tehnologii de detectare a amenințărilor (method). Amenințare detectată de Kaspersky Private Security Network (blacklist): true sau false. Versiunea EDR. Identificator amenințare în EDR. Codul hash MD5 al obiectului.
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Object disinfected

Stare	⚠
Componentă	File Threat Protection Mail Threat Protection Host Intrusion Prevention Scanare malware
ID eveniment Windows	306

ID eveniment Kaspersky Security Center	GNRL_EV_OBJECT_CURED
Parametri eveniment	• GNRL_EA_PARAM_1 este codul hash al obiectului (SHA256). • GNRL_EA_PARAM_2 este numele obiectului. • GNRL_EA_PARAM_5 este numele amenințării, în conformitate cu clasificarea Kaspersky, de exemplu, EICAR-Test-File. • GNRL_EA_PARAM_7 este numele utilizatorului sesiunii. • GNRL_EA_PARAM_8 este tipul de amenințare (type). • GNRL_EA_PARAM_9 sunt informații suplimentare despre obiectul detectat: Componenta aplicației (engine). Tehnologii de detectare a amenințărilor (method). Amenințare detectată de Kaspersky Private Security Network (blacklist): true sau false. Versiunea EDR. Identificator amenințare în EDR. Codul hash MD5 al obiectului.
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Object will be disinfected on restart

Stare	⚠
Componentă	Host Intrusion Prevention File Threat Protection Scanare malware
ID eveniment Windows	324
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Object will be deleted on restart

Stare	⚠
Componentă	Behavior Detection Anti-Cryptor Exploit Prevention Host Intrusion Prevention File Threat Protection Scanare malware
ID eveniment Windows	323
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Object deleted according to settings

Stare	⚠
Componentă	Mail Threat Protection
ID eveniment Windows	342
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Rollback completed

Stare	⚠
Componentă	File Threat Protection Behavior Detection Anti-Cryptor Exploit Prevention Scanare malware
ID eveniment Windows	455
ID eveniment Kaspersky Security Center	000001c7
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Object download was blocked

Stare	⚠
Componentă	Web Threat Protection
ID eveniment Windows	341
ID eveniment Kaspersky Security Center	GNRL_EV_OBJECT_BLOCKED
Parametri eveniment	• GNRL_EA_PARAM_1 este codul hash al obiectului (SHA256). • GNRL_EA_PARAM_2 este numele obiectului. • GNRL_EA_PARAM_5 este numele amenințării, în conformitate cu clasificarea Kaspersky, de exemplu, EICAR-Test-File. • GNRL_EA_PARAM_7 este numele utilizatorului sesiunii. • GNRL_EA_PARAM_8 este tipul de amenințare (type). • GNRL_EA_PARAM_9 sunt informații suplimentare despre obiectul detectat: Componenta aplicației (engine). Tehnologii de detectare a amenințărilor (method). Amenințare detectată de Kaspersky Private Security Network (blacklist): true sau false. Versiunea EDR. Identificator amenințare în EDR. Codul hash MD5 al obiectului.
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Keyboard authorization error

Stare	⚠
Componentă	BadUSB Attack Prevention
ID eveniment Windows	2052
ID eveniment Kaspersky Security Center	00000804
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

The object scan result has been sent to a third-party application

Stare	⚠
Componentă	Protecție AMSI
ID eveniment Windows	1512

ID eveniment Kaspersky Security Center	GNRL_EV_OBJECT_REPORTED
Parametri eveniment	• GNRL_EA_PARAM_1 este codul hash al obiectului (SHA256). • GNRL_EA_PARAM_2 este numele obiectului. • GNRL_EA_PARAM_5 este numele amenințării, în conformitate cu clasificarea Kaspersky, de exemplu, EICAR-Test-File. • GNRL_EA_PARAM_7 este numele utilizatorului sesiunii. • GNRL_EA_PARAM_8 este tipul de amenințare (type). • GNRL_EA_PARAM_9 sunt informații suplimentare despre obiectul detectat: Componenta aplicației (engine). Tehnologii de detectare a amenințărilor (method). Amenințare detectată de Kaspersky Private Security Network (blacklist): true sau false. Versiunea EDR. Identificator amenințare în EDR. Codul hash MD5 al obiectului.
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Task settings applied successfully

Stare	⚠
Componentă	Application Control
ID eveniment Windows	708
ID eveniment Kaspersky Security Center	000002c4
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Warning about undesirable content (local bases)

Stare	⚠
Componentă	Control Web
ID eveniment Windows	708
ID eveniment Kaspersky Security Center	GNRL_EV_WEB_URL_WARNING
Parametri eveniment	• GNRL_EA_PARAM_1 este adresa URL. • GNRL_EA_PARAM_2 este numele utilizatorului sesiunii. • GNRL_EA_PARAM_3 este numele regulii Web Control.
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Warning about undesirable content (KSN)

Stare	⚠
Componentă	Control Web
ID eveniment Windows	708
ID eveniment Kaspersky Security Center	GNRL_EV_WEB_URL_WARNING
Parametri eveniment	• GNRL_EA_PARAM_1 este adresa URL. • GNRL_EA_PARAM_2 este numele utilizatorului sesiunii. • GNRL_EA_PARAM_3 este numele regulii Web Control.
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Undesirable content was accessed after a warning

Stare	⚠
Componentă	Control Web
ID eveniment Windows	754
ID eveniment Kaspersky Security Center	000002f2
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Temporary access to the device activated

Stare	⚠
Componentă	Control dispozitive
ID eveniment Windows	803
ID eveniment Kaspersky Security Center	000002f2
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Operation canceled by the user

Stare	⚠
Componentă	Actualizează
ID eveniment Windows	1016
ID eveniment Kaspersky Security Center	000003f8
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

User has opted out of the encryption policy

Stare	⚠
Componentă	Criptare date
ID eveniment Windows	1306
ID eveniment Kaspersky Security Center	0000051a
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Interrupted applying file encryption / decryption rules

Stare	⚠
Componentă	Criptare date
ID eveniment Windows	903
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

File encryption / decryption interrupted

Stare	⚠
Componentă	Criptare date
ID eveniment Windows	914
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Device encryption / decryption interrupted

Stare	⚠
Componentă	Criptare date
ID eveniment Windows	1303
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Failed to install or upgrade Kaspersky Disk Encryption drivers in the WinRE image

Stare	⚠
Componentă	Criptare date
ID eveniment Windows	1345
ID eveniment Kaspersky Security Center	00000541
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Module signature check failed

Stare	⚠
Componentă	Verificare integritate sistem
ID eveniment Windows	2002
ID eveniment Kaspersky Security Center	000007d2
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Application startup was blocked

Stare	⚠
Componentă	Endpoint Sensor
ID eveniment Windows	2105
ID eveniment Kaspersky Security Center	00000839
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Document opening was blocked

Stare	⚠
Componentă	Endpoint Sensor
ID eveniment Windows	2106
ID eveniment Kaspersky Security Center	0000083a
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Process was terminated by the Kaspersky Anti Targeted Attack Platform server administrator

Stare	⚠
Componentă	Endpoint Sensor
ID eveniment Windows	2112
ID eveniment Kaspersky Security Center	00000840
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

The application was terminated by the Kaspersky Anti Targeted Attack Platform server administrator

Stare	⚠
Componentă	Endpoint Sensor
ID eveniment Windows	2113
ID eveniment Kaspersky Security Center	00000841
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

File or stream was deleted by the Kaspersky Anti Targeted Attack Platform server administrator

Stare	⚠
Componentă	Endpoint Sensor
ID eveniment Windows	2111
ID eveniment Kaspersky Security Center	0000083f
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

File was restored from quarantine on the Kaspersky Anti Targeted Attack Platform server by the administrator

Stare	⚠
Componentă	Endpoint Sensor
ID eveniment Windows	2110
ID eveniment Kaspersky Security Center	0000083e
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

File was quarantined on the Kaspersky Anti Targeted Attack Platform server by the administrator

Stare	⚠
Componentă	Endpoint Sensor
ID eveniment Windows	2109
ID eveniment Kaspersky Security Center	0000083d
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Network activity of all third-party applications is blocked

Stare	⚠
Componentă	Endpoint Sensor
ID eveniment Windows	2107
ID eveniment Kaspersky Security Center	0000083b
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Network activity of all third-party applications is unblocked

Stare	⚠
Componentă	Endpoint Sensor
ID eveniment Windows	2108
ID eveniment Kaspersky Security Center	0000083c
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Object will be deleted after restart (Sandbox)

Stare	⚠
Componentă	Sandbox
ID eveniment Windows	2605
ID eveniment Kaspersky Security Center	00000a2d
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Total size of scan tasks exceeded the limit

Stare	⚠
Componentă	Sandbox
ID eveniment Windows	2612
ID eveniment Kaspersky Security Center	00000a34
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Object startup allowed, event logged

Stare	⚠
Componentă	Endpoint Detection and Response
ID eveniment Windows	2553
ID eveniment Kaspersky Security Center	000009fa
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Process startup allowed, event logged

Stare	⚠
Componentă	Endpoint Detection and Response
ID eveniment Windows	2554
ID eveniment Kaspersky Security Center	000009f8
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Object will be deleted after restart (Endpoint Detection and Response)

Stare	⚠
Componentă	Endpoint Detection and Response
ID eveniment Windows	2558
ID eveniment Kaspersky Security Center	000009fe
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Network isolation

Stare	⚠
Componentă	Endpoint Detection and Response
ID eveniment Windows	2700
ID eveniment Kaspersky Security Center	00000a8c
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Termination of network isolation

Stare	⚠
Componentă	Endpoint Detection and Response
ID eveniment Windows	2701
ID eveniment Kaspersky Security Center	00000a8d
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Restart required to complete the task

Stare	⚠
Componentă	Auditare sistem
ID eveniment Windows	225
ID eveniment Kaspersky Security Center	0000057b
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Application startup blockage message to administrator

Stare	⚠
Componentă	Application Control
ID eveniment Windows	503
ID eveniment Kaspersky Security Center	GNRL_EV_AC_USER_REQUEST
Parametri eveniment	• GNRL_EA_DESCRIPTION este mesajul către utilizator. • GNRL_EA_PARAM_2 este numele utilizatorului sesiunii. • GNRL_EA_PARAM_6 este numele fișierului executabil al aplicației (de exemplu, chrome.exe). • GNRL_EA_PARAM_7 este calea către fișierul executabil. • GNRL_EA_PARAM_8 este codul hash al obiectului (SHA256). • GNRL_EA_PARAM_9 este versiunea aplicației pe care utilizatorul încearcă să o execute.
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Device access blockage message to administrator

Stare	⚠
Componentă	Control dispozitive
ID eveniment Windows	804
ID eveniment Kaspersky Security Center	GNRL_EV_DC_USER_REQUEST
Parametri eveniment	• c_er_descr este mesajul către utilizator. • GNRL_EA_PARAM_1 este ID-ul hardware (HWID). • GNRL_EA_PARAM_2 este numele utilizatorului sesiunii.
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Web page access blockage message to administrator

Stare	⚠
Componentă	Control Web
ID eveniment Windows	755
ID eveniment Kaspersky Security Center	GNRL_EV_WC_USER_REQUEST
Parametri eveniment	• GNRL_EA_DESCRIPTION este mesajul către utilizator. • GNRL_EA_PARAM_1 este adresa URL. • GNRL_EA_PARAM_2 este numele utilizatorului sesiunii.
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Device connection blocked

Stare	⚠
Componentă	Control dispozitive
ID eveniment Windows	807
ID eveniment Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
Parametri eveniment	• GNRL_EA_PARAM_1 este ID-ul hardware (HWID). • GNRL_EA_PARAM_2 este numele utilizatorului sesiunii.
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Application activity blockage message to administrator

Stare	⚠
Componentă	File Integrity Monitor
ID eveniment Windows	2901
ID eveniment Kaspersky Security Center	00000b55
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Stare	⚠
Componentă	File Integrity Monitor
ID eveniment Windows	2900
ID eveniment Kaspersky Security Center	00000b54
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Stare	⚠
Componentă	Control adaptiv al anomaliilor
ID eveniment Windows	503
ID eveniment Kaspersky Security Center	GNRL_EV_ADSEC_USER_REQUEST
Parametri eveniment	• GNRL_EA_DESCRIPTION este mesajul către utilizator. • GNRL_EA_PARAM_1 este numele regulii Control adaptiv al anomaliilor. • GNRL_EA_PARAM_2 este ID-ul regulii euristice. • GNRL_EA_PARAM_3 este numele utilizatorului sesiunii. • GNRL_EA_PARAM_4 este procesul sursă. • GNRL_EA_PARAM_5 este obiectul sursă. • GNRL_EA_PARAM_6 este procesul țintă. • GNRL_EA_PARAM_7 este obiectul țintă. • GNRL_EA_PARAM_8 sunt informații suplimentare despre obiectul detectat: Codurile hash ale procesului/obiectului sursă și ale procesului/obiectului țintă. Proces blocat (verdict_type): true sau false. ID securitate utilizator (SID).
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Starting the cloud service client application is blocked

Stare	⚠
Componentă	Cloud Discovery
ID eveniment Windows	2212
ID eveniment Kaspersky Security Center	000008a4
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Access to the cloud service is blocked

Stare	⚠
Componentă	Cloud Discovery
ID eveniment Windows	2213
ID eveniment Kaspersky Security Center	000008a5
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

File or folder change was detected

Stare	ⓘ / ⚠ / ⓔ
Componentă	Monitorizare integritate sistem
ID eveniment Windows	2950
ID eveniment Kaspersky Security Center	00000b86
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Pentru a configura perioada de păstrare pentru acest eveniment, accesează secțiunea **Event configuration** a politicii și setează perioada de păstrare pentru evenimentul Monitorizare integritate sistem general – *File or folder change was detected*.

Object changes too often. Event aggregation started

Stare	ⓘ / ⚠ / ⓔ
Componentă	Monitorizare integritate sistem
ID eveniment Windows	2955
ID eveniment Kaspersky Security Center	00000b8b
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Report on object modification for the aggregation period

Stare	ⓘ / ⚠ / ⓔ
Componentă	Monitorizare integritate sistem
ID eveniment Windows	2956
ID eveniment Kaspersky Security Center	00000b8c
Jurnal de evenimente Windows (implicit)	–

Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Pentru a configura perioada de păstrare pentru acest eveniment, accesează secțiunea **Event configuration** a politicii și setează perioada de păstrare pentru evenimentul Monitorizare integritate sistem general – *File or folder change was detected*.

Registry change was detected

Stare	ⓘ / ⚠ / ⓔ
Componentă	Monitorizare integritate sistem
ID eveniment Windows	2951
ID eveniment Kaspersky Security Center	00000b87
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Pentru a configura perioada de păstrare pentru acest eveniment, accesează secțiunea **Event configuration** a politicii și setează perioada de păstrare pentru evenimentul Monitorizare integritate sistem general – *File or folder change was detected*.

Device connection / disconnection is detected

Stare	ⓘ / ⚠ / ⓔ
Componentă	Monitorizare integritate sistem
ID eveniment Windows	2952
ID eveniment Kaspersky Security Center	00000b88
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Pentru a configura perioada de păstrare pentru acest eveniment, accesează secțiunea **Event configuration** a politicii și setează perioada de păstrare pentru evenimentul Monitorizare integritate sistem general – *File or folder change was detected*.

Domeniul de monitorizare include obiecte incorecte

Stare	ⓘ / ⚠ / ⓔ
Componentă	Monitorizare integritate sistem
ID eveniment Windows	2903
ID eveniment Kaspersky Security Center	00000b89
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Pentru a configura perioada de păstrare pentru acest eveniment, accesează secțiunea **Event configuration** a politicii și setează perioada de păstrare pentru evenimentul Monitorizare integritate sistem general – *File or folder change was detected*.

