kaspersky

Kaspersky Endpoint Security for Windows 11.6.0

Cuprins

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 de viruși 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 sociale?

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?

Noutăți

Actualizare 11.6.0

Kaspersky Endpoint Security 11.6.0 for Windows oferă următoarele caracteristici și îmbunătățiri:

1. Compatibilitate pentru Windows 10 21H1. Pentru detalii referitoare la suportul pentru sistemul de operare Microsoft Windows 10, consultați Baza de cunoștințe a Serviciului de asistență tehnică.

2. Componenta Managed Detection and Response a fost adăugată. Această componentă facilitează interacțiunea cu soluția cunoscută drept Kaspersky Managed Detection and Response. Componenta *Kaspersky Managed Detection and Response (MDR)* asigură protecție continuă împotriva unui număr în creștere de amenințări capabile să treacă de mecanismele de protecție automate pentru organizații cărora le este dificil să găsească experți foarte calificați sau care dispun de resurse interne limitate. Pentru informații detaliate despre modul în care funcționează soluțiile, *consultați Ghidul de ajutor Kaspersky Managed Detection and Response*.

3. Kaspersky Endpoint Agent, inclus în kitul de distribuție, a fost actualizat la versiunea 3.10. Kaspersky Endpoint Agent 3.10 oferă caracteristici noi, rezolvă unele probleme anterioare și dispune de stabilitate îmbunătățită. Pentru mai multe detalii despre aplicație, consultați documentația soluțiilor Kaspersky compatibile cu Kaspersky Endpoint Agent.

4. Acum oferă capabilitatea de a gestiona protecția împotriva atacurilor precum Supraîncărcare rețea și Scanare port în setările Network Threat Protection.

5. S-a adăugat o nouă metodă de creare a regulilor de rețea pentru Firewall. Puteți adăuga reguli de pachete și reguli de aplicație pentru conexiunile care sunt afișate în fereastra Monitor rețea. Cu toate acestea, setările conexiunii pentru regula de rețea vor fi configurate automat.

6. Interfața Monitor rețea este acum îmbunătățită. S-au adăugat informații despre activitatea de rețea: ID-ul procesului, care inițiază activitatea de rețea; tipul de rețea (rețea locală sau internet); porturile locale. În mod implicit, informațiile despre tipul de rețea sunt ascunse.

7. Acum există capabilitatea de creare automată a conturilor Agent de autentificare pentru utilizatorii Windows noi. Agentul permite unui utilizator să finalizeze autentificarea pentru accesul la unitățile care au fost criptate utilizând tehnologia Kaspersky Disk Encryption și să încarce sistemul de operare. Informații privind sumele de verificare ale aplicației despre conturile utilizatorilor Windows de pe computer. 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. Prin urmare, nu trebuie să adăugați manual conturi Agent de autentificare pentru computerele cu unitățile de hard disk deja criptate.

8. Acum există capabilitatea să monitorizați procesul de criptare a discului în interfața aplicației pe computerele utilizatorilor (Kaspersky Disk Encryption și BitLocker). Puteți executa instrumentul Monitor criptare din fereastra principală a aplicației.

Actualizare 11.5.0

Kaspersky Endpoint Security 11.6.0 for Windows oferă următoarele caracteristici și îmbunătățiri:

1. Compatibilitate pentru Windows 10 20H2. Pentru detalii referitoare la suportul pentru sistemul de operare Microsoft Windows 10, consultați Baza de cunoștințe a Serviciului de asistență tehnică.

2. Interfață aplicație actualizată. De asemenea, au fost actualizate pictograma aplicației din zona de notificare, notificările aplicației și casetele de dialog.

3. Interfață îmbunătățită a plug-inului web Kaspersky Endpoint Security pentru componentele Application Control, Control dispozitive și Control adaptiv al anomaliilor.

4. Funcționalitate adăugată pentru importul și exportul listelor de reguli și excluderi în format XML. Formatul XML vă permite să editați listele după ce acestea sunt exportate. Puteți gestiona listele numai în consola Kaspersky Security Center. Următoarele liste sunt disponibile pentru export/import:

   - Behavior Detection (listă de excluderi).
   - Web Threat Protection (lista adreselor URL de încredere).
   - Mail Threat Protection (lista extensiilor de filtru de atașament).
   - Network Threat Protection (listă de excluderi).
   - Firewall (lista regulilor pachetelor de rețea).
   - Application Control (lista regulilor).
   - Control Web (listă de reguli).
   - Monitorizarea porturilor de rețea (liste de porturi și aplicații monitorizate de Kaspersky Endpoint Security).
   - Kaspersky Disk Encryption (listă de excluderi).
   - Criptare unități amovibile (listă de reguli).

5. Informațiile MD5 despre obiect au fost adăugate la raportul de detectare a amenințărilor. În versiunile anterioare ale aplicației, Kaspersky Endpoint Security afișa doar hashul SHA256 al unui obiect.

6. S-a adăugat capacitatea de a atribui prioritatea regulilor de acces la dispozitiv în setările Control dispozitive. Atribuirea priorității permite configurarea mai flexibilă a accesului utilizatorului la dispozitive. 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. De exemplu, puteți acorda permisiuni numai de citire grupului Oricine și acorda permisiuni de citire/scriere grupului de administratori. Pentru aceasta, atribuiți o prioritate 0 pentru grupul de administratori și atribuiți o prioritate de 1 pentru grupul Oricine. Puteți configura prioritatea numai pentru dispozitivele care au un sistem de fișiere. Aceasta include hard diskuri, unități amovibile, dischete, unități CD/DVD și dispozitive portabile (MTP).

7. Funcționalitate nouă adăugată:

   - Gestionare notificări audio.
   - Comunicațiile în rețea sensibile la costuri Kaspersky Endpoint Security își limitează propriul trafic de rețea dacă conexiunea la internet este limitată (de exemplu, printr-o conexiune mobilă).
   - Gestionați setările Kaspersky Endpoint Security prin aplicații de gestionare la distanță de încredere (cum ar fi TeamViewer, LogMeIn Pro și Remotely Anywhere). Puteți utiliza aplicații de administrare la distanță pentru a porni Kaspersky Endpoint Security și pentru a gestiona setările din interfața aplicației.
   - Gestionați setările pentru scanarea traficului securizat în Firefox și Thunderbird. Puteți selecta stocarea certificatelor care va fi utilizată de Mozilla: stocarea certificatelor Windows sau stocarea certificatelor Mozilla. Această funcționalitate este disponibilă numai pentru computerele care nu au o politică aplicată. Dacă se aplică o politică unui computer, Kaspersky Endpoint Security permite automat utilizarea stocării certificatelor Windows în Firefox și Thunderbird.

8. Capacitate adăugată de configurare a modului de scanare securizată a traficului: scanează întotdeauna traficul chiar dacă componentele de protecție sunt dezactivate sau scanează traficul când este solicitat de componentele de protecție.