The prohibited operation was allowed in test mode

Stare	⚠
Componentă	Monitorizare integritate sistem
ID eveniment Windows	2961
ID eveniment Kaspersky Security Center	00000b91
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Nu s-a putut realiza conexiunea la Serverul de integrare pentru mai mult de 30 de minute. Verifică starea Serverului de integrare și setările rețelei

Stare	⚠
Componentă	Light Agent
ID eveniment Windows	3102
ID eveniment Kaspersky Security Center	00000c1e
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Nu se poate conecta la Serverul de integrare. Verifică starea Serverului de integrare și setările rețelei

Stare	⚠
Componentă	Light Agent
ID eveniment Windows	3101
ID eveniment Kaspersky Security Center	00000c1d
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Șablonul mașinii virtuale trebuie actualizat

Stare	⚠
Componentă	Light Agent
ID eveniment Windows	3181
ID eveniment Kaspersky Security Center	00000c6d
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

The Standard license is terminated. The application is running under the Enterprise license

Stare	⚠
Componentă	Light Agent
ID eveniment Windows	3171
ID eveniment Kaspersky Security Center	00000c64
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Mesaj de informare

Application started

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	235
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Application stopped

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	236
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Self-Defense restricted access to the protected resource

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	213
ID eveniment Kaspersky Security Center	000000d5
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Report cleared

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	217
ID eveniment Kaspersky Security Center	000000d9
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Group policy disabled

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	220

ID eveniment Kaspersky Security Center	000000dc
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Application settings changed

Stare	
Componentă	Auditare sistem
ID eveniment Windows	218
ID eveniment Kaspersky Security Center	000000da
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Task started

Stare	
Componentă	Auditare sistem
ID eveniment Windows	221
ID eveniment Kaspersky Security Center	000000dd
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Task completed

Stare	
Componentă	Auditare sistem
ID eveniment Windows	223
ID eveniment Kaspersky Security Center	000000df
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

All application components that are defined by the license have been installed and run in normal mode

Stare	
Componentă	Auditare sistem
ID eveniment Windows	227
ID eveniment Kaspersky Security Center	000000e3
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Subscription settings have changed

Stare	
Componentă	Auditare sistem
ID eveniment Windows	238

ID eveniment Kaspersky Security Center	000000ee
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Subscription has been renewed

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	239
ID eveniment Kaspersky Security Center	000000ef
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Object restored from Backup

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	335
ID eveniment Kaspersky Security Center	0000014f
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

User name and password input

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	2000
ID eveniment Kaspersky Security Center	000007d0
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Participation in KSN enabled

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	2020
ID eveniment Kaspersky Security Center	000007e4
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

KSN servers available

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	2022

ID eveniment Kaspersky Security Center	000007e6
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

The application works and processes data under relevant laws and uses the appropriate infrastructure

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	2024
ID eveniment Kaspersky Security Center	000007e8
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Object restored from Quarantine

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	345
ID eveniment Kaspersky Security Center	00000159
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Object deleted from Quarantine

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	347
ID eveniment Kaspersky Security Center	0000015b
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

A backup copy of the object was created

Stare	ⓘ
Componentă	File Threat Protection Mail Threat Protection Behavior Detection Anti-Cryptor Host Intrusion Prevention Sandbox Scanare malware
ID eveniment Windows	308
ID eveniment Kaspersky Security Center	00000134
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Overwritten by a copy that was disinfected earlier

Stare	ⓘ
Componentă	File Threat Protection Host Intrusion Prevention Scanare malware
ID eveniment Windows	327
ID eveniment Kaspersky Security Center	00000147
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Password-protected archive detected

Stare	ⓘ
Componentă	File Threat Protection Web Threat Protection Mail Threat Protection Protecție AMSI Host Intrusion Prevention Scanare malware
ID eveniment Windows	322
ID eveniment Kaspersky Security Center	GNRL_EV_PASSWD_ARCHIVE_FOUND
Parametri eveniment	• GNRL_EA_PARAM_2 este numele obiectului. • GNRL_EA_PARAM_3 este data creării obiectului (opțional). • GNRL_EA_PARAM_7 este numele utilizatorului sesiunii. • GNRL_EA_PARAM_9 sunt informații suplimentare despre obiectul detectat: Componenta aplicației (engine). Tehnologii de detectare a amenințărilor (method). Amenințare detectată de Private KSN (listă de respinse): true vsau fals.
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Information about detected object

Stare	ⓘ
Componentă	File Threat Protection Web Threat Protection Mail Threat Protection Protecție AMSI Host Intrusion Prevention Scanare malware
ID eveniment Windows	332
ID eveniment Kaspersky Security Center	0000014c
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

The object is in the Kaspersky Private Security Network allowlist

Stare	ⓘ
Componentă	File Threat Protection Web Threat Protection Mail Threat Protection Protecție AMSI Host Intrusion Prevention Scanare malware
ID eveniment Windows	340

ID eveniment Kaspersky Security Center	00000154
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Object renamed

Stare	
Componentă	Mail Threat Protection Exploit Prevention Behavior Detection Anti-Cryptor Scanare malware
ID eveniment Windows	329
ID eveniment Kaspersky Security Center	00000149
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Object processed

Stare	
Componentă	Host Intrusion Prevention File Threat Protection Web Threat Protection Mail Threat Protection Scanare malware
ID eveniment Windows	301
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Object skipped

Stare	
Componentă	Host Intrusion Prevention File Threat Protection Protecție AMSI Scanare malware
ID eveniment Windows	315
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Archive detected

Stare	
Componentă	Host Intrusion Prevention File Threat Protection Web Threat Protection Mail Threat Protection Protecție AMSI Scanare malware
ID eveniment Windows	318

ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Packed object detected

Stare	ⓘ
Componentă	Host Intrusion Prevention File Threat Protection Web Threat Protection Mail Threat Protection Protecție AMSI Scanare malware
ID eveniment Windows	319
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Link processed

Stare	ⓘ
Componentă	Web Threat Protection
ID eveniment Windows	361
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Application startup allowed

Stare	ⓘ
Componentă	Application Control
ID eveniment Windows	701
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Update source is selected

Stare	ⓘ
Componentă	Actualizează
ID eveniment Windows	1001
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

S-a selectat serverul proxy

Stare	ⓘ
Componentă	Actualizează
ID eveniment Windows	1002
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

The link is in the Kaspersky Private Security Network allowlist

Stare	ⓘ
Componentă	Web Threat Protection
ID eveniment Windows	370
ID eveniment Kaspersky Security Center	00000172
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Application placed in the trusted group

Stare	ⓘ
Componentă	Host Intrusion Prevention
ID eveniment Windows	401
ID eveniment Kaspersky Security Center	00000191
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Application placed in restricted group

Stare	ⓘ
Componentă	Host Intrusion Prevention
ID eveniment Windows	402
ID eveniment Kaspersky Security Center	00000192
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Host Intrusion Prevention was triggered

Stare	ⓘ
Componentă	Host Intrusion Prevention
ID eveniment Windows	403
ID eveniment Kaspersky Security Center	00000193
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

File restored

Stare	ⓘ
Componentă	Behavior Detection Anti-Cryptor Exploit Prevention Host Intrusion Prevention
ID eveniment Windows	457
ID eveniment Kaspersky Security Center	000001c9
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Registry value restored

Stare	ⓘ
Componentă	Behavior Detection Exploit Prevention
ID eveniment Windows	458
ID eveniment Kaspersky Security Center	000001ca
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Registry value deleted

Stare	ⓘ
Componentă	Behavior Detection Exploit Prevention
ID eveniment Windows	459
ID eveniment Kaspersky Security Center	000001cb
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Process action skipped

Stare	ⓘ
Componentă	Control adaptiv al anomaliilor
ID eveniment Windows	2201
ID eveniment Kaspersky Security Center	GNRL_EV_ADSEC_DETECT
Parametri eveniment	• GNRL_EA_PARAM_1 este numele regulii Control adaptiv al anomaliilor. • GNRL_EA_PARAM_2 este ID-ul regulii euristice. • GNRL_EA_PARAM_3 este numele utilizatorului sesiunii. • GNRL_EA_PARAM_4 este procesul sursă. • GNRL_EA_PARAM_5 este obiectul sursă. • GNRL_EA_PARAM_6 este procesul țintă. • GNRL_EA_PARAM_7 este obiectul țintă. • GNRL_EA_PARAM_8 sunt informații suplimentare despre obiectul detectat: Codurile hash ale procesului/obiectului sursă și ale procesului/obiectului țintă. Proces blocat (verdict_type): true sau false. ID securitate utilizator (SID).
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Keyboard authorized

Stare	ⓘ
Componentă	BadUSB Attack Prevention
ID eveniment Windows	2050
ID eveniment Kaspersky Security Center	00000802
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Network activity allowed

Stare	ⓘ
Componentă	Firewall
ID eveniment Windows	601
ID eveniment Kaspersky Security Center	00000259
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Application startup prohibited in test mode

Stare	ⓘ
Componentă	Application Control
ID eveniment Windows	703
ID eveniment Kaspersky Security Center	GNRL_EV_APP_LAUNCH_TESTED_DENIED
Parametri eveniment	• GNRL_EA_PARAM_2 este numele utilizatorului sesiunii. • GNRL_EA_PARAM_3 este identificatorul categoriei creat manual. • GNRL_EA_PARAM_4 este identificatorul de securitate al contului (SID). • GNRL_EA_PARAM_5 sunt informații despre semnătura digitală a aplicației. • GNRL_EA_PARAM_6 este numele fișierului executabil al aplicației (de exemplu, chrome.exe). • GNRL_EA_PARAM_7 este calea către fișierul executabil. • GNRL_EA_PARAM_8 este codul hash al obiectului (SHA256). • GNRL_EA_PARAM_9 este versiunea aplicației pe care utilizatorul încearcă să o execute.
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Application startup allowed in test mode

Stare	ⓘ
Componentă	Application Control
ID eveniment Windows	704
ID eveniment Kaspersky Security Center	GNRL_EV_APP_LAUNCH_TESTED_ALLOW
Parametri eveniment	• GNRL_EA_PARAM_2 este numele utilizatorului sesiunii. • GNRL_EA_PARAM_3 este identificatorul categoriei creat manual. • GNRL_EA_PARAM_4 este identificatorul de securitate al contului (SID). • GNRL_EA_PARAM_5 sunt informații despre semnătura digitală a aplicației.
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

A page that is allowed was opened

Stare	
Componentă	Control Web
ID eveniment Windows	751
ID eveniment Kaspersky Security Center	000002f4
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Operation with the device allowed

Stare	
Componentă	Control dispozitive
ID eveniment Windows	801
ID eveniment Kaspersky Security Center	00000321
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

File operation performed

Stare	
Componentă	Control dispozitive
ID eveniment Windows	808
ID eveniment Kaspersky Security Center	GNRL_EV_USB_FILE_OPERATION
Parametri eveniment	• GNRL_EA_PARAM_1 este operațiunea cu fișiere (scriere sau ștergere). • GNRL_EA_PARAM_2 este calea către fișier. • GNRL_EA_PARAM_3 este numele dispozitivului. • GNRL_EA_PARAM_4 este numele utilizatorului sesiunii. • GNRL_EA_PARAM_5 este ID-ul hardware (HWID).
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

No available updates

Stare	
Componentă	Actualizează
ID eveniment Windows	1020
ID eveniment Kaspersky Security Center	000003fc
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Update distribution completed successfully

Stare	
Componentă	Actualizează
ID eveniment Windows	1022
ID eveniment Kaspersky Security Center	000003fe

Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Downloading files

Stare	ⓘ
Componentă	Actualizează
ID eveniment Windows	1003
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

File downloaded

Stare	ⓘ
Componentă	Actualizează
ID eveniment Windows	1004
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

File installed

Stare	ⓘ
Componentă	Actualizează
ID eveniment Windows	1005
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

File updated

Stare	ⓘ
Componentă	Actualizează
ID eveniment Windows	1006
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

File rolled back due to update error

Stare	ⓘ
Componentă	Actualizează
ID eveniment Windows	1007
ID eveniment Kaspersky Security Center	–

Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Updating files

Stare	ⓘ
Componentă	Actualizează
ID eveniment Windows	1008
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Distributing updates

Stare	ⓘ
Componentă	Actualizează
ID eveniment Windows	1009
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Rolling back files

Stare	ⓘ
Componentă	Actualizează
ID eveniment Windows	1010
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Creating the list of files to download

Stare	ⓘ
Componentă	Actualizează
ID eveniment Windows	1013
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Downloading patches

Stare	ⓘ
Componentă	Actualizează
ID eveniment Windows	2150
ID eveniment Kaspersky Security Center	–

Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Installing patch

Stare	ⓘ
Componentă	Actualizează
ID eveniment Windows	2151
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Patch installed

Stare	ⓘ
Componentă	Actualizează
ID eveniment Windows	2152
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Rolling back patch

Stare	ⓘ
Componentă	Actualizează
ID eveniment Windows	2154
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Patch rolled back

Stare	ⓘ
Componentă	Actualizează
ID eveniment Windows	2155
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Started applying file encryption / decryption rules

Stare	ⓘ
Componentă	Criptare date
ID eveniment Windows	901
ID eveniment Kaspersky Security Center	00000385

Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Finished applying file encryption / decryption rules

Stare	ⓘ
Componentă	Criptare date
ID eveniment Windows	902
ID eveniment Kaspersky Security Center	00000386
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Resumed applying file encryption / decryption rules

Stare	ⓘ
Componentă	Criptare date
ID eveniment Windows	905
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

File encryption / decryption started

Stare	ⓘ
Componentă	Criptare date
ID eveniment Windows	910
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

File encryption / decryption completed

Stare	ⓘ
Componentă	Criptare date
ID eveniment Windows	911
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

File has not been encrypted because it is an exclusion

Stare	ⓘ
Componentă	Criptare date
ID eveniment Windows	913
ID eveniment Kaspersky Security Center	–

Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Portable mode enabled

Stare	ⓘ
Componentă	Criptare date
ID eveniment Windows	950
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Portable mode disabled

Stare	ⓘ
Componentă	Criptare date
ID eveniment Windows	952
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Device encryption / decryption started

Stare	ⓘ
Componentă	Criptare date
ID eveniment Windows	1301
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Device encryption / decryption completed

Stare	ⓘ
Componentă	Criptare date
ID eveniment Windows	1302
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Device encryption / decryption resumed

Stare	ⓘ
Componentă	Criptare date
ID eveniment Windows	1304
ID eveniment Kaspersky Security Center	–

Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Device is not encrypted

Stare	ⓘ
Componentă	Criptare date
ID eveniment Windows	1307
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Device encryption / decryption process has been switched to active mode

Stare	ⓘ
Componentă	Criptare date
ID eveniment Windows	1308
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Device encryption / decryption process has been switched to passive mode

Stare	ⓘ
Componentă	Criptare date
ID eveniment Windows	1309
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Encryption module loaded

Stare	ⓘ
Componentă	Criptare date
ID eveniment Windows	1310
ID eveniment Kaspersky Security Center	0000051e
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

New Authentication Agent account created

Stare	ⓘ
Componentă	Criptare date
ID eveniment Windows	1330
ID eveniment Kaspersky Security Center	00000532

Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Authentication Agent account deleted

Stare	
Componentă	Criptare date
ID eveniment Windows	1331
ID eveniment Kaspersky Security Center	00000533
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Authentication Agent account password changed

Stare	
Componentă	Criptare date
ID eveniment Windows	1332
ID eveniment Kaspersky Security Center	00000534
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Successful Authentication Agent login

Stare	
Componentă	Criptare date
ID eveniment Windows	1333
ID eveniment Kaspersky Security Center	00000535
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Failed Authentication Agent login attempt

Stare	
Componentă	Criptare date
ID eveniment Windows	1334
ID eveniment Kaspersky Security Center	00000536
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Hard drive accessed using the procedure of requesting access to encrypted devices

Stare	
Componentă	Criptare date
ID eveniment Windows	1335
ID eveniment Kaspersky Security Center	00000537

Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Failed attempt to access the hard drive using the procedure of requesting access to encrypted devices

Stare	
Componentă	Criptare date
ID eveniment Windows	1336
ID eveniment Kaspersky Security Center	00000538
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Account was not added. This account already exists

Stare	
Componentă	Criptare date
ID eveniment Windows	1337
ID eveniment Kaspersky Security Center	00000539
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Account was not modified. This account does not exist

Stare	
Componentă	Criptare date
ID eveniment Windows	1338
ID eveniment Kaspersky Security Center	0000053a
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Account was not deleted. This account does not exist

Stare	
Componentă	Criptare date
ID eveniment Windows	1339
ID eveniment Kaspersky Security Center	0000053b
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

FDE upgrade successful

Stare	
Componentă	Criptare date
ID eveniment Windows	1341
ID eveniment Kaspersky Security Center	0000053d

Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

FDE upgrade rollback successful

Stare	ⓘ
Componentă	Criptare date
ID eveniment Windows	1343
ID eveniment Kaspersky Security Center	0000053f
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Failed to uninstall Kaspersky Disk Encryption drivers from the WinRE image

Stare	ⓘ
Componentă	Criptare date
ID eveniment Windows	1346
ID eveniment Kaspersky Security Center	00000542
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

BitLocker recovery key was changed

Stare	ⓘ
Componentă	Criptare date
ID eveniment Windows	1370
ID eveniment Kaspersky Security Center	0000055a
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

BitLocker password / PIN was changed

Stare	ⓘ
Componentă	Criptare date
ID eveniment Windows	1371
ID eveniment Kaspersky Security Center	0000055b
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

BitLocker recovery key was saved to a removable drive

Stare	ⓘ
Componentă	Criptare date
ID eveniment Windows	1372
ID eveniment Kaspersky Security Center	0000055c

Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Processing of tasks from the Kaspersky Anti Targeted Attack Platform server is inactive

Stare	ⓘ
Componentă	Endpoint Sensor
ID eveniment Windows	2103
ID eveniment Kaspersky Security Center	00000837
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Endpoint Sensor connected to server

Stare	ⓘ
Componentă	Endpoint Sensor
ID eveniment Windows	2101
ID eveniment Kaspersky Security Center	00000835
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Connection to the Kaspersky Anti Targeted Attack Platform server restored

Stare	ⓘ
Componentă	Endpoint Sensor
ID eveniment Windows	2102
ID eveniment Kaspersky Security Center	00000836
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Tasks from the Kaspersky Anti Targeted Attack Platform server are being processed

Stare	ⓘ
Componentă	Endpoint Sensor
ID eveniment Windows	2104
ID eveniment Kaspersky Security Center	00000838
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Object deleted

Stare	ⓘ
Componentă	Ștergere date
ID eveniment Windows	2251
ID eveniment Kaspersky Security Center	000008cb

Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Wipe task statistics

Stare	ⓘ
Componentă	Endpoint Detection and Response Expert (on-premises)
ID eveniment Windows	2853
ID eveniment Kaspersky Security Center	00000b25
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Stare	ⓘ
Componentă	Ștergere date
ID eveniment Windows	2253
ID eveniment Kaspersky Security Center	000008cd
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Object quarantined (Sandbox)

Stare	ⓘ
Componentă	Sandbox
ID eveniment Windows	2602
ID eveniment Kaspersky Security Center	00000a2a
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Object deleted (Sandbox)

Stare	ⓘ
Componentă	Sandbox
ID eveniment Windows	2604
ID eveniment Kaspersky Security Center	00000a2c
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

IOC Scan started

Stare	ⓘ
Componentă	Endpoint Detection and Response
ID eveniment Windows	2652
ID eveniment Kaspersky Security Center	00000a5c
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

IOC Scan completed

Stare	ⓘ
Componentă	Endpoint Detection and Response
ID eveniment Windows	2653
ID eveniment Kaspersky Security Center	00000a5d
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Object quarantined (Endpoint Detection and Response)

Stare	ⓘ
Componentă	Endpoint Detection and Response
ID eveniment Windows	2555
ID eveniment Kaspersky Security Center	000009fb
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Object deleted (Endpoint Detection and Response)

Stare	ⓘ
Componentă	Endpoint Detection and Response
ID eveniment Windows	2557
ID eveniment Kaspersky Security Center	000009fd
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Application components successfully changed

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	1402
ID eveniment Kaspersky Security Center	0000057a
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Stare	ⓘ
Componentă	Sandbox
ID eveniment Windows	2606
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Stare	ⓘ
Componentă	Sandbox
ID eveniment Windows	2609
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Stare	ⓘ
Componentă	Sandbox
ID eveniment Windows	2610
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Stare	ⓘ
Componentă	Sandbox
ID eveniment Windows	2616
ID eveniment Kaspersky Security Center	–
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	–