9. Procedură revizuită pentru ștergerea informațiilor din rapoarte. Un utilizator poate șterge numai toate rapoartele. În versiunile anterioare ale aplicației, un utilizator putea selecta anumite componente ale aplicației ale căror informații vor fi șterse din rapoarte.

10. Procedură revizuită pentru importul unui fișier de configurare care conține setările Kaspersky Endpoint Security și procedură revizuită pentru restabilirea setărilor aplicației. Înainte de import sau restaurare, Kaspersky Endpoint Security afișează doar un avertisment. În versiunile anterioare ale aplicației, puteați vedea valorile noilor setări înainte de a fi aplicate.

11. Procedură simplificată pentru restabilirea accesului la o unitate care a fost criptată de BitLocker. După finalizarea procedurii de recuperare a accesului, Kaspersky Endpoint Security îi solicită utilizatorului să seteze o nouă parolă sau un nou cod PIN. După setarea unei parole noi, BitLocker va cripta unitatea. În versiunea anterioară a aplicației, utilizatorul a trebuit să reseteze manual parola în setările BitLocker.

12. Utilizatorii au acum capacitatea de a-și crea 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. Un administrator poate permite sau bloca utilizarea excluderilor locale sau a aplicațiilor locale de încredere. Un administrator poate utiliza Kaspersky Security Center pentru a vizualiza, adăuga, edita sau șterge elemente de listă din proprietățile computerului.

13. S-a adăugat capacitatea de a introduce comentarii în proprietățile aplicațiilor de încredere. Comentariile simplifică căutările și sortarea aplicațiilor de încredere.

14. Gestionarea aplicației prin REST API:

    - Există acum capacitatea de a configura setările extensiei Mail Threat Protection pentru Outlook.

    - Este interzisă dezactivarea detectării virușilor, viermilor și troienilor.

Actualizare 11.4.0

Kaspersky Endpoint Security 11.4.0 for Windows oferă următoarele caracteristici și îmbunătățiri:

1. Design nou al pictogramei aplicației în zona de notificare a barei de activități. Noul  este acum afișat în locul pictogramei vechi  . Dacă utilizatorul este obligat să efectueze o acțiune (de exemplu, să repornească computerul după actualizarea aplicației), pictograma se va schimba în  . În cazul în care componentele de protecție ale aplicației sunt dezactivate sau au funcționat defectuos, pictograma se va schimba în  sau  . Dacă treceți cu mouse-ul peste pictogramă, Kaspersky Endpoint Security va afișa o descriere a problemei în protecția computerului.

2. Kaspersky Endpoint Agent, inclus în kitul de distribuție, a fost actualizat la versiunea 3.9. Kaspersky Endpoint Agent 3.9 acceptă integrarea cu noile soluții Kaspersky. Pentru mai multe detalii despre aplicație, consultați documentația soluțiilor Kaspersky compatibile cu Kaspersky Endpoint Agent.

3. S-a adăugat starea *Nu este acceptată de licență* pentru componentele Kaspersky Endpoint Security. Puteți vizualiza starea componentelor făcând clic pe butonul **Componente de protecție** în fereastra principală a aplicației.

4. Noile evenimente din Exploit Prevention au fost adăugate în Rapoarte.

5. Driverele pentru tehnologia Kaspersky Disk Encryption sunt acum adăugate automat la Windows Recovery Environment (WinRE) atunci când este pornită criptarea unității. Versiunea anterioară a Kaspersky Endpoint

Security a adăugat drivere la instalarea aplicației. Adăugarea de drivere în WinRE poate îmbunătăți stabilitatea aplicației atunci când restaurați sistemul de operare pe computere protejate de tehnologia Kaspersky Disk Encryption.

Componenta Senzor Endpoint a fost eliminată din Kaspersky Endpoint Security. Puteți configura totuși setările componentei Senzor Endpoint într-o politică, cu condiția ca Kaspersky Endpoint Security versiunea 11.0.0 până la 11.3.0 să fie instalată pe computer.

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.

Pentru a vă proteja computerul, Kaspersky Endpoint Security utilizează următoarele tehnologii de detectare a menințărilor:

- **Tehnologie Machine learning**. Kaspersky Endpoint Security utilizează un model pentru tehnologia machine learning. Acest model a fost dezvoltat de experții Kaspersky. Pe parcursul utilizării, modelul continuă să primească date actualizate despre amenințări de la KSN, instruind astfel modelul.

- **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 expert**. Kaspersky Endpoint Security utilizează datele despre amenințări adăugate de analiștii de viruși ai Kaspersky. Analiștii de viruși verifică 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 primite de Kaspersky și apoi determină reputația obiectelor și adaugă datele corespunzătoare în baza de date antivirus. Dacă sistemul nu poate determina reputația unui obiect, acesta trimite o solicitare către analiștii de viruși ai Kaspersky.

- **Kaspersky Sandbox**. Kaspersky Endpoint Security scanează obiectele de pe o mașină virtuală. Kaspersky Sandbox analizează comportamentul unui obiect și ia o decizie privind reputația acestuia. Această tehnologie este disponibilă doar dacă utilizați Kaspersky Sandbox.

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.

Următoarele componente ale aplicației reprezintă componente de control:

- **Application Control**. Această componentă monitorizează încercările utilizatorilor de a porni aplicații și reglementează pornirea aplicațiilor.

- **Control dispozitive**. Această componentă îți permite să configurezi restricții flexibile privind accesul la dispozitive de stocare a datelor (precum unitățile de hard disk, unitățile amovibile și discurile CD/DVD), echipamente pentru transmitere de date (precum modemurile), echipamente de convertire a informațiilor (precum imprimantele) sau interfețe pentru conectarea de dispozitive la computere (precum USB și Bluetooth).

- **Control Web**. Această componentă îți permite să setezi restricții flexibile asupra accesului la resursele Web pentru diverse grupuri de utilizatori.

- **Control adaptiv al anomaliilor**. Această componentă monitorizează și controlează acțiunile potențial dăunătoare care nu sunt tipice pentru computerul protejat.

Următoarele componente ale aplicației reprezintă componentele protecției:

- **Behavior Detection**. Această componentă primește informații despre acțiunile aplicațiilor de pe computer și transmite aceste informații altor componente pentru o protecție mai eficientă.

- **Exploit Prevention**. Această componentă urmărește fișierele executabile care sunt executate de aplicații vulnerabile. Atunci când se încearcă executarea unui fișier executabil de către o aplicație vulnerabilă, executare

care nu a fost inițiată de utilizator, Kaspersky Endpoint Security blochează executarea acestui fișier.