Serverul de administrare la care este conectat dispozitivul tău este setat ca fiind de încredere

Stare	ⓘ
Componentă	Protecție conexiune Server de administrare
ID eveniment Windows	3300
ID eveniment Kaspersky Security Center	00000ce4
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Dispozitivultău este conectat la un nou Server de administrare de încredere

Stare	ⓘ
Componentă	Protecție conexiune Server de administrare
ID eveniment Windows	3302
ID eveniment Kaspersky Security Center	00000ce6
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Serverul de administrare la care este conectat dispozitivul tău nu mai este setat ca fiind de încredere

Stare	ⓘ
Componentă	Protecție conexiune Server de administrare
ID eveniment Windows	3303

ID eveniment Kaspersky Security Center	00000ce7
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Asynchronous Sandbox detection

Stare	ⓘ
Componentă	Sandbox
ID eveniment Windows	2619
ID eveniment Kaspersky Security Center	GNRL_EV_APP_INCIDENT_OCCURED
Parametri eveniment	• GNRL_EA_PARAM_1 sunt parametrii componentelor Sandbox. • GNRL_EA_PARAM_2 este calea către obiect. • GNRL_EA_PARAM_3 este ID-ul incidentului. • GNRL_EA_PARAM_4 este codul hash al obiectului (SHA256).
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

The scan task has been successfully sent to Sandbox by a user

Stare	ⓘ
Componentă	Sandbox
ID eveniment Windows	2622
ID eveniment Kaspersky Security Center	00000a3e
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Device is connected

Stare	ⓘ
Componentă	Control dispozitive
ID eveniment Windows	805
ID eveniment Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUGGED
Parametri eveniment	• GNRL_EA_PARAM_1 este ID-ul hardware (HWID). • GNRL_EA_PARAM_2 este numele utilizatorului sesiunii.
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Device is disconnected

Stare	ⓘ
Componentă	Control dispozitive
ID eveniment Windows	806
ID eveniment Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_UNPLUGGED
Parametri eveniment	• GNRL_EA_PARAM_1 este ID-ul hardware (HWID). • GNRL_EA_PARAM_2 este numele utilizatorului sesiunii.
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Error removing the previous version of the application

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	246
ID eveniment Kaspersky Security Center	000000f6
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Successful connection to the EDR Expert server

Stare	ⓘ
Componentă	Endpoint Detection and Response Expert (on-premises)
ID eveniment Windows	2853
ID eveniment Kaspersky Security Center	00000b25
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Conectare reușit la serverul de răspuns EDR Expert

Stare	ⓘ
Componentă	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID eveniment Windows	2853
ID eveniment Kaspersky Security Center	00000b25
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Conectare reușită la serverul de colectare a telemetriei EDR Expert

Stare	ⓘ
Componentă	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID eveniment Windows	2857
ID eveniment Kaspersky Security Center	00000b26
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Conectare reușită la serverul NDR

Stare	ⓘ
Componentă	Network Detection and Response (KATA)
ID eveniment Windows	3083
ID eveniment Kaspersky Security Center	00000c0b

Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Starting the cloud service client application is allowed

Stare	ⓘ
Componentă	Cloud Discovery
ID eveniment Windows	2210
ID eveniment Kaspersky Security Center	000008a2
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Access to the cloud service is allowed

Stare	ⓘ
Componentă	Cloud Discovery
ID eveniment Windows	2211
ID eveniment Kaspersky Security Center	000008a3
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Acces la zona protejată

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	2004
ID eveniment Kaspersky Security Center	000007d4
Jurnal de evenimente Windows (implicit)	✓
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

File or folder change was detected

Stare	ⓘ / ⚠ / !
Componentă	Monitorizare integritate sistem
ID eveniment Windows	2950
ID eveniment Kaspersky Security Center	00000b86
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Pentru a configura perioada de păstrare pentru acest eveniment, accesează secțiunea **Event configuration** a politicii și setează perioada de păstrare pentru evenimentul Monitorizare integritate sistem general – *File or folder change was detected*.

Object changes too often. Event aggregation started

Stare	/ /
Componentă	Monitorizare integritate sistem
ID eveniment Windows	2955
ID eveniment Kaspersky Security Center	00000b8b
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Report on object modification for the aggregation period

Stare	/ /
Componentă	Monitorizare integritate sistem
ID eveniment Windows	2956
ID eveniment Kaspersky Security Center	00000b8c
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Pentru a configura perioada de păstrare pentru acest eveniment, accesează secțiunea **Event configuration** a politicii și setează perioada de păstrare pentru evenimentul Monitorizare integritate sistem general – *File or folder change was detected*.

Registry change was detected

Stare	/ /
Componentă	Monitorizare integritate sistem
ID eveniment Windows	2951
ID eveniment Kaspersky Security Center	00000b87
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Pentru a configura perioada de păstrare pentru acest eveniment, accesează secțiunea **Event configuration** a politicii și setează perioada de păstrare pentru evenimentul Monitorizare integritate sistem general – *File or folder change was detected*.

Device connection / disconnection is detected

Stare	/ /
Componentă	Monitorizare integritate sistem
ID eveniment Windows	2952
ID eveniment Kaspersky Security Center	00000b88
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Pentru a configura perioada de păstrare pentru acest eveniment, accesează secțiunea **Event configuration** a politicii și setează perioada de păstrare pentru evenimentul Monitorizare integritate sistem general – *File or folder change was detected*.

Domeniul de monitorizare include obiecte incorecte

Stare	ⓘ / ⚠ / ⓘ
Componentă	Monitorizare integritate sistem
ID eveniment Windows	2903
ID eveniment Kaspersky Security Center	00000b89
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Pentru a configura perioada de păstrare pentru acest eveniment, accesează secțiunea **Event configuration** a politicii și setează perioada de păstrare pentru evenimentul Monitorizare integritate sistem general – *File or folder change was detected*.

Baseline created

Stare	ⓘ
Componentă	Monitorizare integritate sistem
ID eveniment Windows	2957
ID eveniment Kaspersky Security Center	00000b8d
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Baseline updated

Stare	ⓘ
Componentă	Monitorizare integritate sistem
ID eveniment Windows	2958
ID eveniment Kaspersky Security Center	00000b8e
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

An operation is performed by the trusted user

Stare	ⓘ
Componentă	Monitorizare integritate sistem
ID eveniment Windows	2962
ID eveniment Kaspersky Security Center	00000b92
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Pentru a configura perioada de păstrare pentru acest eveniment, accesează secțiunea **Event configuration** a politicii și setează perioada de păstrare pentru evenimentul Monitorizare integritate sistem general – *File or folder change was detected*.

Connected to SVM

Stare	ⓘ
Componentă	Light Agent

ID eveniment Windows	3152
ID eveniment Kaspersky Security Center	00000c50
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

A new temporary password was created

Stare	ⓘ
Componentă	Auditare sistem
ID eveniment Windows	265
ID eveniment Kaspersky Security Center	00000109
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Connected to the Integration Server

Stare	ⓘ
Componentă	Light Agent
ID eveniment Windows	3105
ID eveniment Kaspersky Security Center	00000c21
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Restoring connection to the Integration Server

Stare	ⓘ
Componentă	Light Agent
ID eveniment Windows	3104
ID eveniment Kaspersky Security Center	00000c20
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Conectare reușită la serverul KUMA

Stare	ⓘ
Componentă	Integrare KUMA
ID eveniment Windows	2857
ID eveniment Kaspersky Security Center	00000b29
Jurnal de evenimente Windows (implicit)	–
Jurnal de evenimente Kaspersky Security Center (implicit)	✓

Anexa 7. Extensii de fișiere acceptate pentru prevenirea executării

Kaspersky Endpoint Security acceptă prevenirea deschiderii fișierelor în format office în anumite aplicații. Informațiile despre extensiile de fișiere și aplicațiile acceptate sunt listate în tabelul următor.

Extensii de fișiere acceptate pentru prevenirea executării

Nume aplicație	Executable file	Extensia fișierului
Microsoft Word	winword.exe	rtf doc dots 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

Nume aplicație	Executable file	Extensia fișierului
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	
Browser Tor	tor.exe	

Anexa 8. Interpreți de script acceptați pentru Prevenirea executării

Prevenirea executării acceptă următorii interpreți de script:

- 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

Prevenirea executării acceptă lucrul cu aplicații Java în mediul de execuție Java (procesele java.exe și javaw.exe).

Anexa 9. Domeniu de scanare IOC în registru (RegistryItem)

Când adaugi tipul de date **Windows registry - RegistryItem** la domeniul de scanare IOC, Kaspersky Endpoint Security scanează următoarele chei de registru în mod implicit:

```
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
```

Anexa 10. Cerințe privind fișierele IOC

Când creați activități de Scanare IOC, țineți cont de următoarele cerințe și limitări privind fișierul IOC:

- Aplicația acceptă fișiere IOC cu extensiile IOC și XML în standardul deschis OpenIOC versiunile 1.0 și 1.1 pentru descrierea indicatorilor de compromitere.
- După încărcarea fișierelor IOC, poți edita manual fișierele în editorul încorporat, direct în proprietățile activității. Kaspersky Endpoint Security acceptă editarea fișierelor IOC care sunt conforme cu standardul OpenIOC 1.1. Nu este posibilă modificarea conținutului fișierelor IOC compatibile cu OpenIOC versiunea 1.0.
- Dacă în timpul creării unei activități *IOC Scan* în linia de comandă, încărcați fișiere IOC, unele dintre acestea nefiind acceptate, atunci când activitatea este executată, aplicația utilizează numai fișierele IOC acceptate. Dacă în timpul creării unei activități *IOC Scan* în linia de comandă, toate fișierele IOC pe care le încarci rezultă că nu sunt acceptate, activitatea poate fi totuși executată, dar nu va detecta niciun indicator de compromitere. Nu este posibilă încărcarea fișierelor IOC neacceptate folosind Web Console sau Cloud Console.

- Erorile semantice și termenii și etichetele IOC neacceptate nu determină eșuarea executării activității. În astfel de secțiuni ale fișierelor IOC, aplicația nu detectează nicio potrivire.
- Identificatorii tuturor fișierelor IOC utilizați într-o activitate unică Scanare IOC trebuie să fie unici. Dacă există fișiere IOC cu același identificator, acest lucru ar putea afecta rezultatele executării activității.
- Un singur fișier IOC nu trebuie să aibă o dimensiune mai mare de 2 MO. Utilizarea unor fișiere mai mari va face ca activitatea Scanare IOC să se finalizeze cu o eroare. Dimensiunea totală a tuturor fișierelor adăugate la colecția IOC nu poate depăși 10 MO. Dacă dimensiunea totală a tuturor fișierelor depășește 10 MO, trebuie să divizați colecția IOC și să creați mai multe activități *IOC Scan*.
- Este recomandat să creați un fișier IOC per amenințare. Acest lucru facilitează analizarea rezultatelor activității *IOC Scan*.

Fișierul pe care îl puteți descărca făcând clic pe linkul de mai jos, conține un tabel cu lista completă a termenilor IOC din standardul OpenIOC.

DESCARCĂ FIȘIERUL IOC_TERMS.XLSX

Caracteristicile și limitările acceptării de către aplicație a standardului OpenIOC sunt prezentate în tabelul următor.

Caracteristicile și limitările acceptării OpenIOC versiunile 1.0 și 1.1.

Condiții acceptate	OpenIOC 1.0:
	
	`is`
	`isnot` (ca excepție de la set)
	`contains`
	`containsnot` (ca excepție de la set)
	OpenIOC 1.1:
	
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`
	
	Pentru termenii E-mail/*, sunt acceptate numai condițiile `contains` și `is`. Pentru ca funcția Scanare IOC retrospectivă să funcționeze corect, atunci când utilizezi condiția `is`, adresele de e-mail din fișierele IOC trebuie specificate în următorul format: `"name@example.org" <SMTP:name@example.org>`. Când se execută normal activitatea *Scanare IOC*, este suficient să specifici adresa de e-mail în următorul format: `name@example.org`.

Atribute condiție acceptate	OpenIOC 1.1:
	
	`preserve-case`
	`negate`

Operatori acceptați	`AND` `OR`
Tipuri de date acceptate	`"date"`: data (condiții aplicabile: `is`, `greater-than`, `less-than`) `"int"`: număr întreg (condiții aplicabile: `is`, `greater-than`, `less-than`) `"string"`: șir (condiții aplicabile: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"`: durata în secunde (condiții aplicabile: `is`, `greater-than`, `less-than`)

Caracteristici ale interpretării tipului de date	Tipurile de date `"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"` și `"base64Binary"` sunt interpretate ca șir.
	
	Aplicația acceptă interpretarea setării pentru `Content` pentru tipurile de date `int` și `date` când este setată sub formă de intervale:
	
	OpenIOC 1.0:
	Utilizarea operatorului `TO` în câmpul `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:
	Utilizarea condițiilor `greater-than` și `less-than`
	Utilizarea operatorului `TO` în câmpul `Content`
	Aplicația acceptă interpretarea tipurilor de date `date` și `duration` dacă indicatorii sunt setați în formatul `ISO 8601, Zulu time zone, UTC`.

Anexa 11. API pentru Răspunsul la amenințare EDR

Kaspersky Endpoint Security 12.9 for Windows introduce suport pentru acțiunile EDR Threat Response (EDR responses) folosind un Kaspersky Security Center OpenAPI. Adică, puteți folosi metode OpenAPI pentru a automatiza răspunsul la amenințările EDR folosind Python. Puteți folosi aceste metode atunci când sunt integrate cu soluțiile SIEM. *Kaspersky Unified Monitoring and Analysis Platform*, soluția Kaspersky SIEM, acceptă EDR Threat Response OpenAPI începând cu versiunea 3.4.1. Pentru scripturi de exemplu, vezi documentația KUMA.

Pentru a efectua acțiuni EDR Threat Response, trebuie să creezi o solicitare și să o trimiți folosind KSC Open API (`AddIncident`). După procesarea cererii, este creată o sarcină specială în consola Kaspersky Security Center.

Pentru a crea sarcini atunci când răspunzi la amenințările EDR, trebuie stabilită o conexiune de fundal între Serverul de administrare și Consola web Kaspersky Security Center. Serviciul de conectare în fundal este disponibil în Kaspersky Security Center Windows 14.2 sau o versiune ulterioară și în Kaspersky Security Center Linux 15.2 sau o versiune ulterioară. Alte console, inclusiv consolele soluțiilor Kaspersky Detection and Response, nu sunt acceptate.

Pentru EDR Threat Response, trebuie să specifici parametrii de bază de solicitare, de exemplu, în format JSON:

- `task` este tipul sarcinii (vezi mai jos).
- `targetHost` este ID-ul computerului pe care trebuie rulat scriptul. Argument obligatoriu. Scriptul primește acest argument de la eveniment.
- `responseEventIncidentArea` este numele aplicației care a rulat scriptul (de exemplu, `KUMA`). Acest parametru este adăugat la numele sarcinii create.

Pentru a configura EDR Threat Response, trebuie să specifici setările sarcinii în format JSON în parametrul `"KLINCDT_BODY": json.dumps(data)`. Ca rezultat, aplicația creează `[Response][KUMA] <task type> - <Date> <Time> - <ID>` în consola Kaspersky Security Center.

Conectarea la Kaspersky Security Center OpenAPI

Ca parte a EDR Threat Response, aplicația creează sarcini speciale în consola Kaspersky Security Center. Crearea acestor sarcini necesită stabilirea unei conexiuni între computer și Kaspersky Security Center. Pentru a realiza acest lucru, parametrii de conexiune Kaspersky Security Center trebuie să fie specificați în cerere.

În Kaspersky XDR versiunea 2.1, metoda de autorizare a solicitărilor s-a modificat. Kaspersky XDR folosește token-uri PAT în loc de autentificarea cu nume de utilizator și parolă. Prin urmare, nu este posibilă executarea de scripturi în Kaspersky XDR. Pentru mai multe detalii despre autorizarea solicitărilor, consultă Ajutor Kaspersky XDR.

Parametrii de conexiune Kaspersky Security Center

Parametru	Tip	Descriere
`kscHost`	`string`	Adresă a serverului de administrare Kaspersky Security Center. Parametru obligatoriu.
`kscPort`	`int`	Port de conectare la Serverul de administrare. Parametru obligatoriu.
`kscCert`	`string`	Calea către un fișier de certificat pentru conectarea la serverul de administrare Kaspersky Security Center. Implicit, parametrul este setat la `False`.
`kscUser`	`string`	Numele contului de utilizator. Parametru obligatoriu.
`kscPassword`	`string`	Parola contului de utilizator. Parametru obligatoriu.

Exemplu

```
# 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})
```

Datele contului de utilizator nu sunt protejate, prin urmare trebuie să aloci un utilizator separat care va fi folosit doar pentru a efectua aceste acțiuni.

Obținere fișier – getFile

Setări activitate Obținere fișier

Parametru	Tip	Descriere
`md5hash`	`string`	Hash MD5 al fișierului pe care vrei să îl obții.
`sha256hash`	`string`	SHA256 hash al fișierului pe care vrei să îl obții.
`path`	`string`	Calea către fișierul pe care vrei să îl obții.

Exemplu

```
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;
};
```

Șterge fișier – deleteFile

Setări activitate Șterge fișier

Parametru	Tip	Descriere
`md5hash`	`string`	Hash MD5 al fișierului pe care vrei să îl ștergi.
`sha256hash`	`string`	SHA256 hash al fișierului pe care vrei să îl ștergi.
`path`	`string`	Calea către fișierul pe care vrei să îl ștergi.
`searchInSubfolders?`	`boolean`	Caută fișierul pe care dorești să îl ștergi în sub-directoare.

Exemplu

```
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;
};
```

Mută fișierul în Carantină – quarantineFile

Setări activitate Mută fișierul în Carantină

Parametru	Tip	Descriere
`md5hash`	`string`	Hash MD5 al fișierului pe care vrei să îl pui în carantină.
`sha256hash`	`string`	Hash SHA256 al fișierului pe care vrei să îl pui în carantină.
`path`	`string`	Calea către fișierul pe care vrei să îl pui în carantină.