- **Host Intrusion Prevention**. Această componentă înregistrează acțiunile aplicațiilor în sistemul de operare și reglementează activitatea aplicațiilor în funcție de grupul de încredere din care face parte o anumită aplicație. Pentru fiecare grup de aplicații este specificat un set de reguli. Aceste reguli reglementează accesul aplicațiilor la datele utilizatorului și la resursele sistemului de operare. Aceste date includ fișiere de-ale utilizatorului din directorul Documents (Documente), module cookie, fișiere jurnal despre activitatea utilizatorului și fișiere, directoare și chei de registru care conțin setări și informații importante pentru aplicațiile utilizate cel mai frecvent.

- **Remediation Engine**. Această componentă permite Kaspersky Endpoint Security să deruleze înapoi acțiuni care au fost executate de către programe malware în sistemul de operare.

- **File Threat Protection**. Această componentă protejează sistemul de fișiere al computerului împotriva infectării. Componenta pornește imediat după lansarea Kaspersky Endpoint Security, rămâne permanent activă în memoria RAM a computerului și scanează toate fișierele deschise, salvate sau lansate pe computer și pe toate dispozitivele de stocare conectate. Această componentă interceptează orice încercare de accesare a unui fișier și scanează fișierul pentru a detecta virușii și alte amenințări.

- **Web Threat Protection**. Această componentă scanează traficul care ajunge pe computerul utilizatorului prin protocoalele HTTP și FTP și verifică dacă adresele Web sunt rău intenționate sau de phishing.

- **Mail Threat Protection**. Această componentă scanează mesajele de e-mail primite și trimise pentru a detecta virușii și alte amenințări.

- **Network Threat Protection**. Această componentă inspectează traficul de intrare al rețelei pentru a detecta activități tipice atacurilor de rețea. Atunci când este detectată o încercare de atac de rețea care are drept țintă computerul tău, Kaspersky Endpoint Security blochează activitatea de rețea de la computerul agresor.

- **Firewall**. Această componentă protejează datele stocate pe computer și blochează majoritatea amenințărilor posibile pentru sistemul de operare, atunci când computerul este conectat la Internet sau la o rețea locală.

- **BadUSB Attack Prevention**. Această componentă împiedică dispozitivele USB infectate care emulează o tastatură să se conecteze la computer.

- **Protecție AMSI**. Această componentă scanează obiecte pe baza unei solicitări din partea aplicațiilor terțe și notifică aplicația solicitantă cu privire la rezultatul scanării.

În afară de protecția în timp real pe care o oferă componentele aplicației, vă recomandăm să *scanați computerul* în mod regulat în vederea detectării virușilor și a altor amenințări. Acest lucru ajută la excluderea posibilității de răspândire de programe malware care nu au fost detectate de componentele de protecție, de exemplu din cauza unui nivel scăzut de securitate.

Pentru a menține protecția computerului actualizată, trebuie să *actualizați bazele de date și modulele* pe care le utilizează aplicația. Aplicația se actualizează automat în mod implicit, dar, dacă este necesar, poți actualiza manual bazele de date și modulele aplicației.

Kaspersky Endpoint Security pune la dispoziție următoarele activități:

- **Verificare integritate**. 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.

- **Scanare completă**. Kaspersky Endpoint Security scanează sistemul de operare, inclusiv memoria kernel, obiectele încărcate la pornirea sistemului de operare, sectoarele de boot ale discului, zona de copii de rezervă a sistemului de operare, precum și toate unitățile de hard disk și unitățile amovibile.

- **Scanare particularizată**. Kaspersky Endpoint Security scanează obiectele selectate de utilizator.

- **Scanare zone critice**. Kaspersky Endpoint Security scanează memoria kernel, obiectele încărcate la pornirea sistemului de operare și sectoarele de boot ale discului.

- **Actualizare**. 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.

- **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.

Funcții de service ale aplicației

Kaspersky Endpoint Security include un număr de funcții de depanareservice. Funcțiile de servicedepanare sunt furnizate pentru a asigura actualizarea aplicației, a extinde funcționalitatea ei și a ajuta utilizatorul în folosirea aplicației.

- **Rapoarte**. În cursul funcționării, aplicația ține evidența componentelor sale creând câte un raport pentru fiecare. Poți utiliza, de asemenea, rapoartele pentru a urmări rezultatele activităților finalizate. Rapoartele conțin liste de evenimente care au avut loc în timpul funcționării Kaspersky Endpoint Security și toate operațiile efectuate de aplicație. În cazul unui incident, poți trimite rapoarte la Kaspersky, unde specialiștii serviciului de asistență tehnică vor analiza problema în mod detaliat.

- **Zonă de stocare a datelor**. Dacă aplicația detectează fișiere infectate la scanarea computerului în vederea detectării de viruși și alte amenințări, fișierele respective sunt blocate. Kaspersky Endpoint Security stochează copiile fișierelor dezinfectate și șterse în *Copii de rezervă*. Kaspersky Endpoint Security mută fișierele neprocesate (indiferent de motiv) în *lista de amenințări active*. Poți scana fișiere, poți restaura fișiere în directoarele lor inițiale și poți goli zona de stocare a datelor.

- **Serviciul de notificare**. Serviciul de notificare ajută utilizatorul să urmărească evenimentele care influențează starea de protecție a computerului și funcționarea Kaspersky Endpoint Security. Notificările pot fi afișate pe ecran sau pot fi trimise prin e-mail.

- **Kaspersky Security Network**. Participarea utilizatorilor la Kaspersky Security Network eficientizează protejarea computerelor prin utilizarea în timp real a informațiilor privind reputația fișierelor, resurselor Web și software-urilor primite de la utilizatori din întreaga lume.

- **Licență**. Achiziționarea unei licențe deblochează funcționalitatea completă a aplicației, oferă acces la actualizările bazei de date și ale modulelor aplicației și asistență prin telefon sau prin e-mail cu privire la instalarea, configurarea și utilizarea aplicației.

- **Asistență**. Toți utilizatorii înregistrați ai aplicației Kaspersky Endpoint Security pot contacta serviciul de asistență tehnică pentru a primi asistență. Poți să trimiți o solicitare la Serviciul de asistență tehnică Kaspersky prin intermediul portalului Kaspersky CompanyAccount sau să apelezi telefonic Serviciul de asistență tehnică.

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.

Kitul de distribuire

Kitul de distribuire include următoarele pachete de distribuire:

- **Strong encryption (AES256)**

  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.

- **Lite encryption (AES56)**

  Acest pachet de distribuire conține instrumente criptografice care implementează algoritmul de criptare AES cu o lungime efectivă a cheii de 56 de biți.

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 a Plug-inului de gestionare Kaspersky Endpoint Security pentru Kaspersky Security Center.
`bases.cab`	Fișiere ale pachetului de actualizare utilizate în timpul instalării.
`cleaner.cab`	Fișiere pentru eliminarea software-urilor incompatibile.
`incompatible.txt`	Fișier care conține o listă de software-uri incompatibile.
`ksn_<language_ID>.txt`	Fișiere unde poți 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.
`endpointagent.msi`	Pachet de instalare pentru Kaspersky Endpoint Agent versiunea 3.10, aplicația necesară pentru integrarea cu alte soluții Kaspersky (de exemplu, Kaspersky Sandbox).
`NDP<versiune>-<pproprietăți pachet>`	Pachet de instalare Microsoft .NET Framework.
`keswin_web_plugin.zip`	Arhivă care conține fișierele necesare pentru instalarea plug-inului web Kaspersky Endpoint Security.

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

Cerințe hardware și software

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

Cerințe minime generale:

- 2 GB spațiu liber pe unitatea de hard disk
- Procesor:
  - Stație de lucru: 1 GHz
  - Server: 1.4 GHz
  - Compatibilitate pentru setul de instrucțiuni SSE2
- RAM:
  - Stație de lucru (x86): 1 GO
  - Stație de lucru (x64): 2 GO
  - Server: 2 GO
- Microsoft .NET Framework 4.0 sau o versiune mai recentă

Sisteme de operare acceptate pentru stații de lucru:

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 sau o versiune ulterioară;
- Windows 8 Professional/Enterprise;
- Windows 8.1 Professional/Enterprise;
- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise.

Algoritmul de semnare a modulului SHA-1 a fost retras de Microsoft. Actualizarea KB4474419 este necesară pentru instalarea cu succes a Kaspersky Endpoint Security pe un computer care rulează sistemul de operare Microsoft Windows 7. Pentru mai multe detalii despre această actualizare, vizitați site-ul web de asistență tehnică Microsoft.

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

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 sau o versiune ulterioară;
- Windows Server 2012 Foundation/Essentials/Standard/Datacenter;
- Windows Server 2012 R2 Foundation/Essentials/Standard/Datacenter;
- Windows Server 2016 Essentials/Standard/Datacenter;
- Windows Server 2019 Essentials/Standard/Datacenter.

Algoritmul de semnare a modulului SHA-1 a fost retras de Microsoft. Actualizarea KB4474419 este necesară pentru instalarea cu succes a Kaspersky Endpoint Security pe un computer care rulează sistemul de operare Microsoft Windows Server 2008 R2. Pentru mai multe detalii despre această actualizare, vizitați site-ul web de asistență tehnică Microsoft.

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.

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.

Platforme virtuale acceptate:

- VMWare Workstation 16 Pro
- VMware ESXi 7.0 Update 1a
- Microsoft Hyper-V Server 2019
- Citrix Virtual Apps and Desktops 7
- Citrix Provisioning 2009
- Citrix Hypervisor 8.2 LTSR

Kaspersky Endpoint Security acceptă funcționarea cu următoarele versiuni ale Kaspersky Security Center:

- Kaspersky Security Center 11
- Kaspersky Security Center 12
- Kaspersky Security Center 12 Patch A
- Kaspersky Security Center 12 Patch B

- Kaspersky Security Center 13
- Kaspersky Security Center 13,1
- Kaspersky Security Center 13,2

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).

Comparație a caracteristicilor aplicației Kaspersky Endpoint Security

Caracteristică	Stație de lucru	Server
Advanced Threat Protection		
Kaspersky Security Network	✓	✓
Behavior Detection	✓	✓
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		
Application Control	✓	✓
Control dispozitive	✓	–
Control Web	✓	–
Control anomalie adaptivă	✓	–
Data Encryption		
Kaspersky Disk Encryption	✓	–
BitLocker Drive Encryption	✓	✓
File Level Encryption	✓	–
Criptare unități amovibile	✓	–

Endpoint Agent	✓	✓
Managed Detection and Response	✓	✓

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 12:

- 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 prin Kaspersky Security Center Cloud Console, *consultați Ghidul de ajutor pentru Kaspersky Security Center Cloud Console*.

Comparație a caracteristicilor aplicației Kaspersky Endpoint Security

Caracteristică	Kaspersky Security Center 12		Kaspersky Security Center
	Consola de administrare	Web Console	Cloud Console
Advanced Threat Protection			
Kaspersky Security Network	✓	✓	✓
Kaspersky Private Security Network	✓	✓	–
Behavior Detection	✓	✓	✓
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	✓	✓	✓
Managed Detection and Response	✓	✓	✓
Protecție AMSI	✓	✓	✓

Security Controls			
Application Control	✓	✓	✓
Control dispozitive	✓	✓	✓
Control Web	✓	✓	✓
Control anomalie adaptivă	✓	✓	✓
Data Encryption			
Kaspersky Disk Encryption	✓	✓	–
BitLocker Drive Encryption	✓	✓	✓
File Level Encryption	✓	✓	–
Criptare unități amovibile	✓	✓	–
Endpoint Agent	✓	✓	✓
Activități			
Adăugare cheie	✓	✓	✓
Modificarea componentelor aplicației	✓	✓	✓
Inventar	✓	✓	✓
Actualizare	✓	✓	✓
Derulare înapoi actualizare	✓	✓	✓
Scanare de viruși	✓	✓	✓
Verificare integritate	✓	✓	–
Ștergere date	✓	✓	✓
Gestionarea conturilor Agentului de Autentificare	✓	✓	–

Compatibilitatea cu alte aplicații

Înainte de instalare, Kaspersky Endpoint Security verifică prezența pe computer a aplicațiilor Kaspersky. Aplicația verifică și computerul pentru software incompatibil. Lista programelor software incompatibile este disponibilă în fișierul incompatible.txt, care este inclus în kitul de distribuție.

DESCARCAȚI FIȘIERUL INCOMPATIBLE.TXT

Aplicația Kaspersky Endpoint Security este incompatibilă cu următoarele aplicații Kaspersky:

- Kaspersky Small Office Security.
- Kaspersky Internet Security.
- Kaspersky Anti-Virus.
- Kaspersky Total Security.
- Kaspersky Safe Kids.

- Kaspersky Free.
- Kaspersky Anti-Ransomware Tool.
- Kaspersky Anti Targeted Attack Platform (inclusiv componenta Senzor Endpoint).
- Kaspersky Sandbox (inclusiv Kaspersky Endpoint Agent).
- Kaspersky Endpoint Detection and Response (inclusiv componenta Senzor Endpoint).

  În cazul în care componenta Agent Endpoint a fost instalată pe un computer folosind instrumentele de implementare ale aplicațiilor Kaspersky, componenta va fi eliminată automat în timpul instalării Kaspersky Endpoint Security. Kaspersky Endpoint Security poate include, de asemenea, componenta Senzor Endpoint/Kaspersky Endpoint Agent dacă ați selectat Agentul Endpoint în lista componentelor aplicației.

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

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.
- la distanță, prin Kaspersky Security Center 12
- la distanță, prin intermediul editorului de gestionare a politicilor de grup pentru Microsoft Windows (pentru mai multe detalii, consultați *Site web de asistență tehnică 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.

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

Implementarea prin Kaspersky Security Center 12

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. Kaspersky Security Center 12 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 12 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 12*.