Exemplu

```
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;
};
```

Scanare IOC – iocScan

Setări activitate Scanare IOC

Parametru	Tip	Descriere
`ioc`	`string`	Calea către arhiva ZIP cu fișiere IOC pe care dorești să le utilizezi pentru scanare.
`isolateHost`	`boolean`	Izolează computerul de rețea atunci când este detectat un indicator de compromis pentru a preveni răspândirea amenințării.
`scanCriticalAreas`	`boolean`	Rulează sarcina *Scanare zone critice* atunci când este detectat un indicator de compromis.
`quarantineObject`	`boolean`	Șterge obiectul rău intenționat atunci când un indicator de compromis este detectat. Înainte de a șterge obiectul, Kaspersky Endpoint Security creează o copie de rezervă în caz că obiectul trebuie restaurat ulterior. Kaspersky Endpoint Security mută copia de rezervă în Carantină.

Exemplu

```
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;
};
```

Pornește procesul – startProcess

Setări activitate Pornește procesul

Parametru	Tip	Descriere
executablePath	string	Calea către fișierul executabil care este utilizat pentru a începe procesul.
arguments?	string	Argumente suplimentare ale liniei de comandă pentru pornirea procesului.
workingFolder?	string	Calea către folderul de lucru al procesului.

Exemplu

```
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;
};
```

Termină procesul – terminateProcess

Setări activitate Termină procesul

Parametru	Tip	Descriere
md5hash	string	Hash MD5 al fișierului al cărui proces vrei să îl închizi.
sha256hash	string	Hash SHA256 al fișierului al cărui proces vrei să îl închizi.
path	string	Calea către fișierul pe care vrei să îl ștergi.
caseSensitive	boolean	Sensibilitate la litere mari și mici la căutarea fișierului.

Exemplu

```
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;
};
```

Izolarea rețelei de computere – isolateHost

Setările izolării rețelei de computere

Parametru	Tip	Descriere
`action`	`string`	Modul de funcționare al izolării rețelei.

Exemplu

```
type isolateHost = {
  task: 'isolateHost';
  targetHost: string;
  params: {
    // 0 - turning off network isolation, 1 - turning on network isolation
    action: number;
  };
  responseEventIncidentArea: string;
};
```

Prevenirea executării – preventExecution

Setările pentru prevenirea executării

Parametru	Tip	Descriere
`hash`	`string`	Hash MD5 al fișierului pe care vrei să îl împiedici să ruleze.
`path`	`string`	Calea către fișierul pe care vrei să îl împiedici să ruleze.
`caseSensitive`	`boolean`	Sensibilitate la litere mari și mici la căutarea fișierului.

Exemplu

```
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;
};
```

Scanare malware – onDemandScan

Setări activitate Scanare malware

Parametru	Tip	Descriere
`path`	`string`	Listă de fișiere și foldere delimitate de spațiu pentru scanare personalizată.
`recursive`	`boolean`	Mod de scanare recursiv.

Parametru	Tip	Descriere
type	number	Domeniu de scanare.

```
ScanObjectType = Enum("ScanObjectType",
                      [
                          ("SystemMemory", 14),
                          ("StartupObjectsAndRunningProcesses", 15),
                          ("DiskBootSectors", 16),
                          ("SystemBackupStorage", 17),
                          ("Email", 18),
                          ("Folder", 22),
                          ("AllRemovableDrives", 23),
                          ("AllNetworkDrives", 24),
                          ("AllFixedDrives", 25)])
```

Exemplu

```
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;
};
```

Anexa 12. Conturi de utilizatori în regulile componentelor aplicației

Pentru a configura unele componente ale aplicației, trebuie să adaugi reguli speciale. De exemplu, pentru Control Web, trebuie să adaugi o regulă cu o listă de adrese web pe care dorești să le blocheze aplicația. În regulile componentelor aplicației, poți configura și o planificare pentru componentă sau poți selecta utilizatori cărora aplicația trebuie să le aplice regula.

Trebuie adăugate reguli pentru a configura următoarele componente ale aplicației:

- Application Control.
- Control Web.
- Control dispozitive.
- Inspecție jurnal.
- Control adaptiv al anomaliilor.
- Monitorizare integritate sistem.

Începând cu Endpoint Security for Windows 12.5, poți selecta utilizatori nu doar din Active Directory, ci și din lista de utilizatori din Kaspersky Security Center. De asemenea, poți introduce manual datele contului de utilizator local. Aceasta înseamnă că poți adăuga utilizatori în următoarele moduri:

- Active Directory (recomandat)
- Lista utilizatorilor din Kaspersky Security Center
- Contul de utilizator local

Pentru a utiliza corect toate metodele de selectare a utilizatorului, trebuie să actualizezi aplicația Kaspersky Endpoint Security și plug-in-ul de management la versiunea 12.5 sau la o versiune ulterioară.

Kaspersky recomandă utilizarea conturilor de utilizator locale numai în cazuri speciale, când nu este posibilă utilizarea conturilor de utilizator de domeniu. Pentru detalii despre riscurile de securitate ale utilizării conturilor locale, consultă Baza de cunoștințe Microsoft. Ești în totalitate răspunzător pentru securitatea unui computer dacă sunt utilizate conturi de utilizator locale; în special, aceasta include responsabilitatea de a controla și restricționa accesul la setările Kaspersky Endpoint Security.

Aplicația folosește SID-ul (Security Identifier) utilizatorului pentru a identifica utilizatorii. Când sunt utilizate conturi de utilizator din Active Directory sau din lista de utilizatori Kaspersky Security Center, aplicația determină SID-ul pe serverul de administrare. Aceasta înseamnă că aplicația nu solicită suplimentar computerul pentru a identifica un utilizator. Dacă ai adăugat mai mult de 1.000 de conturi de utilizator locale la o regulă de aplicație, aplicațiile contactează controlerul de domeniu pentru a identifica utilizatorul. Aceasta înseamnă că încărcarea computerului este crescută. Pentru a optimiza impactul asupra performanței pe computer, îți recomandăm să utilizez conturi de utilizator din Active Directory sau din lista de utilizatori Kaspersky Security Center.

Aplicația utilizează nume NetBIOS pentru identificarea conturilor de utilizator adăugate manual în formatele `<username>` și `<hostname>\<username>`. Un nume NetBIOS poate avea o lungime de până la 16 octeți (15 caractere). Dacă numele computerului are mai mult de 15 caractere, aplicația nu poate identifica utilizatorul. Apoi, aplicația dezactivează regula și generează o eroare, de exemplu, *Web Control: rule triggering disabled for user accounts without matching security identifier (SID)*. Pentru ca regula să funcționeze, trebuie să scurtezi manual numele computerului. Poți adăuga conturi de utilizator din Active Directory sau Kaspersky Security Center. În acest caz, aplicația scurtează automat numele computerului.

Kaspersky Endpoint Security acceptă, de asemenea, utilizatori și grupuri încorporate (cum ar fi grupul „Toate”) în cadrul regulilor. Datorită modului în care este determinat SID-ul unui utilizator, aplicația permite utilizarea numai a conturilor de utilizator încorporate adăugate din Active Directory sau din lista de utilizatori din Kaspersky Security Center. Regulile în care un cont de utilizator încorporat este adăugat local nu funcționează.

Informații juridice

Furnizarea datelor

Această secțiune conține informații despre datele pe care aplicația Kaspersky Endpoint Security le poate stoca pe dispozitiv și le poate transmite automat către Kaspersky în timpul funcționării sale.

Informațiile primite sunt protejate de Kaspersky conform legii și cerințelor și regulamentelor aplicabile ale Kaspersky. Datele sunt transmise prin canale de comunicare criptate.

Furnizarea datelor conform Acordului de licență pentru utilizatorul final

Dacă se aplică un cod de activare pentru activarea Kaspersky Endpoint Security, sunteți de acord să transmiteți periodic către Kaspersky, în mod automat, următoarele informații, cu scopul verificării utilizării corecte a aplicației:

- tipul, versiunea și locația aplicației Kaspersky Endpoint Security;
- versiunile actualizărilor instalate pentru aplicația Kaspersky Endpoint Security;
- ID-ul computerului și ID-ul instalării aplicației Kaspersky Endpoint Security pe computer;
- numărul de serie și identificatorul cheii active;
- tipul, versiunea și rata de biți a sistemului de operare, precum și numele mediului virtual (dacă aplicația Kaspersky Endpoint Security este instalată într-un mediu virtual);
- ID unic al solicitării către serviciile Titularului drepturilor;
- ID-urile componentelor aplicației Kaspersky Endpoint Security care sunt active în momentul transmiterii informațiilor.

De asemenea, Kaspersky poate folosi aceste informații pentru a genera statistici cu privire la diseminarea și utilizarea software-ului aparținând Kaspersky.

Prin utilizarea unui cod de activare, ești de acord să transmiți automat datele listate mai sus. Dacă nu sunteți de acord să transmiți aceste informații către Kaspersky, trebuie să folosiți un fișier cheie pentru a activa aplicația Kaspersky Endpoint Security.

Acceptând termenii Acordului de licență pentru utilizatorul final, ești de acord să transmiți în mod automat informațiile următoare:

- Când faci upgrade-ul produsului Kaspersky Endpoint Security:
  - versiunea aplicației Kaspersky Endpoint Security;
  - ID-ul aplicației Kaspersky Endpoint Security;

- cheia activă;
- ID-ul unic al pornirii activității de upgrade;
- ID-ul unic al instalării aplicației Kaspersky Endpoint Security.

- Când accesezi linkurile din interfața Kaspersky Endpoint Security:
  - versiunea aplicației Kaspersky Endpoint Security;
  - versiunea sistemului de operare;
  - data activării aplicației Kaspersky Endpoint Security;
  - data expirării licenței;
  - data creării cheii;
  - data instalării aplicației Kaspersky Endpoint Security;
  - ID-ul aplicației Kaspersky Endpoint Security;
  - ID-ul vulnerabilității detectate în sistemul de operare;
  - ID-ul ultimei actualizări instalate pentru Kaspersky Endpoint Security;
  - codul hash al fișierului detectat cu o amenințare și numele acestei amenințări conform clasificării Kaspersky;
  - categoria erorii de activare a aplicației Kaspersky Endpoint Security;
  - codul de eroare la activarea aplicației Kaspersky Endpoint Security;
  - numărul de zile până la expirarea cheii;
  - numărul de zile trecute de la adăugarea cheii;
  - numărul de zile trecute de la expirarea licenței;
  - numărul de computere pe care se aplică licența curentă;
  - cheia activă;
  - termenii licenței Kaspersky Endpoint Security;
  - starea curentă a licenței;
  - tipul licenței curente;
  - tipul aplicației;
  - ID-ul unic al pornirii activității de upgrade;
  - ID-ul unic al instalării Kaspersky Endpoint Security pe computer;
  - limba interfeței Kaspersky Endpoint Security.

Informațiile primite sunt protejate de Kaspersky conform legii și cerințelor și regulamentelor aplicabile ale Kaspersky. Datele sunt transmise prin canale de comunicare criptate.

Citește Acordul de licență pentru utilizatorul final și vizitează site-ul Web Kaspersky pentru a afla mai multe despre cum primim, procesăm, depozităm și distrugem informații despre utilizarea aplicației după ce accepți Acordul de licență pentru utilizatorul final și ești de acord cu Kaspersky Security Network Statement. Fișierele license.txt și ksn_<ID limbă>.txt conțin textul Acordului de licență pentru utilizatorul final și Kaspersky Security Network Statement și sunt incluse kitul de distribuire al aplicației.

Furnizarea datelor când folosiți Kaspersky Security Network

Setul de date pe care Kaspersky Endpoint Security îl trimite către Kaspersky depinde de tipul de licență și de setările de utilizare a Kaspersky Security Network.

Utilizarea KSN sub licență pe cel mult 4 computere

Acceptând Kaspersky Security Network Statement, ești de acord să transmiți automat informațiile următoare:

- informații despre actualizările de configurare KSN: identificatorul configurației active, identificatorul configurației primite, codul de eroare al actualizării configurației;
- informații despre fișiere și adrese URL care trebuie scanate: sumele de verificare ale fișierului scanat (MD5, SHA2-256, SHA1) și modelele fișierelor (MD5), dimensiunea modelului, tipul amenințării detectate și numele acestea după clasificarea Titularului de drepturi, identificatorul bazelor de date de viruși, adresa URL pentru care este solicitată reputația, dar și adresa URL de referință, identificatorul protocolului conexiunii și numărul portului utilizat;
- ID-ul activității de scanare care a detectat amenințarea;
- informații despre certificatele digitale utilizate de care este nevoie pentru a le verifica autenticitatea: sumele de verificare (SHA256) ale certificatului utilizat pentru a semna obiectul scanat și cheia publică a certificatului;
- identificatorul componentei software care efectuează scanarea;
- ID-urile bazelor de date antivirus și ale înregistrărilor din aceste baze de date antivirus;
- informații despre activarea software-ului pe computer: antetul semnat al tichetului de la serviciul de activare (identificatorul centrului de activare regional, suma de verificare a codului de activare, suma de verificare a tichetului, data creării tichetului, identificatorul unic al tichetului, versiunea tichetului, starea licenței, data de început/sfârșit și ora validării tichetului, identificatorul unic al licenței, versiunea licenței), identificatorul certificatului utilizat pentru semnarea antetului tichetului, suma de verificare (MD5) a fișierului cheie;
- informații despre software-ul titularului de drepturi: versiunea completă, tipul, versiunea de protocol utilizate pentru conectarea la serviciile Kaspersky.

Utilizarea KSN sub licență pe 5 sau mai multe computere

Acceptând Kaspersky Security Network Statement, ești de acord să transmiți automat informațiile următoare:

În cazul în care caseta de selectare **Kaspersky Security Network** este bifată și caseta de selectare **Activează modul KSN extins** este debifată, aplicația va transmite informațiile următoare:

- informații despre actualizările de configurare KSN: identificatorul configurației active, identificatorul configurației primite, codul de eroare al actualizării configurației;
- informații despre fișiere și adrese URL care trebuie scanate: sumele de verificare ale fișierului scanat (MD5, SHA2-256, SHA1) și modelele fișierelor (MD5), dimensiunea modelului, tipul amenințării detectate și numele acestea după clasificarea Titularului de drepturi, identificatorul bazelor de date de viruși, adresa URL pentru care este solicitată reputația, dar și adresa URL de referință, identificatorul protocolului conexiunii și numărul portului utilizat;
- ID-ul activității de scanare care a detectat amenințarea;
- informații despre certificatele digitale utilizate de care este nevoie pentru a le verifica autenticitatea: sumele de verificare (SHA256) ale certificatului utilizat pentru a semna obiectul scanat și cheia publică a certificatului;
- identificatorul componentei software care efectuează scanarea;
- ID-urile bazelor de date antivirus și ale înregistrărilor din aceste baze de date antivirus;
- informații despre activarea software-ului pe computer: antetul semnat al tichetului de la serviciul de activare (identificatorul centrului de activare regional, suma de verificare a codului de activare, suma de verificare a tichetului, data creării tichetului, identificatorul unic al tichetului, versiunea tichetului, starea licenței, data de început/sfârșit și ora validării tichetului, identificatorul unic al licenței, versiunea licenței), identificatorul certificatului utilizat pentru semnarea antetului tichetului, suma de verificare (MD5) a fișierului cheie;
- informații despre software-ul titularului de drepturi: versiunea completă, tipul, versiunea de protocol utilizate pentru conectarea la serviciile Kaspersky.

În cazul în care este bifată atât caseta de selectare **Activează modul KSN extins**, cât și caseta de selectare **Kaspersky Security Network**, în plus față de informațiile de mai sus, aplicația mai transmite și informațiile următoare:

- informații despre rezultatele stabilirii categoriilor resurselor web solicitate, care conțin adresele URL și IP procesate ale gazdei, versiunea componentei Software care a efectuat ordonarea pe categorii, metoda de ordonare pe categorii și seturile de categorii definite pentru resursele web;
- informații despre software-ul instalat pe computer: numele aplicațiilor software și ale furnizorilor de software, ale cheilor de registru și valorile acestora, informații despre fișierele componentelor software instalate (sumele de verificare (MD5, SHA2-256, SHA1), numele, calea către fișierul de pe computer, dimensiunea, versiunea și semnătura digitală);
- informații despre starea de protecție antivirus a computerului: versiunile și marcajele temporale ale lansării bazelor de date antivirus utilizate, ID-ul sarcinii și ID-ul software-ului care efectuează scanarea;
- informații despre fișierele descărcate de către Utilizatorul final: adresele URL și IP ale descărcării și paginile descărcate, identificatorul protocolului de descărcare și numărul portului conexiunii, starea adreselor URL ca fiind dăunătoare sau nu, atributele fișierelor, dimensiunea și sumele de verificare (MD5, SHA2-256, SHA1), informații despre procesul care a descărcat fișierul (sumele de verificare (MD5, SHA2-256, SHA1), ora și data creării/versiunii, starea redării automate, atributele, numele aplicațiilor de arhivare, informații privind semnăturile, semnalizatorul fișierelor executabile, identificatorul formatului și entropia), numele fișierului și calea acestuia pe computer, semnătura digitală a fișierului și marcajul de timp al generării sale, adresa URL la care a avut loc detectarea, numărul scriptului în pagina care pare suspectă sau dăunătoare, informații despre solicitările HTTP generate și răspunsul la acestea;

- informații referitoare la aplicațiile aflate în execuție și modulele acestora: date referitoare la procesele care sunt executate în sistem (ID proces (PID), numele procesului, informații despre contul care a inițiat procesul, aplicația și comanda care au inițiat procesul, simbolul programului sau procesului de încredere, calea completă către fișierele procesului și sumele lor de verificare (MD5, SHA2-256, SHA1) și linia de comandă inițială, nivelul de integritate a procesului, o descriere a produsului căruia aparține procesul (numele produsului și informații despre editor), precum și certificatele digitale utilizate și informațiile necesare pentru verificarea autenticității acestora sau informații despre absența unei semnături digitale a unui fișier), precum și informații despre modulele încărcate în procese (numele acestora, dimensiunile, tipurile, datele de creare, atributele, sumele de verificare (MD5, SHA2-256, SHA1), căile către acestea), informații despre antetul fișierului PE, numele utilitarelor de împachetare (dacă fișierul a fost împachetat);