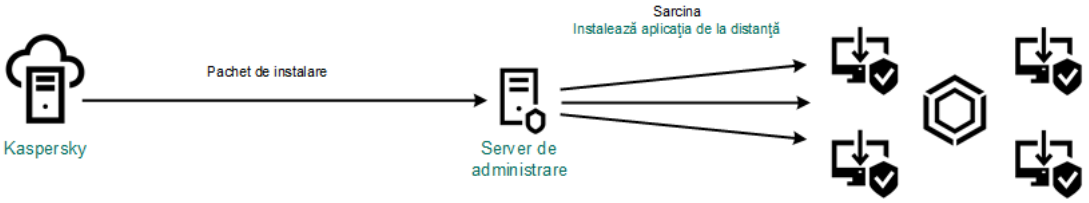
Instalarea standard a aplicației

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 distribuire a aplicației. Pachetul de instalare pentru Kaspersky Endpoint Security este comun pentru toate versiunile de Windows și tipurile de arhitecturi acceptate.

2. Crearea activității *Instalare aplicație la distanță* 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. În Consola de administrare, accesați directorul **Server de administrare → Suplimentar → Instalare la distanță**.

2. Faceți clic pe link-ul **Implementare pachet de instalare pe dispozitivele gestionate (stații de lucru)**.

Astfel va porni Expertul de implementare a securității. 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 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 3. Definirea setărilor activității de instalare la distanță

Configurați următoarele setări suplimentare ale aplicației:

- **Forțare descărcare pachet de instalare**. Selectați metoda de instalare a aplicației:
  - **Utilizare Agent rețea**. Dacă Agentul de rețea nu a fost instalat pe computer, primul Agent de rețea va fi instalat utilizându-se instrumentele din sistemul de operare. După aceea, Kaspersky Endpoint Security este instalat de instrumentele din Agentul de rețea.
  - **Utilizarea resurse sistem de operare prin puncte de distribuire**. 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 distribuire, *consultați Ajutor pentru Kaspersky Security Center*.

- **Utilizarea resurse sistem de operare prin Serverul de administrare**. 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.

- **Comportamentul dispozitivelor gestionate de alte servere**. 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.

- **Nu se instalează aplicația dacă este deja instalată**. Debifați această casetă de selectare dacă, de exemplu, dorești să instalezi o versiune anterioară a aplicației.

- **Atribuire instalare Agent de rețea în politicile de grup Active Directory**. 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 4. 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 *Adăugare cheie*.

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. 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 7. 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 8. Pornirea instalării

Ieșiți din Expert. Dacă este necesar, bifați caseta de selectare **Nu executa sarcina după ce Expertul de instalare la distanță finalizează**. 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 **Descoperire dispozitiv și implementare** → **Implementare și atribuire** → **Expert de implementare a securității**.

Astfel va porni Expertul de implementare a securității. 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 *Adăugare cheie*.

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:

- **Forțare descărcare pachet de instalare**. Selectarea metodei de instalare a aplicației:
  - **Utilizare Agent rețea**. Dacă Agentul de rețea nu a fost instalat pe computer, primul Agent de rețea va fi instalat utilizându-se instrumentele din sistemul de operare. După aceea, Kaspersky Endpoint Security este instalat de instrumentele din Agentul de rețea.
  - **Utilizarea resurse sistem de operare prin puncte de distribuire**. 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 distribuire, *consultați Ajutor pentru Kaspersky Security Center*.
  - **Utilizarea resurse sistem de operare prin Serverul de administrare**. 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.
- **Nu se instalează aplicația dacă este deja instalată**. Debifați această casetă de selectare dacă, de exemplu, dorești să instalezi o versiune anterioară a aplicației.
- **Atribuire instalare pachet în politicile de grup Active Directory**. 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 **Dispozitive neatribuite**.

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 **Executare activitate după terminarea Expertului**. 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 distribuire a 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 **Server de administrare** → **Suplimentar** → **Instalare la distanță** → **Pachete de instalare**.

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

2. Faceți clic pe butonul **Creare pachet de instalare**.

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

Pasul 1. Selectarea tipului pachetului de instalare

Selectați opțiunea **Creare pachet de instalare pentru aplicația Kaspersky**.

Pasul 2. Definirea numelui pachetului de instalare

Introduceți numele pachetului de instalare, de exemplu, `Kaspersky Endpoint Security for Windows 11.6.0`.

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, actualizați bazele de date antivirus din pachetul de instalare utilizând caseta de selectare **Copiere actualizări din depozit în pachetul de instalare**.

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, puteți selecta, de asemenea, componentele aplicației și puteți configura setările de instalare a aplicației (consultați tabelul de mai jos). 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 Consolei Web, selectați **Descoperire dispozitive și implementare** → **Implementare și atribuire** → **Pachete de instalare**.

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

2. Faceți clic pe butonul **Adăugare**.

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

Pasul 1. Selectarea tipului pachetului de instalare

Selectați opțiunea **Creare pachet de instalare pentru aplicația Kaspersky**.

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.

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.

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, puteți selecta, de asemenea, componentele aplicației și puteți configura setările de instalare a aplicației (consultați tabelul de mai jos). 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.

Setări pentru pachetului de instalare

Secțiune	Descriere
Componente protecție	În această secțiune poți selecta componentele aplicației care vor fi disponibile. Poți să modifici ulterior setul de componente ale aplicației folosind activitatea *Modificare componente aplicație*. Componenta BadUSB Attack Prevention, componenta Endpoint Agent și componentele de criptare a datelor nu se instalează în mod implicit. Aceste componente se pot adăuga în setările pachetului de instalare.
Setări instalare	**Adăugare locație aplicație la variabila de mediu %PATH%**. Puteți adăuga calea de instalare la variabila %PATH% pentru utilizare comodă a interfeței liniei de comandă. **Nu se protejează procesul de instalare**. 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. Dacă însă 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. **Asigurare compatibilitate cu Citrix PVS**. Poți activa suportul de la serviciile de asigurare a accesului Citrix pentru a instala aplicația Kaspersky Endpoint Security pe o mașină virtuală.

	Calea către directorul de instalare a aplicației. Poți schimba calea de instalare a aplicației Kaspersky Endpoint Security pe un computer client. În mod implicit, aplicația este instalată în directorul `%ProgramFiles%\Kaspersky Lab\Kaspersky Endpoint Security for Windows`. **Fișier de configurare**. Poți încărca 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, utilizați activitatea *Descărcare actualizări în depozitul Serverului de administrare* a Serverului de administrare. Pentru mai multe informații despre actualizarea bazelor de date antivirus din depozitul Serverului de administrarec, consultați *Ghidul de ajutor al Kaspersky Security Center*.

Puteți actualiza bazele de date din pachetul de instalare numai în Consola de administrare și Kaspersky Security Center 12 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. În Consola de administrare, accesați directorul **Server de administrare** → **Suplimentar** → **Instalare la distanță** → **Pachete de instalare**.

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

2. Deschideți proprietățile pachetului de instalare.

3. În secțiunea **General**, faceți clic pe butonul **Actualizare baze de date**.

   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 Consolei Web, selectați **Descoperire dispozitive și implementare** → **Implementare și atribuire** → **Pachete de instalare**.

   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 **Informații generale**, faceți clic pe linkul **Actualizare baze de date**.

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 *Instalare aplicație la distanță* este concepută pentru instalarea la distanță a Kaspersky Endpoint Security. Activitatea *Instalare aplicație la distanță* 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. În Consola de administrare, accesați directorul **Server de administrare** → **Activități**.

   Lista activităților se deschide.

2. Faceți clic pe butonul **Activitate nouă**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Selectarea tipului activității

Selectați **Server de administrare Kaspersky Security Center** → **Instalare aplicație la distanță**.

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:

- **Forțare descărcare pachet de instalare**. Selectați metoda de instalare a aplicației:
  - **Utilizare Agent rețea**. Dacă Agentul de rețea nu a fost instalat pe computer, primul Agent de rețea va fi instalat utilizându-se instrumentele din sistemul de operare. După aceea, Kaspersky Endpoint Security este instalat de instrumentele din Agentul de rețea.
  - **Utilizarea resurse sistem de operare prin puncte de distribuire**. 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 distribuire, *consultați Ajutor pentru Kaspersky Security Center*.
  - **Utilizarea resurse sistem de operare prin Serverul de administrare**. 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.
- **Comportamentul dispozitivelor gestionate de alte servere**. 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.

- **Nu se instalează aplicația dacă este deja instalată**. 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 11.6.0`.

Pasul 10. Finalizarea creării activității

Ieșiți din Expert. Dacă este necesar, bifați caseta de selectare **Executare activitate după terminarea Expertului**. 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 Consolei Web, selectează **Devices** → **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe butonul **Adăugare**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Configurarea setările generale ale activității

Configurați setările generale pentru activitate:

1. În lista verticală **Aplicație**, selectați **Kaspersky Security Center**.
2. În lista verticală **Tip activitate**, selectează **Instalare aplicație la distanță**.
3. În câmpul **Nume activitate**, introdu o descriere succint, de exemplu `Instalare Kaspersky Endpoint Security pentru manageri`.
4. În secțiunea **Dispozitive la care se va atribui activitatea**, selectează 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, configurează setările pentru pachetul de instalare**:**

1. Selectați pachetul de instalare Kaspersky Endpoint Security for Windows (11.6.0).
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 secțiunea **Forțare descărcare pachet de instalare**, selectează metoda de instalare a aplicației:

   - **Utilizare Agent rețea**. Dacă Agentul de rețea nu a fost instalat pe computer, primul Agent de rețea va fi instalat utilizându-se instrumentele din sistemul de operare. După aceea, Kaspersky Endpoint Security este instalat de instrumentele din Agentul de rețea.
   - **Utilizarea resurse sistem de operare prin puncte de distribuire**. 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 distribuire, *consultați Ajutor pentru Kaspersky Security Center*.
   - **Utilizarea resurse sistem de operare prin Serverul de administrare**. 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 **Număr maxim de descărcări simultane**, setează o limită pentru numărul de solicitări de descărcare a pachetului de instalare trimise către Serverul de administrare. O limită pentru numărul de solicitări va ajuta la prevenirea supraîncărcării rețelei.

5. În câmpul **Număr de încercări de instalare**, 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, debifează caseta de selectare **Nu se instalează aplicația dacă este deja instalată**. Acest lucru permite, de exemplu, instalarea uneia dintre versiunile anterioare ale aplicației.

7. Dacă este necesar, debifați caseta de selectare **Se verifică versiunea sistemului de operare înainte de instalare**. 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, bifează caseta de selectare **Atribuire instalare pachet în politicile de grup Active Directory**. 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, bifează caseta de selectare **Se oferă utilizatorilor posibilitatea să închidă aplicațiile care se execută**. 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 secțiunea **Comportare dispozitive gestionate de acest Server**, 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 **Pornire**. 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.

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:

- Prezența programelor software incompatibile instalate (lista programelor software incompatibile este disponibilă în fișierul incompatible.txt, care este inclus în kitul de distribuție).
- Sunt sau nu îndeplinite cerințele hardware și software.
- 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.

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 11.6.0 for Windows, iar versiunea anterioară a aplicației este eliminată automat. Acest lucru este aplicabil pentru următoarele versiuni ale aplicației:

- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 4 for Windows (versiunea 10.2.6.3733).
- Kaspersky Endpoint Security 10 Service Pack 2 for Windows (versiunea 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 1 for Windows (versiunea 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 2 for Windows (versiunea 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 3 for Windows (versiunea 10.3.3.275).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 for Windows (versiunea 10.3.3.304).
- Kaspersky Endpoint Security 11.0.0 for Windows (versiunea 11.0.0.6499).
- Kaspersky Endpoint Security 11.0.1 for Windows (versiunea 11.0.1.90).
- Kaspersky Endpoint Security 11.0.1 for Windows SF1 (versiunea 11.0.1.90).
- Kaspersky Endpoint Security 11.1.0 for Windows (versiunea 11.1.0.15919).

- Kaspersky Endpoint Security 11.1.1 for Windows (versiunea 11.1.1.126).
- Kaspersky Endpoint Security 11.2.0 for Windows (versiunea 11.2.0.2254).
- Kaspersky Endpoint Security 11.2.0 for Windows CF1 (versiunea 11.2.0.2254).
- Kaspersky Endpoint Security 11.3.0 for Windows (versiunea 11.3.0.773).
- Kaspersky Endpoint Security 11.4.0 for Windows (versiunea 11.4.0.233).
- Kaspersky Endpoint Security 11.5.0 for Windows (versiunea 11.5.0.590).

Componentele Kaspersky Endpoint Security

În timpul procesului de instalare puteți selecta componentele Kaspersky Endpoint Security pe care doriți să le instalați. Componenta File Threat Protection trebuie să fie instalată în mod obligatoriu. Nu poți anula instalarea ei.

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

- BadUSB Attack Prevention.
- File Level Encryption.
- Full Disk Encryption.
- Gestionare Bitlocker.
- Agent Endpoint. *Endpoint Agent* instalează Kaspersky Endpoint Agent 3.10 pentru interacțiunea dintre aplicație și soluțiile Kaspersky concepute pentru a detecta amenințări avansate (de exemplu, Kaspersky Sandbox).

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

Protejare proces de instalare aplicație. 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. Dacă însă 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 serviciile de asigurare acces Citrix. Poți activa suportul de la serviciile de asigurare a accesului Citrix pentru a instala aplicația Kaspersky Endpoint Security pe o mașină virtuală.

Adăugare locație aplicație la variabila de mediu %PATH%. Puteți adăuga calea de instalare la variabila %PATH% pentru utilizare comodă a interfeței liniei de comandă.