- informații despre toate obiectele și activitățile potențial periculoase: numele obiectului detectat și calea completă spre obiectul respectiv pe computer, sumele de verificare ale fișierelor procesate (MD5, SHA2-256, SHA1), data și ora detectării, numele și dimensiunile fișierelor infectate și căile spre acestea, codul șablonului căii, semnalizatorul fișierului executabil, specificația care indică dacă obiectul este un container, numele arhivatorului (în cazul în care fișierul a fost arhivat), codul tipului fișierului, ID-ul formatului fișierului, lista acțiunilor efectuate de programul malware și decizia luată de software și de utilizator ca răspuns la aceste acțiuni, ID-urile bazelor de date antivirus și ale înregistrărilor din aceste baze de date antivirus care au fost utilizate pentru a lua decizia, indicatorul unui obiect potențial rău intenționat, numele amenințării detectate în funcție de clasificarea proprietarului drepturilor asupra software-ului, nivelul de pericol, starea detectării și metoda de detectare, motivul includerii în contextul analizat și numărul de ordine al fișierului în context, sumele de verificare (MD5, SHA2-256, SHA1), numele și atributele fișierului executabil al aplicației prin care a fost transmis mesajul sau linkul infectat, adresele IP (IPv4 și IPv6) depersonalizate ale gazdei obiectului blocat, entropia fișierului, indicatorul de executare automată al fișierului, momentul în care fișierul a fost detectat pentru prima dată în sistem, numărul de executări ale fișierului de la trimiterea ultimelor statistici, informații despre nume, sumele de verificare (MD5, SHA2-256, SHA1) și dimensiunea clientului de e-mail prin care a fost primit obiectul periculos, ID-ul activității software care a efectuat scanarea, specificația care indică dacă s-a verificat reputația sau semnătura fișierului, rezultatul procesării fișierului, suma de verificare (MD5) a modelului colectat pentru obiect, dimensiunea modelului în octeți și specificațiile tehnice ale tehnologiilor de detectare aplicate;

- informații despre obiectele scanate: grupul de încredere alocat către care și/sau de la care a fost plasat fișierul, motivul pentru care fișierul a fost plasat în categoria respectivă, identificatorul categoriei, informații despre sursa categoriilor și versiunea bazei de date corespunzătoare categoriei, permisiunea de certificat de încredere a fișierului, numele furnizorului fișierului, versiunea fișierului, numele și versiunea software-ului care include fișierul;

- informații despre vulnerabilitățile detectate: ID-ul acestora din baza de date pentru vulnerabilități, clasa de pericol corespunzătoare vulnerabilității;

- informații despre emularea fișierului executabil: dimensiunea fișierului și sumele de verificare ale acestuia (MD5, SHA2-256, SHA1), versiunea componentei de emulare, profunzimea emulării, o gamă de proprietăți de seturi logice și funcții în cadrul seturilor logice obținute în timpul emulării, date de la antetele PE ale fișierului executabil;

- adresele IP ale computerului atacator (IPv4 și IPv6), numărul de porturi de pe computer către care este îndreptat atacul, identificatorul protocolului pachetului IP care conține atacul, ținta atacului (numele, site-ul web al organizației), permisiunea pentru reacția la atac, seriozitatea atacului, nivelul de încredere;

- informații despre atacurile asociate cu resursele falsificate ale rețelei, adresele DNS și IP (IPv4 și IPv6) ale site-urilor web vizitate;

- adresele DNS și IP (IPv4 sau IPv6) ale resurselor web solicitate, informații despre fișier și clientul web care accesează resursa web, numele, dimensiunea și sumele de verificare (MD5, SHA2-256, SHA1) ale fișierului, calea completă către fișier și codul șablonului căii, rezultatul verificării semnăturii digitale și starea acestuia în KSN;

- informații despre restaurarea acțiunilor programelor malware: datele din fișierul a cărui activitate a fost restaurată (numele fișierului, calea completă către fișier, dimensiunea și sumele de verificare ale acestuia (MD5, SHA2-256, SHA1)), datele despre acțiunile reușite sau nereușite de ștergere, de redenumire și copiere a fișierelor și de restaurare a valorilor în registru (numele cheilor de registru și valorile acestora) și informațiile despre fișierele de sistem modificate de malware, înainte și după restaurare;

- informații despre setul de excluderi pentru componenta Control adaptiv al anomaliilor: ID-ul stării pentru regula care a fost declanșată, acțiunea efectuată de software când a fost declanșată regula, tipul contului de utilizator sub care procesul sau șirul efectuează activitatea suspectă, informații despre procesul care a fost efectuat sau supus activității suspecte (ID-ul scriptului sau numele fișierului de proces, calea completă a fișierului de proces, codul șablonului căii, sumele de verificare (MD5, SHA2-256, SHA1) ale fișierului de proces); informații despre obiectul care a efectuat acțiunile suspecte, precum și despre obiectul care a fost supus acțiunilor suspecte (numele cheii de registru sau numele fișierului, calea completă a fișierului, codul șablonului căii și sumele de verificare (MD5, SHA2-256, SHA1) ale fișierului).

- informații despre modulele software încărcate: numele, dimensiunea și sumele de verificare (MD5, SHA2-256, SHA1) ale fișierului modulului, calea completă către acesta și codul șablonului căii, setările semnăturii digitale a fișierului modulului, data și ora creării semnăturii, numele subiectului și al organizației care a semnat fișierul modulului, ID-ul procesului în care s-a încărcat modulul, numele furnizorului modulului și numărul de ordine al modulului în coada de încărcare;

- informații despre calitatea interacțiunii software-ului cu serviciile KSN: data și ora începerii și terminării perioadei în care au fost generate statisticile, informații despre calitatea solicitărilor și a conexiunii la fiecare dintre serviciile KSN utilizate (ID-ul serviciului KSN, numărul de solicitări reușite, numărul de solicitări cu răspunsuri din memoria cache, numărul de solicitări nereușite (probleme de rețea, dezactivarea KSN din setările software-ului, rutarea incorectă), intervalul de timp între solicitările reușite, intervalul de timp între solicitările anulate, intervalul de timp între solicitările cu limită de timp depășită, numărul de conexiuni la KSN preluate din memoria cache, numărul de conexiuni reușite la KSN, numărul de conexiuni nereușite la KSN, numărul de tranzacții reușite, numărul de tranzacții nereușite, intervalul de timp între conexiunile reușite la KSN, intervalul de timp între conexiunile nereușite la KSN, intervalul de timp între tranzacțiile reușite, intervalul de timp între tranzacțiile nereușite);

- dacă se detectează un potențial obiect rău intenționat, se vor furniza informații legate de datele din memoria proceselor: elemente ale ierarhiei obiectelor din sistem (ObjectManager), date din memoria BIOS UEFI, nume ale cheilor de registru și valorile acestora;

- informații despre evenimente din jurnalele sistemelor: marcajul temporal al evenimentului, numele jurnalului în care a fost găsit evenimentul, tipul și categoria evenimentului, numele sursei evenimentului și descrierea evenimentului;

- informații despre conexiunile la rețea: versiunea și sumele de verificare (MD5, SHA2-256, SHA1) ale fișierului din care a fost inițiat procesul care a deschis portul, calea către fișierul procesului și semnătura digitală a acestui fișier, adresele IP locale și la distanță, numerele porturilor de conexiune locale și la distanță, starea conexiunii, marcajul temporal aferent deschiderii portului;

- informații despre data instalării și activării software-ului pe computer: ID-ul partenerului care a vândut licența, numărul de serie al licenței, antetul semnat al tichetului de la serviciul de activare (ID-ul unui centru regional de activare, suma de verificare a codului de activare, suma de verificare a tichetului, data creării tichetului, ID-ul unic al tichetului, versiunea tichetului, starea licenței, data și ora de începere/sfârșit a tichetului, ID-ul unic al licenței, versiunea licenței), ID-ul certificatului utilizat pentru semnarea antetului tichetului, suma de control (MD5) a fișierului cheie, ID-ul unic al instalării software-ului pe computer, tipul și ID-ul aplicației care se actualizează, ID-ul activității de actualizare;

- informații despre setul tuturor actualizărilor instalate și setul celor mai recente actualizări instalate/dezinstalate, tipul evenimentului care a cauzat trimiterea informațiilor de actualizare, durata de la ultima actualizare, informații despre toate bazele de date anti-virus instalate curent;

- informații despre funcționarea software-ului pe computer: date despre utilizarea procesorului, date despre utilizarea memoriei (octeți privați, acumulator fără paginare, acumulator cu paginare), numărul firelor active în procesul software și al firelor în așteptare, precum și durata de funcționare a software-ului înainte de apariția erorii;

- numărul de evenimente software dump și system dump (erori critice cu ecran albastru BSOD) de la instalarea software-ului și de la momentul ultimei actualizări, identificatorul și versiunea modulului software care a generat eroarea, stiva de memorie din procesul aplicației, precum și informații despre bazele de date anti-virus de la momentul erorii;

- date despre system dump (BSOD): un marcaj care să indice apariția sau lipsa apariției ecranului albastru, numele driverului care a cauzat apariția ecranului albastru, adresa și stiva de memorie din driver, un marcaj care să indice durata sesiunii de utilizare a sistemului de operare înaintea apariției ecranului albastru, stiva de memorie cu drivere care a cedat, tipul imaginii de memorie stocate, marcajul sesiunii sistemului de operare înainte ca BSOD să dureze mai mult de 10 minute, identificatorul unic al imaginii, marca de timp pentru BSOD;

- informații despre erorile sau despre problemele de performanță care au apărut în timpul funcționării componentelor Software-ului: ID-ul de stare al Software-ului, tipul, codul și cauza erorii, precum și momentul în care a apărut eroarea, ID-urile componentei, ale modulului și ale procesului în care a apărut eroarea, ID-ul sarcinii sau al categoriei de actualizare în timpul căreia a apărut eroarea, jurnalele driverelor utilizate de Software (codul erorii, numele modulului, numele fișierului sursă și linia în care a apărut eroarea);

- informații despre actualizările bazelor de date antivirus și ale componentelor Software-ului: numele, data și ora fișierelor de indexare descărcate în timpul ultimei actualizări și aflate în curs de descărcare în timpul actualizării curente;

- informații despre încetarea anormală a funcționării Software-ului: data și ora creării erorii, tipul acesteia, tipul evenimentului care a cauzat încetarea anormală a funcționării Software-ului (oprirea neașteptată, eroarea unei aplicații terțe) și ora opririi neașteptate;

- informații despre compatibilitatea driverelor Software-ului cu hardware-ul și Software-ul: informații despre proprietățile sistemului de operare care restricționează funcționalitatea componentelor Software-ului (Secure Boot, KPTI, WHQL Enforce, BitLocker, Case Sensitivity), tipul Software-ului de descărcare instalat (UEFI, BIOS), identificatorul Trusted Platform Module (TPM), versiunea specificației TPM, informații despre procesorul instalat pe computer, modul de operare și parametrii integrității codului și a protecției dispozitivului, modul de operare al driverelor și motivul de utilizare a modului curent, versiunea driverelor Software-ului, starea suportului de virtualizare software și hardware al computerului;

- informații despre aplicațiile terțe care au cauzat eroarea: numele, versiunea și localizarea, codul de eroare și informații despre eroare din jurnalul de sistem al aplicațiilor, adresa erorii și stiva de memorie a aplicației terțe, un marcaj care să indice apariția erorii în componenta Software, precum și durata pentru care aplicația terță a funcționat înainte de apariția erorii, sumele de verificare (MD5, SHA2-256, SHA1) ale imaginii procesului aplicației în care a apărut eroarea, calea către imaginea procesului aplicației și codul șablonului căii, informații din jurnalul sistemului cu descrierea erorii asociate cu aplicația, informații despre modulul aplicației în care a apărut eroarea (identificatorul excepției, adresa memoriei cache ca decalaj în modulul aplicației, numele și versiunea modulului, identificatorul căderii aplicației în insertul Deținătorului drepturilor și stiva de memorie a căderii, durata sesiunii aplicației înaintea căderii);

- versiunea componentei de actualizare a Software-ului, numărul erorilor componentei de actualizare apărute în timp ce rulează sarcini de actualizare în timpul duratei de viață a componentei, ID-ul tipului sarcinii de actualizare, numărul încercărilor eșuate ale componentei de actualizare de a executa sarcinile de actualizare;

- informații despre funcționarea componentelor de monitorizare a sistemului Software-ului: versiunile complete ale componentelor, data și ora la care au pornit componentele, codul evenimentului care a depășit coada evenimentului și numărul de astfel de evenimente, numărul total de evenimente de depășire a cozii, informații despre fișierul de proces al inițiatorului evenimentului (numele fișierului și calea acestuia pe computer, codul șablonului căii pentru fișier, sumele de verificare (MD5, SHA2-256, SHA1) ale procesului asociat cu fișierul, versiunea fișierului), identificatorul interceptării de eveniment care a apărut, versiunea completă a filtrului de interceptare, identificatorul tipului de eveniment interceptat, dimensiunea cozii evenimentului și numărul de evenimente între primul eveniment din coadă și evenimentul curent, numărul de evenimente depășite din coadă, informații despre fișierul de proces al inițiatorului evenimentului curent (numele fișierului și calea acestuia pe computer, codul șablonului căii pentru fișier, sumele de verificare (MD5, SHA2-256, SHA1) ale procesului asociat cu fișierul), durata procesării evenimentului, durata maximă a procesării evenimentului, probabilitatea de trimitere a statisticilor, informații despre evenimentele sistemului de operare pentru care a fost depășită limita de timp a procesării (data și ora evenimentului, numărul de inițializări repetate ale bazelor de date antivirus, data și ora ultimei inițializări repetate a bazelor de date antivirus după actualizarea acestora, timpul de întârziere a procesării evenimentului pentru fiecare componentă de monitorizare a sistemului, numărul de evenimente din coadă, numărul de evenimente procesate, numărul de evenimente întârziate ale tipului curent, timpul total de întârziere pentru evenimentele tipului curent, timpul total de întârziere pentru toate evenimentele);

- informații din instrumentul Windows de urmărire a evenimentelor (Event Tracing for Windows, ETW) în cazul problemelor de performanță ale Software-ului, furnizorii evenimentelor SysConfig/SysConfigEx/WinSATAssessment din Microsoft: informații despre computer (model, producător, factorul de formă a carcasei, versiunea), informații despre măsurătorile de performanță Windows (evaluările WinSAT, indicele de performanță Windows), numele domeniului, informații despre procesoarele fizice și logice (numărul de procesoare fizice și logice, producătorul, modelul, nivelul de modificare a instrucțiunilor, numărul de nuclee, frecvența ceasului, CPUID, caracteristicile memoriei cache, caracteristicile procesoarelor logice, indicatorii modurilor și ai instrucțiunilor suportate), informații despre modulele RAM (tip, factor de formă, producător, model, capacitate, granularitatea alocării memoriei), informații despre interfețele de rețea (adresele IP și MAC, numele, descrierea, configurarea interfețelor de rețea, detalierea numărului și a dimensiunii pachetelor de rețea după tip, viteza schimbului de rețea, detalierea numărului de erori de rețea după tip), configurarea controlerului IDE, adresele IP ale serverelor DNS, informații despre placa video (model, descriere, producător, compatibilitate, capacitate memorie video, permisiune ecran, număr de biți pe pixel, versiune BIOS), informații despre dispozitivele plug-and-play (numele, descrierea, identificatorul dispozitivului [PnP, ACPI], informații despre discuri și dispozitive de stocare (numărul de discuri sau de unități flash, producător, model, capacitate disc, număr de cilindri, număr de piste pe cilindru, număr de sectoare pe pistă, capacitate sector, caracteristici memorie cache, număr secvențial, numărul de partiții, configurarea controlerului SCSI), informații despre discurile logice (numărul secvențial, capacitatea partiției, capacitatea volumului, litera de volum, tipul partiției, tipul sistemului de fișiere, numărul de clustere, dimensiunea clusterelor, numărul de sectoare pe cluster, numărul de clustere goale și ocupate, litera volumului care poate fi inițializat, adresa de decalaj a partiției în raport cu începutul discului), informații despre placa de bază BIOS (producător, dată de eliberare, versiune), informații despre placa de bază (producător, model, tip), informații despre memoria fizică (capacitate partajată și liberă), informații despre serviciile sistemului de operare (nume, descriere, stare, etichetă, informații despre procese [nume și PID]), parametrii consumului de energie pentru computer, configurarea controlerului de întrerupere, calea directoarelor de sistem Windows (Windows și System32), informații despre sistemul de operare (versiune, generare, data eliberării, nume, tip, data instalării), dimensiunea fișierului paginii, informații despre monitoare (număr, producător, permisiune ecran, capacitate rezoluție, tip), informații despre driverul plăcii video (producător, data eliberării, versiune);

- informații din ETW, furnizorii evenimentelor EventTrace/EventMetadata de la Microsoft: informații despre secvența evenimentelor de sistem (tip, oră, dată, fus orar), metadate despre fișierul cu rezultatele urmăririi (nume, structură, parametrii urmăririi, detalierea numărului de operații de urmărire după tip), informații despre SO (nume, tip, versiune, generare, data eliberării, ora începerii);

- informații din ETW, furnizorii evenimentelor Process/Microsoft Windows Kernel Process/Microsoft Windows Kernel Processor Power din Microsoft: informații despre procesele începute și finalizate (nume, PID, parametri de pornire, linie de comandă, cod de retur, parametri de gestionare a alimentării, oră de început și de sfârșit, tipul simbolului de acces, SID, SessionID, număr de descriptori instalați), informații despre modificările proprietăților pentru șir (TID, prioritate, oră), informații despre operațiile procesului pe disc (tip, oră, capacitate, număr), istoricul modificărilor în structura și capacitatea proceselor de memorie utilizabilă;

- informații din ETW, furnizorii evenimentelor StackWalk/Perfinfo de la Microsoft: informații despre contoarele de performanță (performanța secțiunilor individuale de coduri, secvența apelurilor de funcții, PID, TID, adresele și atributele ISR-urilor și ale DPC-urilor);