Instalarea aplicației din linia de comandă

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. 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.

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. Deschideți directorul în care se află pachetul de distribuție Kaspersky Endpoint Security.
3. Executați următoare comandă:

   ```
   setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 [/pKSN=1|0] [/pALLOWREBOOT=1]
   [/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<nume utilizator>
   /pKLPASSWD=<parolă> /pKLPASSWDAREA=<domeniu parolă>] [/pENABLETRACES=1|0 /pTRACESLEVEL=
   <nivel urmărire>] [/s]
   ```

   sau

   ```
   msiexec /i <nume kit distribuție> EULA=1 PRIVACYPOLICY=1 [KSN=1|0]
   [ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1] [KLLOGIN=<nume utilizator> KLPASSWD=<parolă>
   KLPASSWDAREA=<domeniu parolă>] [ENABLETRACES=1|0 TRACESLEVEL=<nivel urmărire>] [/qn]
   ```

`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. 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.
`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`	Dezactivarea verificării existenței programelor software incompatibile. Lista programelor software incompatibile 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, instalarea aplicației Kaspersky Endpoint Security va fi oprită.
`SKIPPRODUCTUNINSTALL=1`	Dezactivarea eliminării automate a programelor software incompatibile detectate. Dacă nu este setată nicio valoare pentru acest parametru, Kaspersky Endpoint Security încearcă să elimine software-ul incompatibil. Eliminarea automată a software-ului incompatibil nu poate fi activată când se instalează Kaspersky Endpoint Security folosind programul de instalare msiexec. Folosiți setup_kes.exe pentru a activa eliminarea automată a software-ului incompatibil.
`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.
`ENABLETRACES`	Activarea sau dezactivarea urmăririi aplicațiilor. După ce Kaspersky Endpoint Security pornește, acesta salvează fișierele de urmărire în directorul %ProgramData%\Kaspersky Lab\KES\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.
`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.
`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 `<DOMENIU>\<NumeUtilizator>` (de exemplu, `RESTAPI_User=COMPANIE\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.
`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.

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 Expertul de activare a aplicației sau a 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
- install.cfg – setări legate de funcționarea Kaspersky Endpoint Security
- setup.reg – chei de registru

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.ini și setup.reg, plasați aceste fișiere 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=<cale către fișierul setup.reg>`.

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 secțiunea **Gestionare aplicații**, selectați **Pachete**.
3. În partea de sus a consolei, în panoul de control, faceți clic pe butonul **Creare pachet**.
   Este lansat *Expert pachet nou și aplicație*.
4. În Expert pachet nou și aplicație:
   a. În secțiunea **Pachet**:
      - În câmpul **Nume**, introdu numele pachetului de instalare.
      - În câmpul **Director sursă**, specifică o cale către directorul care conține kitul de distribuție pentru Kaspersky Endpoint Security.
   b. În secțiunea **Tip aplicație**, selectați opțiunea **Aplicație standard**.
   c. În secțiunea **Aplicație standard**:
      - În câmpul **Nume**, introdu numele unic pentru pachetul de instalare (de exemplu, numele aplicației, inclusiv versiunea).
      - În câmpul **Linie de comandă**, specifică opțiunile de instalare din linia de comandă pentru Kaspersky Endpoint Security.
      - Faceți clic pe butonul **Răsfoire** pentru a introduce o cale către fișierul executabil al aplicației.
      - Asigură-te că lista **Mod de executare** are selectat elementul **Executare cu drepturi de administrator**.
   d. În secțiunea **Cerințe**:
      - Bifați caseta de selectare **Pornește altă aplicație mai întâi** dacă dorești ca o altă aplicație să fie lansată înainte de a instala Kaspersky Endpoint Security.

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

- Selectați opțiunea **Această aplicație poate fi pornită numai pe platformele specificate** în secțiunea **Cerințe platformă**, dacă dorești 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 **Sumar**, verifică toate valorile introduse pentru setări și faceți clic pe **Următorul**.

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

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

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

   b. În secțiunea **Conține**, 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 **Sumar**, verifică toate valorile introduse pentru setări și faceți clic pe **Următorul**.

   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 Server. Pentru a aplica setări din fișierul setup.ini, plasează acest fișier în directorul care conține pachetul de distribuție Kaspersky Endpoint Security.

DESCARCAȚI FIȘUL SETUP.INI

Fișierul setup.ini constă din următoarele secțiuni:

- `[Setup]` – setări generale ale instalării aplicației.
- `[Components]` – selecția componentelor de aplicație de instalat. 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.

Componenta Managed Detection and Response lipsește, de asemenea, din această secțiune. Pentru a instala această componentă, trebuie să activați componenta Managed Detection and Response în Kaspersky Security Center Console.

- `[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.

Valorile alternative pentru valoarea `1` sunt `yes`, `on`, `enable` și `enabled`.

Valorile alternative pentru valoarea `0` sunt `no`, `off`, `disable` și `disabled`.

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=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. 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.

	`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 `Nume de conectare`, 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 `Conectare` și `Parolă`). 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.
	`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. Dacă însă 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.
	`Reboot=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.
	`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.
	`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 Kaspersky Endpoint Security pornește, acesta salvează fișierele de urmărire în directorul

		%ProgramData%\Kaspersky Lab\KES\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.
	`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 `<DOMENIU>\<NumeUtilizator>` (de exemplu, `RESTAPI_User=COMPANIE\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.
`[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.
	`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.
	`ApplicationControl`	Application Control.
	`AdaptiveAnomaliesControl`	Control adaptiv al anomaliilor.
	`FileEncryption`	Biblioteci File Level Encryption.
	`DiskEncryption`	Biblioteci Full Disk Encryption.
	`BadUSBAttackPrevention`	BadUSB Attack Prevention.
	`AntiAPT`	Endpoint Agent. *Endpoint Agent* instalează Kaspersky Endpoint Agent 3.10 pentru interacțiunea dintre aplicație și soluțiile Kaspersky concepute pentru a detecta amenințări avansate (de exemplu, Kaspersky Sandbox).
	`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.
`[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.

- La distanță prin Kaspersky Security Center.

  Activitatea *Modificare componente aplicație* 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.

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

1. În Consola de administrare, accesați directorul **Server de administrare** → **Activități**.

   Lista activităților se deschide.

2. Faceți clic pe butonul **Activitate nouă**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Selectarea tipului activității

Selectați **Kaspersky Endpoint Security for Windows (11.6.0)** → **Modificare componente ale aplicației**.

Pasul 2. Setările activităților pentru modificarea componentelor aplicației

Selectați componentele aplicației care vor fi disponibile pe computerul utilizatorului.

Bifați caseta de selectare **Eliminare aplicații de la terți incompatibile**. Lista aplicațiilor incompatibile poate fi vizualizată în `incompatible.txt`, care este inclus în kitul de distribuție. Dacă pe computer sunt instalate aplicații incompatibile, instalarea aplicației Kaspersky Endpoint Security se termină cu o eroare.