- informații din ETW, furnizorul evenimentelor KernelTraceControl-ImageID de la Microsoft: informații despre fișierele executabile și bibliotecile dinamice (nume, dimensiune imagine, cale completă), informații despre fișierele PDB (nume, identificator), datele despre resurse VERSIONINFO pentru fișierele executabile (nume; descriere, creator, locație, versiune și identificator aplicație, versiune și identificator fișier);

- informații din ETW, furnizorii evenimentelor FileIo/DiskIo/Image/Windows Kernel Disk de la Microsoft: informații despre operațiile din fișier și de pe disc (tip, capacitate, oră de început, oră de sfârșit, durată, stare finalizare, PID, TID, adresele apelurilor de funcții pentru drivere, Pachetul de solicitări I/O (IRP), atributele de obiect ale fișierelor Windows), informații despre fișierele implicate în operațiile din fișier și de pe disc (numele, versiunea, dimensiunea, calea completă, atribute, decalaj, suma de verificare a imaginilor, opțiunile de deschidere și de acces);

- informații din ETW, furnizorul evenimentelor PageFault de la Microsoft: informații despre erorile de acces la pagina de memorie (adresă, oră, capacitate, PID, TID, atributele obiectului de fișiere Windows, parametri de alocare a memoriei);

- informații din ETW, furnizorul evenimentelor Thread de la Microsoft: informații despre crearea/finalizarea șirurilor, informații despre șirurile începute (PID, TID, dimensiunea stivei, prioritățile și alocarea resurselor procesorului, resursele I/O, paginile de memorie între șiruri, adresa stivei, adresa funcției init, adresa Thread Environment Block (TEB), eticheta serviciului Windows);

- informații din ETW, furnizorul de evenimente Microsoft Windows Kernel Memory de la Microsoft: informații despre operațiile de gestionare a memoriei (stare finalizare, oră, cantitate, PID), structura de alocare a memoriei (tip, capacitate, SessionID, PID);

- informații despre funcționarea Software-ului în cazul problemelor de performanță: identificatorul de instalare a Software-ului, tipul și valoarea scăderii performanței, informații despre secvența de evenimente din cadrul Software-ului (oră, fus orar, tip, stare finalizare, identificatorul componentei Software-ului, identificatorul scenariului de funcționare a Software-ului, TIP, PID, adresele de apelare a funcțiilor), informații despre conexiunile de rețea de verificat (URL, direcția conexiunii, dimensiunea pachetului de rețea), informații despre fișierele PDB (nume, identificator, dimensiunea imaginii pentru fișierul executabil), informații despre fișierele de verificat (nume, cale completă, sumă de verificare), parametri de monitorizare a performanței Software-ului;

- informații despre ultima încercare nereușită de reinițializare a sistemului de operare: numărul reinițializărilor nereușite de la instalarea sistemului de operare până în prezent, date despre erorile de sistem (codul și parametri unei erori, nume, versiune și suma de verificare (CRC32) a modulului care a cauzat o eroare a sistemului de operare, adresa erorii, sumele de verificare (MD5, SHA2-256, SHA1) ale erorilor de sistem);

- informații verificarea autenticității certificatelor digitale utilizate pentru a semna fișiere: amprenta certificatului, algoritmul sumei de verificare, cheia publică și numărul de serie ale certificatului, numele emitentului certificatului, rezultatul validării certificatului și identificatorul bazei de date a certificatului;

- informații despre procesul care execută atacul asupra componentei de autoapărare a Software-ului: numele și dimensiunea fișierului procesului, sumele sale de verificare (MD5, SHA2-256, SHA1), calea completă a fișierului procesului și codul șablonului căii fișierului, marcajul temporal al creării/compilării, marcajul fișierului executabil, atributele fișierului procesului, informații despre certificatul utilizat pentru a semna fișierul procesului, codul contului utilizat la lansarea procesului, ID-ul operațiunilor efectuate pentru a accesa procesul, tipul resursei cu care se efectuează operațiunea (proces, fișier, obiect de registru, funcția de căutare FindWindow), numele resursei cu care se efectuează operațiunea, marcaj care indică reușita operațiunii, starea fișierului procesului și semnătura acestuia conform KSN;

- informații despre software-ul titularului de drepturi: versiunea completă, tipul, localizarea și starea de funcționare a software-ului utilizat, versiunile componentelor software instalate și starea de funcționare a acestora, informații despre actualizările software instalate, valoarea filtrului TARGET, versiunea protocolului utilizat pentru conectarea la serviciile titularului de drepturi;

- informații despre componentele hardware instalate pe computer: tip, nume, numele modelului, versiunea firmware-ului, parametri dispozitivelor incluse și conectate, identificatorul unic al computerului cu Software-ul instalat;

- informații despre versiunile sistemului de operare și despre actualizările instalate, dimensiunea cuvintelor, ediția și parametrii modului de funcționare al sistemului de operare, versiunea și sumele de verificare (MD5, SHA2-256, SHA1) ale fișierului kernel al sistemului de operare și data și ora de început a sistemului de operare;

- fișiere executabile și neexecutabile, total sau parțial;

- porțiuni din memoria RAM a computerului;

- sectoarele implicate în procesul de pornire a sistemului de operare;

- Pachete de date despre traficul de rețea;

- pagini web și e-mailuri care conțin obiecte suspecte și periculoase;

- descrierea claselor și instanțelor claselor din depozitul WMI;

- rapoarte de activitate ale aplicațiilor:

    - numele, dimensiunea și versiunea fișierului trimis, descrierea și sumele de verificare ale acestuia (MD5, SHA2-256, SHA1), identificatorul formatului de fișier, numele furnizorului fișierului, numele produsului căruia îi aparține fișierul, calea completă către fișier de pe computer, codul șablonului căii, informații despre data și ora creării și modificării fișierului;

    - data/ora începerii și terminării perioadei de valabilitate a certificatului (dacă fișierul are semnătură digitală), data și ora semnăturii, numele emitentului certificatului, informații despre deținătorul certificatului, amprenta, cheia publică a certificatului și algoritmii aferenți și numărul de serie al certificatului;

    - numele contului din care este executat procesul;

    - sumele de verificare (MD5, SHA2-256, SHA1) ale numelui computerului pe care este executat procesul;

    - denumirile ferestrelor procesului;

    - identificatorul bazelor de date antivirus, numele amenințării detectate conform clasificării Deținătorului drepturilor;

    - date despre licența instalată, inclusiv ID-ul, tipul și data expirării acesteia;

    - ora locală a computerului în momentul furnizării informațiilor;

    - numele și căile fișierelor care au fost accesate de către proces;

    - numele cheilor de registru care au fost accesate de către proces și valorile acestora;

    - adresele URL și IP care au fost accesate de către proces;

    - adresele URL și IP de la care a fost descărcat fișierul aflat în execuție.

Furnizarea datelor atunci când se utilizează soluțiile Detection and Response

Pe computerele cu Kaspersky Endpoint Security instalat, datele pregătite pentru trimitere automată către serverele Kaspersky Endpoint Detection and Response, Kaspersky Sandbox și Kaspersky Anti Targeted Attack Platform sunt stocate. Fișierele sunt stocate pe computere într-o formă simplă, necriptată.

Setul specific de date depinde de soluția în cadrul căreia este utilizat Kaspersky Endpoint Security.

Kaspersky Endpoint Detection and Response

Toate datele pe care aplicația le stochează local pe computer sunt șterse de pe computer atunci când Kaspersky Endpoint Security este dezinstalat.

Datele primite ca urmare a executării activității IOC Scan (activitate standard)

Kaspersky Endpoint Security trimite automat date despre executarea activității *Scanare IOC* către Kaspersky Security Center.

Datele din rezultatele executării activității *Scanare IOC* pot conține următoarele informații:

- Adresa IP din tabelul ARP
- Adresa fizică din tabelul ARP
- Tipul și numele înregistrării DNS
- Adresa IP a computerului protejat
- Adresa fizică (adresa MAC) a computerului protejat
- Identificatorul din intrarea în jurnalul de evenimente
- Numele sursei de date în jurnal
- Nume jurnal
- Oră eveniment
- Hash-urile MD5 și SHA256 ale fișierului
- Numele complet al fișierului (inclusiv calea)
- Mărimea fișierului
- Adresa IP la distanță și portul la care a fost stabilită conexiunea în timpul scanării

- Adresa IP a adaptorului local
- Portul deschis pe adaptorul local
- Protocolul ca număr (în conformitate cu standardul IANA)
- Numele procesului
- Argumentele procesului
- Calea către fișierul de proces
- Identificatorul Windows (PID) al procesului
- Identificatorul Windows (PID) al procesului părinte
- Contul de utilizator care a pornit procesul
- Data și ora la care a fost pornit procesul
- Nume serviciu
- Descrierea serviciului
- Calea și numele serviciului DLL (pentru svchost)
- Calea și numele serviciului executabil al serviciului
- Identificatorul Windows (PID) al serviciului
- Tipul serviciului (de exemplu, un driver sau o placă de kernel)
- Starea serviciului
- Modul de lansare a serviciului
- Numele contului de utilizator
- Numele volumului
- Litera volumului
- Tipul volumului
- Valoarea registry-ului Windows
- Valoarea secțiunii registry
- Calea cheii de registry (fără numele secțiunii și valoare)
- Setarea registry-ului
- Sistemul (mediul)
- Numele și versiunea sistemului de operare care este instalat pe computer

- Numele rețelei computerului protejat
- Domeniul sau grupul căruia îi aparține computerul protejat
- Numele browserului
- Versiunea browserului
- Ora la care a fost accesată ultima dată resursa web
- URL-ul din solicitarea HTTP
- Numele contului utilizat pentru solicitarea HTTP
- Numele de fișier al procesului care a efectuat solicitarea HTTP
- Calea completă către fișierul procesului care a efectuat solicitarea HTTP
- Identificatorul Windows (PID) al procesului care a efectuat solicitarea HTTP
- Pagina vizitată anterior (URL-ul sursei solicitării HTTP)
- URI-ul resursei solicitate prin HTTP
- Informații despre agentul utilizator HTTP (aplicația care a efectuat solicitarea HTTP)
- Timpul de execuție a solicitării HTTP
- Identificatorul unic al procesului care a efectuat solicitarea HTTP

Datele pentru crearea unui lanț de dezvoltare a amenințărilor

Datele pentru crearea unui lanț de dezvoltare a amenințărilor sunt stocate, în mod implicit, timp de șapte zile. Datele sunt trimise automat către Kaspersky Security Center.

Datele pentru crearea unui lanț de dezvoltare a amenințărilor pot conține următoarele informații:

- Data și ora incidentului
- Numele obiectului detectat
- Mod scanare
- Starea ultimei acțiuni aferente detectării
- Motivul pentru care procesarea detectării a eșuat
- Tipul obiectului detectat
- Numele obiectului detectat
- Starea amenințării după procesarea obiectului

- Motivul pentru care executarea acțiunilor asupra obiectului a eșuat
- Acțiunile efectuate pentru a derularea înapoi a acțiunilor rău intenționate
- Informații despre obiectul procesat:
  - Identificatorul unic al procesului
  - Identificatorul unic al procesului părinte
  - Identificatorul unic al fișierului procesului
  - Identificatorul procesului Windows (PID)
  - Linia de comandă a procesului
  - Contul de utilizator care a pornit procesul
  - Codul sesiunii de conectare în care se execută procesul
  - Tipul sesiunii în care se execută procesul
  - Nivelul de integritate al procesului în curs de procesare
  - Calitatea de membru al contului de utilizator care a pornit procesul în grupurile locale și domeniile privilegiate
  - Identificatorul obiectului procesat
  - Numele complet al obiectului procesat
  - Identificatorul dispozitivului protejat
  - Numele complet al obiectului (numele fișierului local sau adresa web a fișierului descărcat)
  - Hash-ul MD5 sau SHA256 al obiectului procesat
  - Tipul obiectului procesat
  - Data creării obiectului procesat
  - Data la care obiectul procesat a fost modificat ultima dată
  - Dimensiunea obiectului procesat
  - Atributele obiectului procesat
  - Organizația care a semnat obiectul procesat
  - Rezultatul verificării certificatului digital al obiectului procesat
  - Identificatorul de securitate (SID) al obiectului procesat
  - Identificatorul de fus orar al obiectului procesat
  - Adresa web de unde a fost descărcat obiectul procesat (numai pentru fișierele de pe disc)

- Numele aplicației care a descărcat fișierul
- Hash-urile MD5 și SHA256 ale aplicației care a descărcat fișierul
- Numele aplicației care a modificat ultima dată fișierul
- Hash-urile MD5 și SHA256 ale aplicației care a modificat ultima dată fișierul
- Numărul de porniri ale obiectului procesat
- Data și ora la care a fost pornit prima dată obiectul procesat
- Identificatorii unici ai fișierului
- Numele complet al fișierului (numele fișierului local sau adresa web a fișierului descărcat)
- Calea către variabila registry-ului Windows procesat
- Numele variabilei registry-ului Windows procesat
- Valoarea variabilei registry-ului Windows procesat
- Tipul variabilei registry-ului Windows procesat
- Indicatorul stării de membru a cheii de registry procesate în punctul de executare automată
- Adresa web a solicitării web procesate
- Sursa linkului solicitării web procesate
- Agentul de utilizator al solicitării web procesate
- Tipul solicitării web procesate (`GET` sau `POST`)
- Portul IP local al solicitării web procesate
- Portul IP la distanță al solicitării web procesate
- Direcția conexiunii (intrare sau ieșire) a solicitării web procesate
- Identificatorul procesului în care a fost încorporat codul rău intenționat

Kaspersky Sandbox

Toate datele pe care aplicația le stochează local pe computer sunt șterse de pe computer atunci când Kaspersky Endpoint Security este dezinstalat.

Datele serviciului

Kaspersky Endpoint Security stochează următoarele date procesate în timpul răspunsului automat:

- Fișierele procesate și datele introduse de utilizator în timpul configurării agentului încorporat al Kaspersky Endpoint Security:
  - Fișiere carantinate
  - Cheia publică a certificatului utilizat pentru integrarea cu Kaspersky Sandbox
- Cache-ul agentului încorporat al Kaspersky Endpoint Security:
  - Ora la care rezultatele scanării au fost scrise în cache
  - Hash-ul MD5 al activității de scanare
  - Identificatorul activității de scanare
  - Rezultatul scanării pentru obiect
- Coada solicitărilor de scanare a obiectelor:
  - ID-ul obiectului din coadă
  - Ora la care obiectul a fost plasat în coadă
  - Starea procesării obiectului din coadă
  - ID-ul sesiunii utilizatorului din sistemul de operare în care a fost creată activitatea de scanare a obiectului
  - Identificatorul de sistem (SID) al utilizatorului sistemului de operare al cărui cont a fost utilizat pentru a crea activitatea
  - Hash-ul MD5 al activității de scanare a obiectului
- Informații despre activitățile pentru care agentul încorporat al Kaspersky Endpoint Security așteaptă rezultatele scanării de la Kaspersky Sandbox:
  - Ora la care a fost primită activitatea de scanare a obiectului
  - Starea procesării obiectului
  - ID-ul sesiunii utilizatorului din sistemul de operare în care a fost creată activitatea de scanare a obiectului
  - Identificatorul activității de scanare a obiectului
  - Hash-ul MD5 al activității de scanare a obiectului
  - Identificatorul de sistem (SID) al utilizatorului sistemului de operare al cărui cont a fost utilizat pentru a crea activitatea
  - Schema XML a IOC creat automat

- Hash-ul MD5 sau SHA256 al obiectului scanat
- Erorile de procesare
- Numele obiectelor pentru care a fost creată activitatea
- Rezultatul scanării pentru obiect

Datele din solicitările către Kaspersky Sandbox

Următoarele date de la solicitările de la agentul încorporat al Kaspersky Endpoint Security către Kaspersky Sandbox sunt stocate local pe computer:

- Hash-ul MD5 al activității de scanare
- Identificatorul activității de scanare
- Obiectul scanat și toate fișierele aferente

Datele primite ca urmare a executării activității IOC Scan (activitate independentă)

Kaspersky Endpoint Security trimite automat date despre executarea activității *Scanare IOC* către Kaspersky Security Center.

Datele din rezultatele executării activității *Scanare IOC* pot conține următoarele informații:

- Adresa IP din tabelul ARP
- Adresa fizică din tabelul ARP
- Tipul și numele înregistrării DNS
- Adresa IP a computerului protejat
- Adresa fizică (adresa MAC) a computerului protejat
- Identificatorul din intrarea în jurnalul de evenimente
- Numele sursei de date în jurnal
- Nume jurnal
- Oră eveniment
- Hash-urile MD5 și SHA256 ale fișierului
- Numele complet al fișierului (inclusiv calea)
- Mărimea fișierului

- Adresa IP la distanță și portul la care a fost stabilită conexiunea în timpul scanării
- Adresa IP a adaptorului local
- Portul deschis pe adaptorul local
- Protocolul ca număr (în conformitate cu standardul IANA)
- Numele procesului
- Argumentele procesului
- Calea către fișierul de proces
- Identificatorul Windows (PID) al procesului
- Identificatorul Windows (PID) al procesului părinte
- Contul de utilizator care a pornit procesul
- Data și ora la care a fost pornit procesul
- Nume serviciu
- Descrierea serviciului
- Calea și numele serviciului DLL (pentru svchost)
- Calea și numele serviciului executabil al serviciului
- Identificatorul Windows (PID) al serviciului
- Tipul serviciului (de exemplu, un driver sau o placă de kernel)
- Starea serviciului
- Modul de lansare a serviciului
- Numele contului de utilizator
- Numele volumului
- Litera volumului
- Tipul volumului
- Valoarea registry-ului Windows
- Valoarea secțiunii registry
- Calea cheii de registry (fără numele secțiunii și valoare)
- Setarea registry-ului
- Sistemul (mediul)

- Numele și versiunea sistemului de operare care este instalat pe computer
- Numele rețelei computerului protejat
- Domeniul sau grupul căruia îi aparține computerul protejat
- Numele browserului
- Versiunea browserului
- Ora la care a fost accesată ultima dată resursa web
- URL-ul din solicitarea HTTP
- Numele contului utilizat pentru solicitarea HTTP
- Numele de fișier al procesului care a efectuat solicitarea HTTP
- Calea completă către fișierul procesului care a efectuat solicitarea HTTP
- Identificatorul Windows (PID) al procesului care a efectuat solicitarea HTTP
- Pagina vizitată anterior (URL-ul sursei solicitării HTTP)
- URI-ul resursei solicitate prin HTTP
- Informații despre agentul utilizator HTTP (aplicația care a efectuat solicitarea HTTP)
- Timpul de execuție a solicitării HTTP
- Identificatorul unic al procesului care a efectuat solicitarea HTTP

Kaspersky Endpoint Detection and Response Expert (on-premises)

Toate datele pe care aplicația le stochează local pe computer sunt șterse de pe computer atunci când Kaspersky Endpoint Security este dezinstalat.

Datele serviciului

Agentul încorporat al Kaspersky Endpoint Security stochează local următoarele date:

- Date necesare pentru integrarea cu componenta EDR Expert (on-premises):
  - Adresa și portul pentru conectarea la serverul Central Node KATA
  - Adresa și portul pentru conectarea la serverul de transmisie a telemetriei
  - Adresa și portul pentru conectarea la serverul de răspuns

- Informațiile despre certificatele utilizate pentru integrarea cu Central Node KATA
- Informațiile despre certificatele utilizate pentru integrarea cu serverul de transmisie a telemetriei
- Informațiile despre certificatele utilizate pentru integrarea cu serverul de răspuns

- Fișiere carantinate

Date din evenimentele de telemetrie transmise

- **Date de telemetrie**
  - Date despre fișiere:
    - Identificatorii unici ai fișierului
    - Tip de fișier
    - Calea completă a fișierului
    - Mărimea fișierului
    - Atributele fișierului
    - Identificatorul de zonă
    - Data și ora la care s-a creat fișierul
    - Data și ora la care fișierul a fost moficicat ultima dată
    - Numele original al fișierului
    - Nume aplicație
    - Versiunea aplicației
    - Producătorul aplicației
    - Descriere fișier
    - Versiunea fișierului
    - Hash-urile MD5 și SHA256 ale obiectului
    - Rezultatul verificării semnăturii fișierului
    - Numele emitentului certificatului
    - Numele titularului certificatului
    - Numărul de serie al certificatului

- Date despre scanarea AMSI:
  - Identificatorul unic al procesului care a inițiat activitatea
  - Tipul de conținut al obiectului transmis către AMSI
  - Conținutul obiectului transmis către AMSI
  - Numele obiectului
  - Hash-urile MD5 și SHA256 ale obiectului
- Date despre blocarea aplicațiilor:
  - Identificatorul unic al procesului care a inițiat blocarea aplicației
  - Identificatorul unic al procesului părinte
  - Identificatorul unic de sistem al procesului
  - Comanda utilizată pentru a porni un proces
  - ID-ul sesiunii de conectare
  - Nivelul de integritate al procesului
  - Starea procesului
  - Identificatorul unic al fișierului procesului
  - Linia de comandă a procesului
  - Lista identificatorilor unici ai fișierelor interpretate
- Date despre deschiderea fișierelor blocate:
  - Identificatorul unic al procesului care a inițiat deschiderea fișierelor
  - Identificatorii unici ai fișierului
- Date despre încărcarea driverului:
  - Identificatorul unic al driverului încărcat
- Date despre evenimente:
  - Identificatorul unic al evenimentului
  - Data și ora evenimentului
- Date despre modificarea fișierului:
  - Identificatorul unic al procesului care a inițiat modificarea fișierului
  - Identificatorii unici ai fișierului

- Tipul operațiunii de modificare
- Indicator care arată faptul că fișierul va fi șters după repornirea computerului
- Identificatorul unic al fișierului modificat
- Identificatorul unic al fișierului înainte de modificare
- Setul de semnalizatoare de biți care determină modul în care a fost deschis fișierul
- Datele despre operațiunile de pe lista de control al accesului
- Datele despre modificările titularului sau grupului principal al fișierului

- Datele despre sesiunea de conectare:
  - ID-ul sesiunii de conectare
  - Numele utilizatorului care s-a conectat
  - Tipul contului de utilizator
  - Tipul sesiunii
- Datele despre conexiunile la rețea:
  - Identificatorul unic al procesului care a inițiat conexiunea
  - Adresa IP locală utilizată pentru inițierea conexiunii
  - Adresa IP la distanță a punctului final al conexiunii
  - Direcția de conectare
  - Protocolul de transfer a datelor
  - Metoda HTTP
  - Calea fără numele gazdei
  - Numele gazdei
  - Starea dinamică a procesului în momentul conexiunii
  - Indicatorul care arată faptul că conexiunea este deschisă la nivelul soclului brut
  - Versiunea TLS utilizată în sesiunea de conectare
  - Numele serverului TLS
  - Hash-urile MD5 și SHA1 ale certificatului serverului TLS
  - Lista Numelor alternative ale subiectului (SAN) ale certificatului
  - Numele emitentului certificatului TLS

    - Numărul de serie al certificatului
    - Algoritmul de criptare utilizat
    - Datele de început și de sfârșit ale certificatului
    - Amprenta JA3 a clientului TLS
    - Amprenta JA3S a serverului
- Datele capturate în timpul monitorizării pe un port de rețea:
    - Identificatorul unic al procesului care a inițiat conexiunea
- Datele de introducere în linia de comandă:
    - Identificatorul unic al procesului care a inițiat introducerea în consolă
    - Tipul intrării în consolă
    - Textul introdus de un utilizator sau de un proces
- Date despre crearea procesului:
    - Identificatorul unic al procesului
    - Identificatorul unic al procesului părinte
    - Identificatorul unic de sistem al procesului
    - Comanda utilizată pentru a porni un proces
    - ID-ul sesiunii de conectare
    - Nivelul de integritate al procesului
    - Identificatorul unic al fișierului procesului
    - Lista identificatorilor unici ai fișierelor interpretate
    - Tipul procesului
- Date despre modulul încărcat de proces:
    - Identificatorul unic al procesului care a inițiat descărcarea
    - Calea completă către fișierul care a fost încărcat în proces
    - Identificatorul unic al fișierului modulului
    - Numele complet calificat al ansamblului .NET, dacă fișierul încărcat este un modul .NET
    - Indicatoarele ansamblului .NET definite în manifestul său

- Datele despre terminarea procesului:
  - Identificatorul unic al procesului terminat
- Date despre modificarea registrului:
  - Identificatorul unic al procesului care a inițiat modificarea registry-ului
  - Tipul operațiunii din registry
  - Calea completă către cheia de registry
  - Numele valorii dintr-o cheie de registry
  - Tipul de date stocate în valoarea cheii de registry
  - Datele specificate în valoarea cheii de registry
  - Numele cheii înainte de redenumire
  - Informațiile privind o schimbare a proprietarului cheii sau al grupului de chei primar
  - Lista modificărilor aduse listei de control al accesului (ACL) a cheii
- Date despre amenințarea detectată și procesarea acesteia:
  - Indicatorul care arată faptul că detectarea amenințărilor s-a executat în fundal
  - Verdictul privind amenințarea
  - Numele verdictului
  - Identificatorul unic al înregistrării bazei de date
  - Momentul în care înregistrarea amenințării a fost salvată în baza de date
  - Modul de procesare a amenințării
  - Tipul obiectului infectat
  - Numele obiectului infectat
  - Hash-urile MD5 și SHA256 ale obiectului
  - Identificatorul unic al obiectului infectat
  - Identificatorul unic al procesului care a descărcat obiectul infectat de pe internet
  - URL-ul de pe care a fost descărcat obiectul infectat
  - Adresa de e-mail a expeditorului care a trimis obiectul infectat
  - Protocolul de rețea prin care a fost primit obiectul infectat
  - Adresa locală de la care a fost primit obiectul infectat

- Adresa externă de la care a fost primit obiectul infectat
- Tipul de conținut al obiectului
- Conținutul obiectului

- Date despre accesul la procese:
  - Identificatorul unic al procesului care a încercat accesarea
  - Identificatorul unic al procesului țintă care a fost accesat
  - Setul de drepturi solicitate de la procesul țintă
  - Tipul operațiunii
  - Setul de apeluri în momentul accesării unui proces
  - Descriptorul procesului sursă
  - Descriptorul procesului țintă
- Date despre DNS:
  - Identificatorul unic al procesului care a inițiat interogarea DNS
  - Adresa IP a serverului DNS
  - Indicatoarele care gestionează comportamentul unei interogări DNS
  - Starea finalizării solicitării
  - Numele domeniului complet calificat specificat în interogarea DNS
  - Tipul de date din interogarea DNS
  - Răspunsurile serverului DNS
- Date despre injectarea de cod:
  - Identificatorul unic al procesului care a încercat să injecteze cod
  - Metoda de acces utilizată
  - Setul de apeluri în momentul detectării codului injectat
  - Identificatorul unic al procesului țintă în care a fost încărcat codul
  - Datele despre modificările secvenței de comenzi a procesului țintă
  - Adresa procesului țintă
  - Numele bibliotecii DLL care a fost încărcată în procesul țintă
  - Calea completă către fișierul DDL

- Date despre operațiuni cu canale denumite:
  - Identificatorul unic al procesului care a creat sau s-a conectat la canal
  - Numele complet al canalului respectiv
  - Tipul operațiunii (creare sau conectare)
- Date despre interogările WMI:
  - Identificatorul unic al procesului care a inițiat operațiunea WMI
  - Tipul operațiunii WMI
  - Numele dispozitivului țintă pentru interogarea WMI
  - Contul de utilizator care a inițiat interogarea WMI
  - Textul interogării WMI
  - Spațiul de nume în care se execută interogarea WMI
  - Numele filtrului WMI
  - Numele obiectului consumator
  - Textul care descrie acțiunea obiectului consumator
- Date despre interogările LDAP:
  - Identificatorul unic al procesului care a efectuat solicitarea LDAP
  - Domeniul de căutare al interogărilor LDAP
  - Filtrul LDAP
  - Parametrul care specifică partiția Active Directory către care a fost direcționată interogarea
  - Atributele de căutare LDAP
- Date despre dispozitivele USB conectate:
  - Tipul operațiunii dispozitivului USB
  - Tipul dispozitivului USB
  - Identificatorul dispozitivului USB
  - Numele dispozitivului USB
  - Calea către dispozitivul USB
  - Indicatorul care indică faptul că dispozitivul USB este o unitate de sistem
- Datele despre crearea, ștergerea și modificarea unei activități programate

- Datele despre crearea, ștergerea și modificarea serviciilor
- Datele despre montarea/demontarea sistemului de fișiere
- Datele despre funcționarea componentei EDR Expert on-premise:
  - Informațiile despre pornirea/oprirea agentului
  - Informațiile despre instalarea/dezinstalarea agentului
  - Identificatorul unic pentru pornirea agentului
  - Identificatorul de sistem al procesului agentului
  - Identificatorul unic al procesului agentului
  - Motivul terminării agentului
  - Codul terminării procesului agentului
- Setările de filtrare a evenimentelor:
  - Nume modul
  - Căile complete către obiecte
  - Hash-urile MD5 și SHA256 ale obiectelor
  - Identificatorii intrărilor din jurnalul de evenimente Windows
  - Setările certificatului digital
  - Direcția traficului, adresele IP, porturile, protocoalele, căile complete către fișierele executabile
  - Numele de utilizatori
  - Tipurile de conectare a utilizatorului
  - Tipurile de evenimente de telemetrie pentru care se aplică filtre

Datele din solicitările componentei EDR Expert către agentul încorporat al Kaspersky Endpoint Security:

- Setările activității generale:
  - Tip activitate
  - Setările planificării activității
  - Numele și parolele conturilor sub care pot fi executate activitățile
  - Versiunile setărilor

- Identificatorii obiectelor carantinate
- Căile către obiecte
- Hash-urile MD5 și SHA256 ale obiectelor
- Linie de comandă pentru pornirea procesului cu argumente
- Indicatorii acțiunilor suplimentare efectuate la finalizarea activităților
- Identificatorii fișierelor IOC care urmează să fie preluați de pe server
- IOC files
- Nume serviciu
- Tipul pornirii serviciului
- Directoarele pentru care trebuie să fie primite rezultatele activității *Obținerea informații investigație*
- Măștile numelor obiectelor și a extensiilor pentru activitatea *Obținere informații investigație*

- Setările izolării rețelei:
  - Tipurile de setări
  - Versiunile setărilor
  - Listele excluderilor izolării rețelei și setările excluderii: direcția traficului, adresele IP, porturile, protocoalele și căile complete către fișierele executabile
  - Indicatorii acțiunilor suplimentare
  - Ora dezactivării izolării automate
- Setările pentru prevenirea executării:
  - Tipurile de setări
  - Versiunile setărilor
  - Listele cu regulile de prevenire a executării și setările regulilor: căile către obiecte, tipurile de obiecte, hash-urile MD5 și SHA256 ale obiectelor
  - Indicatorii acțiunilor suplimentare

Datele din solicitările trimise de Kaspersky Endpoint Security către componenta EDR Expert

La integrarea cu soluția EDR Expert (on-premises), următoarele date sunt stocate local pe computer:

- În solicitările de sincronizare:
  - ID-ul unic
  - Partea de bază a adresei web a serverului
  - Numele calculatorului
  - Adresa IP a computerului
  - Adresa MAC a computerului
  - Ora locală pe computer
  - Starea de autoprotecție a Kaspersky Endpoint Security
  - Numele și versiunea sistemului de operare care este instalat pe computer
  - Versiunea Kaspersky Endpoint Security
  - Versiunile setărilor aplicației și ale setărilor activităților
  - Stările acțiunilor: identificatorii activităților, stările execuției, codurile de eroare
- În solicitările pentru obținerea fișierelor de pe server:
  - Identificatorii unici ai fișierelor
  - Identificatorul unic al Kaspersky Endpoint Security
  - Identificatorii unici ai certificatelor
  - Partea de bază a adresei web a serverului pe care este instalată componenta Central Node
  - Adresa IP a gazdei
- În rapoartele privind rezultatele executării activităților:
  - Adresa IP a gazdei
  - Informații despre obiectele detectate în timpul unei scanări IOC sau YARA
  - Indicatorii acțiunilor suplimentare efectuate la finalizarea activităților
  - Erorile de execuție a activităților și codurile returnate
  - Stările de finalizare a activităților
  - Ora de finalizare a activităților

- Versiunile setărilor utilizate pentru executarea activităților
- Informații despre obiectele trimise către server, obiectele carantinate și obiectele restaurate din carantină: căile către obiecte, hash-urile MD5 și SHA256, identificatorii obiectelor carantinate
- Informațiile despre procesele pornite sau oprite pe un computer la solicitarea serverului: PID-ul și UniquePID-ul, codul de eroare, hash-urile MD5 și SHA256 ale obiectelor
- Informațiile despre serviciile pornite sau oprite pe un computer la solicitarea serverului: numele serviciului, tipul pornirii, codul de eroare, hash-urile MD5 și SHA256 ale fișierelor imagini ale serviciilor
- Informațiile despre obiectele pentru care s-a efectuat un dump de memorie pentru o scanare YARA (căi, identificatorul fișierului dump)
- Fișierele solicitate de server

- Date despre procesele care rulează:
  - Numele fișierului executabil, inclusiv calea completă și extensia
  - Parametrii de executare automată a procesului
  - ID proces
  - ID-ul sesiunii de conectare
  - Numele sesiunii de conectare
  - Data și ora la care a fost pornit procesul
  - Hash-urile MD5 și SHA256 ale obiectului
- Date despre fișiere:
  - Cale fișier
  - Nume fișier
  - Mărimea fișierului
  - Atributele fișierului
  - Data și ora la care s-a creat fișierul
  - Data și ora la care fișierul a fost moficicat ultima dată
  - Descriere fișier
  - Numele companiei
  - Hash-urile MD5 și SHA256 ale obiectului
  - Cheia de registry (pentru punctele de executare automată)

- Date din erorile care apar atunci când au fost preluate informațiile despre obiecte:
  - Numele complet al obiectului care a fost procesat când a apărut o eroare
  - Cod eroare
- Datele din rezultatele scanării YARA:

  Agentul încorporat al Kaspersky Endpoint Security transferă automat rezultatele scanării YARA către Kaspersky Anti Targeted Attack Platform pentru a construi un lanț de dezvoltare a amenințării.

  Datele sunt stocate temporar local în coada de așteptare pentru trimiterea rezultatelor execuției activităților către serverul Kaspersky Anti Targeted Attack Platform. Datele sunt șterse din stocarea temporară odată ce au fost trimise.

  - Hash-urile MD5 și SHA256 ale fișierului
  - Numele complet al fișierului
  - Cale fișier
  - Mărimea fișierului
  - Numele procesului
  - Argumentele procesului
  - Calea către fișierul de proces
  - Identificatorul Windows (PID) al procesului
  - Identificatorul Windows (PID) al procesului părinte
  - Contul de utilizator care a pornit procesul
  - Data și ora la care a fost pornit procesul
- Datele din rezultatele scanării IOC:
  - Adresa IP din tabelul ARP
  - Adresa fizică din tabelul ARP
  - Numele înregistrării DNS
  - Tipul înregistrării DNS
  - Numele gazdei
  - Adresa IP
  - ID-ul evenimentului în jurnal
  - Numele sursei de date în jurnal
  - Nume jurnal

- Numele utilizatorului
- Data și ora la care a fost generat evenimentul, în format ISO
- Hash-urile MD5 și SHA256 ale fișierului
- Numele complet al fișierului
- Mărimea fișierului
- Adresa IP la distanță și portul la care a fost stabilită conexiunea în timpul scanării
- Adresa IP și portul plăcii locale
- Protocolul
- Numele procesului
- Argumentele procesului
- Calea către fișierul de proces
- Identificatorul Windows (PID) al procesului
- Identificatorul Windows (PID) al procesului părinte
- Contul de utilizator care a pornit procesul
- Data și ora la care a fost pornit procesul
- Calea către cheia de registry
- Nume cheie de registry
- Valoarea text a cheii de registry
- Nume serviciu
- Descrierea serviciului
- Calea și numele serviciului DLL
- Calea și numele serviciului executabil al serviciului
- Identificatorul Windows (PID) al serviciului
- Tipul serviciului
- Starea serviciului
- Modul de lansare a serviciului
- Numele sistemului de operare
- Versiunea sistemului de operare

- Nume rețelei de calculatoare fără domeniu
- Domeniul sau grupul de lucru
- Numele utilizatorului
- Numele volumului
- Litera volumului
- Tipul volumului

Kaspersky Network Detection and Response (KATA)

Toate datele pe care aplicația le stochează local pe computer sunt șterse de pe computer atunci când Kaspersky Endpoint Security este dezinstalat.

Date de telemetrie

- **Date despre fișiere**
  - Identificatorii unici ai fișierului
  - Tip de fișier
  - Calea completă a fișierului
  - Mărimea fișierului
  - Atributele fișierului
  - Identificatorul de zonă
  - Data și ora la care s-a creat fișierul
  - Data și ora la care fișierul a fost moficicat ultima dată
  - Numele original al fișierului
  - Nume aplicație
  - Versiunea aplicației
  - Producătorul aplicației
  - Descriere fișier
  - Versiunea fișierului

- Hash-urile MD5 și SHA256 ale obiectului
- Rezultatul verificării semnăturii fișierului
- Data și ora la care a fost creată semnătura fișierului
- Lanțurile de certificate utilizate în fișierul de semnătură
- Tipul lanțului de certificate
- Certificatele din lanț
- Numele emitentului certificatului
- Numele titularului certificatului
- Numărul de serie al certificatului
- Algoritmul amprentei digitale a certificatului
- Amprenta certificatului
- Perioada de valabilitate a certificatului

- **Datele despre sesiunea de conectare**
  - ID-ul sesiunii de conectare
  - Numele contului utilizatorului care s-a conectat
  - Tipul contului de utilizator
  - Tipul sesiunii
  - Adresa IP a mașinii de pe care s-a făcut încercarea de conectare
  - Adresa IP a mașinii locale pentru care s-a făcut încercarea de conectare
  - Indicatorul care arată faptul că sesiunea reprezentată de acest eveniment are privilegii sporite și drepturi de administrator
  - Parametrul care indică dacă alte sesiuni sunt legate de această sesiune de conectare
  - Protocolul utilizat pentru sesiunea terminalului
  - Protocolul IPv4 utilizat pentru sesiunea terminalului
- **Datele despre comunicarea în rețea**
  - Începutul și sfârșitul intervalului de timp în care au fost colectate datele
  - Lista conexiunilor
  - Adresa IP locală a computerului

- Adresa MAC locală a computerului
- Adresa IP la distanță a computerului
- Adresa MAC la distanță a computerului
- Adresa IP a porții de acces
- Numărul pachetelor de date transmise
- Numărul pachetelor de date recepționate
- Numărul total de octeți transferați
- Protocolul de transfer a datelor
- Câmpul EtherType al cadrului Ethernet
- Prefixul sarcinii primului pachet din interval
- Adresa IPv4 a interfeței de rețea prin care a fost capturată comunicarea

- **Datele despre conexiunea la rețea**
  - Identificatorul unic al procesului care a inițiat conexiunea
  - Protocolul de transfer a datelor
  - Adresa IP locală utilizată pentru inițierea conexiunii
  - Adresa IP la distanță a punctului final al conexiunii
  - Metoda HTTP
  - Calea fără numele gazdei
  - Numele gazdei
  - Starea dinamică a procesului în momentul conexiunii
  - Direcția de conectare
  - Starea dinamică a procesului
  - Câmpul EtherType al cadrului Ethernet
- **Datele capturate în timpul monitorizării pe un port de rețea**
  - Identificatorul unic al procesului care a inițiat conexiunea
  - Protocolul de transfer a datelor
  - Adresa locală
  - Starea dinamică a procesului în momentul conexiunii

- **Rezultatul verificării conexiunii**
  - Setările de rețea ale gazdei
  - Descrierea interfeței de rețea
  - Numele domeniului DNS
  - Adresa MAC locală a computerului
  - Metrica conexiunii IP
  - Lista adreselor IP
  - Adresa IP
  - Masca de rețea
  - Adresa IP a porții de acces
  - Adresa MAC a porții de acces
  - Lista corecțiilor instalate
  - Numărul corecției
  - Data instalării corecției
  - Modelul dispozitivului
  - Vânzătorul dispozitivului
  - ID-ul gazdei în Kaspersky Security Center
  - Descrierea antivirusului Kaspersky instalat
  - Numele componentei antivirusului Kaspersky instalat
  - Versiunea componentei antivirusului Kaspersky instalat
  - Versiunea bazei de date a componentei antivirus Kaspersky instalate
  - Data ultimei actualizări a bazei de date a componentei antivirus Kaspersky instalate
  - Starea componentelor antivirusului Kaspersky instalat
  - Lista cheilor de licență
  - Numărul de serie al cheii
  - Tipul cheii

- Data expirării cheii
- Starea cheii

- **Datele despre crearea procesului pe gazdă**
  - Identificatorul unic al procesului
  - Identificatorul unic al procesului părinte
  - Identificatorul unic de sistem al procesului
  - Comanda utilizată pentru a porni un proces
  - ID-ul sesiunii de conectare
  - ID-ul sesiunii terminalului
  - Identificatorul unic al fișierului procesului
  - Nivelul de integritate al procesului
  - Lista tokenurilor drepturilor proceselor
  - Drepturile atributelor
  - Lista identificatorilor unici ai fișierelor interpretate
  - Starea procesului
  - Comanda utilizată pentru a porni un proces
- **Datele despre terminarea procesului**
  - Identificatorul unic al procesului
- **Datele despre amenințarea detectată**
  - Informațiile despre amenințări
  - Verdictul privind amenințarea
  - Numărul înregistrării AMR
  - Versiunea bazei de date antivirus
  - Tehnologiile de detectare a amenințărilor
  - Identificatorul unic al amenințării
  - Tehnologia de protecție
  - Informațiile despre obiectul infectat
  - Tipul obiectului infectat

- Numele obiectului infectat
- Hash-urile MD5 și SHA256 ale obiectului
- Identificatorul unic al procesului infectat
- Identificatorul unic al obiectului infectat
- Identificatorul unic al procesului care a descărcat obiectul infectat de pe internet
- URL-ul de pe care a fost descărcat obiectul infectat
- Adresa de e-mail a expeditorului care a trimis obiectul infectat
- Protocolul de rețea prin care a fost primit obiectul infectat
- Adresa locală de la care a fost primit obiectul infectat
- Adresa externă de la care a fost primit obiectul infectat
- Tipul de conținut al obiectului
- Contextul amenințării detectate
- Conținutul obiectului
- Indicatorul care arată faptul că detectarea amenințărilor s-a executat în fundal

- **Datele despre procesarea amenințărilor**
  - Informațiile despre amenințări
  - Verdictul privind amenințarea
  - Numărul înregistrării AMR
  - Versiunea bazei de date antivirus
  - Tehnologiile de detectare a amenințărilor
  - Numele obiectului infectat
  - Hash-urile MD5 și SHA256 ale obiectului
  - Identificatorul unic al procesului infectat
  - Identificatorul unic al obiectului infectat
  - Protocolul de rețea prin care a fost primit obiectul infectat
  - Adresa locală de la care a fost primit obiectul infectat
  - Adresa externă de la care a fost primit obiectul infectat
  - Starea procesării amenințării

- Motivul pentru care amenințarea nu a putut fi remediată
- Adresa fizică locală

- **Datele despre utilizatori**
  - SID-ul utilizatorului
  - ID-ul utilizatorului
  - Numele utilizatorului
  - Numele complet al utilizatorului
  - Descrierea utilizatorului
  - Dacă contul este activ sau blocat
  - Dacă parola a expirat
  - Dacă este necesară o schimbare a parolei
  - Dacă este permisă schimbarea parolei
  - Tipul contului de utilizator
  - Dacă este activată autentificarea automată pentru acest cont
  - Lista grupurilor din care face parte utilizatorul

Integrare cu Kaspersky Unified Monitoring and Analysis Platform (KUMA)

Toate datele pe care aplicația le stochează local pe computer sunt șterse de pe computer atunci când Kaspersky Endpoint Security este dezinstalat.

La integrarea cu Kaspersky Unified Monitoring and Analysis Platform (KUMA), sunt transferate datele setărilor conexiunii, precum și toate evenimentele înregistrate în Jurnalele Windows.

Principalele jurnale de evenimente Windows sunt Sistem, Securitate, Aplicații, Evenimente redirecționate și Evenimente hardware. Utilizatorii pot, de asemenea, să creeze și să lucreze cu jurnale personalizate pentru a satisface cerințele lor specifice.

Respectarea legislației Uniunii Europene (GDPR)

Kaspersky Endpoint Security poate transmite date către Kaspersky în următoarele scenarii:

- Utilizarea Kaspersky Security Network.
- Activarea aplicației folosind un cod nou de activare.

- Actualizarea modulelor aplicației și a bazelor de date antivirus.
- Accesarea linkurilor din interfața aplicației.

Indiferent de clasificarea datelor și de teritoriul din care sunt primite datele, Kaspersky respectă standarde înalte de securitate a datelor și utilizează diverse măsuri legale, organizatorice și tehnice pentru a proteja datele utilizatorilor, pentru a garanta securitatea și confidențialitatea datelor, precum și pentru a asigura onorarea drepturilor utilizatorilor, astfel cum sunt garantate de legislația aplicabilă. Textul Politicii de confidențialitate este inclus în kitul de distribuire a aplicației și este disponibil pe site-ul web Kaspersky.

Înainte de a utiliza Kaspersky Endpoint Security, citiți cu atenție descrierea datelor transmise în Acordul de licență pentru utilizatorul final și în Declarația Kaspersky Security Network. Dacă anumite date transmise de la Kaspersky Endpoint Security în oricare dintre scenariile descrise pot fi clasificate drept date cu caracter personal în conformitate cu legislația sau standardul local, trebuie să vă asigurați că aceste date sunt procesate legal și să obțineți consimțământul utilizatorilor finali pentru colectarea și transmiterea unor asemenea date.

Citește Acordul de licență pentru utilizatorul final și vizitează site-ul Web Kaspersky pentru a afla mai multe despre cum primim, procesăm, depozităm și distrugem informații despre utilizarea aplicației după ce accepți Acordul de licență pentru utilizatorul final și ești de acord cu Kaspersky Security Network Statement. Fișierele license.txt și ksn_<ID limbă>.txt conțin textul Acordului de licență pentru utilizatorul final și Kaspersky Security Network Statement și sunt incluse kitul de distribuire al aplicației.

Dacă nu doriți să transmiteți date către Kaspersky, puteți dezactiva furnizarea de date.

Despre Kaspersky Security Network

Prin utilizarea Kaspersky Security Network, sunteți de acord să furnizați automat datele listate în Declarația Kaspersky Security Network. Dacă nu sunteți de acord să furnizați aceste date către Kaspersky, utilizați Kaspersky Private Security Network (KPSN) sau dezactivați utilizarea KSN. Pentru mai multe detalii despre KPSN, consultați documentația cu privire la Kaspersky Private Security Network.

Activarea aplicației folosind un cod nou de activare

Utilizând un cod de activare, sunteți de acord să furnizați automat datele listate în Acordul de licență pentru utilizatorul final. Dacă nu sunteți de acord să transmiți aceste informații către Kaspersky, trebuie să folosiți un fișier cheie pentru a activa aplicația Kaspersky Endpoint Security.

Actualizarea modulelor aplicației și a bazelor de date antivirus

Utilizând serverele Kaspersky, sunteți de acord să furnizați automat datele listate în Acordul de licență pentru utilizatorul final. Kaspersky are nevoie de aceste informații pentru a verifica dacă Kaspersky Endpoint Security este utilizat în mod legitim. Dacă nu sunteți de acord să furnizați aceste informații către Kaspersky, utilizați Kaspersky Security Center pentru actualizări ale bazei de date sau Kaspersky Update Utility.

Accesarea linkurilor din interfața aplicației

Utilizând linkurile din interfața aplicației, sunteți de acord să furnizați automat datele listate în Acordul de licență pentru utilizatorul final. Lista exactă a datelor transmise în fiecare link specifică depinde de locul în care se află legătura în interfața aplicației și de problema pe care intenționează să o rezolve. Dacă nu sunteți de acord să furnizați aceste date Kaspersky, utilizați interfața simplificată a aplicației sau ascundeți interfața aplicației.

Scrierea imaginilor

Dacă ați activat scrierea imaginilor, Kaspersky Endpoint Security va crea un fișier imagine care va conține toate datele de memorie din procesele aplicației în momentul creării acestui fișier imagine.

Note privind mărcile comerciale

Mărcile comerciale înregistrate și mărcile de servicii sunt proprietatea titularilor respectivi.

Adobe, Acrobat, Flash, Reader și Shockwave sunt fie mărci comerciale înregistrate, fie mărci comerciale ale Adobe în Statele Unite ale Americii și/sau în alte țări.

Amazon, Amazon Web Services, AWS sunt mărci comerciale ale Amazon.com, Inc. sau ale afiliaților săi.

Apple, FireWire, iTunes, Mac și Safari sunt mărci comerciale ale Apple Inc.

Arm este o marcă comercială înregistrată a Arm Limited (sau a filialelor sale) în SUA și/sau în alte țări.

AutoCAD este o marcă comercială sau o marcă comercială înregistrată a Autodesk, Inc. și/sau a companiilor sale afiliate în Statele Unite ale Americii și în alte țări.

Cuvântul Bluetooth, marca și logo-ul sunt proprietatea Bluetooth SIG, Inc.

Borland este marca comercială sau marca comercială înregistrată a Borland Software Corporation.

Cisco, Cisco AnyConnect și IOS sunt mărci comerciale înregistrate sau mărci comerciale ale Cisco Systems, Inc. și/sau ale afiliaților săi din Statele Unite ale Americii și din anumite alte țări.

Citrix, Citrix Provisioning, Citrix Provisioning Services, Citrix Virtual Apps and Desktop, XenDesktop, și XenServer sunt fie mărci comerciale înregistrate, fie mărci comerciale ale Cloud Software Group, Inc. și/sau ale filialelor sale din Statele Unite și/sau alte țări.

Cloudflare, Cloudflare Workers și sigla Cloudflare sunt mărci comerciale și/sau mărci comerciale înregistrate ale Cloudflare, Inc. În Statele Unite ale Americii și în alte jurisdicții.

Core este marca comercială a Intel Corporation sau a filialelor sale.

dBase este o marcă comercială a dataBased Intelligence, Inc.

Dell Technologies, Dell, EMC și alte mărci comerciale sunt mărci comerciale ale Dell Inc. Sau ale filialelor sale.

Docker și emblema Docker sunt mărci comerciale sau mărci comerciale înregistrate ale Docker, Inc. în Statele Unite ale Americii și/sau în alte țări. Docker, Inc. și alte părți pot avea, de asemenea, drepturi de marcă comercială în alți termeni utilizați aici.

ESET este o marcă comercială sau o marcă comercială înregistrată a ESET spol. s r.o. sau a respectivei entități ESET.

Foxit este o marcă comercială înregistrată a Foxit Corporation.

Radmin este o marcă comercială înregistrată a Famatech.

Google, Android, Google Public DNS, Google Chrome și Chrome sunt mărci comerciale ale Google LLC.

HUAWEI, FusionCompute și FusionSphere sunt mărci comerciale ale Huawei Technologies Co., Ltd.

ICQ este o marcă comercială și/sau o marcă de serviciu a ICQ LLC.

Intel este marca comercială a Intel Corporation sau a filialelor sale.

IBM este o marcă comercială a International Business Machines Corporation, înregistrată în multe jurisdicții din lume.

Lenovo și Lenovo ThinkPad sunt mărci comerciale ale Lenovo în Statele Unite ale Americii și/sau în alte țări.

Linux este marcă comercială înregistrată a Linus Torvalds în Statele Unite ale Americii și în alte țări.

Logitech fie marcă comercială înregistrată, fie marcă comercială a Logitech în Statele Unite ale Americii și/sau în alte țări.

LogMeIn Pro și Remotely Anywhere sunt mărci comerciale ale LogMeIn, Inc.

Mail.ru este o marcă comercială a Mail.ru LLC.

McAfee este marcă comercială sau marcă comercială înregistrată a McAfee LLC sau a filialelor sale din SUA și/sau din alte țări.

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 și Windows Store sunt mărci comerciale ale grupului de companii Microsoft.

Mozilla, Firefox și Thunderbird sunt mărci comerciale ale Mozilla Foundation în S.U.A. și în alte țări.

NetApp este o marcă comercială sau o marcă comercială înregistrată a NetApp, Inc. în Statele Unite ale Americii și/sau în alte țări.

OpenSSL este o marcă comercială deținută de OpenSSL Software Foundation.

OpenStack este o marcă comercială înregistrată a OpenStack Foundation în Statele Unite ale Americii și în alte țări.

Oracle, Java și JavaScript sunt mărci comerciale înregistrate ale Oracle și/sau ale companiilor sale afiliate.

Python este o marcă comercială sau o marcă comercială înregistrată a Python Software Foundation.

Realtek este o marcă comercială a Realtek Semiconductor Corporation.

SAMSUNG este o marcă comercială a SAMSUNG în Statele Unite ale Americii sau în alte țări.

Thawte este o marcă comercială sau o marcă comercială înregistrată a Symantec Corporation sau a companiilor sale afiliate din Statele Unite ale Americii și din alte țări.

Trend Micro este o marcă comercială sau o marcă comercială înregistrată a Trend Micro Incorporated.

VERISIGN este o marcă comercială înregistrată în Statele Unite și în alte țări sau o marcă comercială neînregistrată a VeriSign, Inc. și a filialelor sale.

VMware, VMware ESXi, VMware Horizon, VMware Workstation, VMware Tools, VMware vSphere sunt mărci comerciale înregistrate și/sau mărci comerciale ale VMware, Inc. în Statele Unite și în alte țări.

Informații despre codurile de la terți

Informațiile despre codurile de la terți sunt conținute în fișierul legal_notices.txt, aflat în directorul de instalare al aplicației.