Dacă este necesar, activează protecția prin parolă pentru funcționarea activității:

1. Faceți clic pe butonul **Suplimentar**.
2. Bifați caseta de selectare **Utilizare parolă pentru modificarea setului componentelor aplicației**.
3. Introduceți acreditările contului de utilizator KLAdmin.

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, de exemplu, `Adăugare componenta Application Control`.

Pasul 6. Finalizarea creării activității

Ieșiți din Expert. Dacă este necesar, bifați caseta de selectare **Executare activitate după terminarea Expertului**. Puteți monitoriza progresul activității în proprietățile activității.

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.

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

1. În fereastra principală a Consolei Web, selectează **Devices** → **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe butonul **Adăugare**.

   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**, selectați **Kaspersky Endpoint Security for Windows (11.6.0)**.
2. În lista verticală **Tip activitate**, selectați **Modificare componente aplicație**.
3. În câmpul **Nume activitate**, introdu o descriere succintă, de exemplu `Adăugare componentă Application Control`.
4. În secțiunea **Select 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

Bifați caseta de selectare **Deschide proprietățile activității după crearea acesteia** și finalizați Expertul. În proprietățile activității, selectați fila **Setări aplicație** și selectați componentele aplicației care vor fi disponibile.

Dacă este necesar, activează protecția prin parolă pentru funcționarea activității:

1. În secțiunea **Setări avansate**, bifați caseta de selectare **Utilizare parolă pentru modificarea setului de componente ale aplicației**.
2. Introduceți acreditările contului de utilizator KLAdmin.

Salvați modificările și executați activitatea.

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.

Actualizarea de la o versiune anterioară a aplicației

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

- Kaspersky Endpoint Security 11.6.0 este compatibil cu Kaspersky Security Center 12.
- Vă recomandăm să închideți toate aplicațiile active înainte de a începe actualizarea.
- În cazul în care computerul are unități de hard disk care sunt criptate folosind Full Disk Encryption (FDE), atunci trebuie să decriptați toate unitățile de hard disk criptate pentru a face upgrade pentru Kaspersky Endpoint Security de la versiunea 10 la versiunea 11.0.0 sau o versiune ulterioară.

  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 10 Service Pack 1 Maintenance Release 4 for Windows (versiunea 10.2.6.3733).
- Kaspersky Endpoint Security 10 Service Pack 2 for Windows (versiunea 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 1 for Windows (versiunea 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 2 for Windows (versiunea 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 3 for Windows (versiunea 10.3.3.275).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 for Windows (versiunea 10.3.3.304).
- Kaspersky Endpoint Security 11.0.0 for Windows (versiunea 11.0.0.6499).
- Kaspersky Endpoint Security 11.0.1 for Windows (versiunea 11.0.1.90).
- Kaspersky Endpoint Security 11.0.1 for Windows SF1 (versiunea 11.0.1.90).
- Kaspersky Endpoint Security 11.1.0 for Windows (versiunea 11.1.0.15919).
- Kaspersky Endpoint Security 11.1.1 for Windows (versiunea 11.1.1.126).
- Kaspersky Endpoint Security 11.2.0 for Windows (versiunea 11.2.0.2254).
- Kaspersky Endpoint Security 11.2.0 for Windows CF1 (versiunea 11.2.0.2254).
- Kaspersky Endpoint Security 11.3.0 for Windows (versiunea 11.3.0.773).
- Kaspersky Endpoint Security 11.4.0 for Windows (versiunea 11.4.0.233).
- Kaspersky Endpoint Security 11.5.0 for Windows (versiunea 11.5.0.590).

Atunci când faceți upgrade de la Kaspersky Endpoint Security 10 Service Pack 2 for Windows la Kaspersky Endpoint Security 11.6.0 for Windows, fișierele care au fost plasate în Copie de rezervă sau în Carantină în versiunea precedentă a aplicației vor fi transferate în Copie de rezervă în noua versiune a aplicației. Pentru versiunile anterioare ale produsului Kaspersky Endpoint Security 10 Service Pack 2 for Windows, fișierele plasate în Copie de rezervă și Carantină într-o versiune anterioară a aplicației nu migrează în versiunea mai nouă.

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

- local, folosind Expertul de configurare.
- local, din linia de comandă.
- la distanță, prin Kaspersky Security Center 12.
- la distanță, prin intermediul editorului de gestionare a politicilor de grup pentru Microsoft Windows (pentru mai multe detalii, consultați *Site web de asistență tehnică 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.

Eliminare aplicație

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

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

- local, folosind Expertul de configurare;
- local, din linia de comandă;
- la distanță, folosind Kaspersky Security Center (pentru mai multe informații, consultați *Ajutor pentru Kaspersky Security Center*);
- la distanță, prin intermediul editorului de gestionare a politicilor de grup pentru Microsoft Windows (pentru mai multe detalii, consultați *Site web de asistență tehnică Microsoft*).

Dacă ați selectat componenta Agent Endpoint în timpul instalării aplicației, următoarele două aplicații vor fi instalate pe computer: Kaspersky Endpoint Security și Kaspersky Endpoint Agent. După dezinstalarea Kaspersky Endpoint Security, Kaspersky Endpoint Agent va fi, de asemenea, dezinstalat automat.

Dezinstalarea prin Kaspersky Security Center

Puteți dezinstala aplicația de la distanță folosind activitatea *Dezinstalare aplicație de la distanță*. 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. În Consola de administrare, accesați directorul **Server de administrare** → **Activități**.

   Lista activităților se deschide.

2. Faceți clic pe butonul **Activitate nouă**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Selectarea tipului activității

Selectați **Server de administrare Kaspersky Security Center** → **Suplimentar** → **Dezinstalare aplicație la distanță**.

Pasul 2. Selectarea aplicației care trebuie eliminată

Selectați **Dezinstalare aplicație acceptată de Kaspersky Security Center** .

Pasul 3. Setările activității pentru dezinstalarea aplicației

Selectați **Kaspersky Endpoint Security for Windows (11.6.0)**.

Pasul 4. Dezinstalarea setărilor utilitare

Configurați următoarele setări suplimentare ale aplicației:

- **Forțați descărcarea utilitarului de dezinstalare**. Selectați metoda de livrare a utilitarului:
  - **Utilizare Agent rețea**. 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.
  - **Utilizarea resurselor Microsoft Windows prin intermediul Serverului de administrare**. 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.
  - **Utilizarea resurse sistem de operare prin puncte de distribuire**. 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 distribuire, *consultați Ajutor pentru Kaspersky Security Center*.
- **Verificați versiunea sistemului de operare înainte de descărcare**. 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 **Utilizare parolă dezinstalare**.
2. Faceți clic pe butonul **Editare**.

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 11.6.0`.

Pasul 10. Finalizarea creării activității

Ieșiți din Expert. Dacă este necesar, bifați caseta de selectare **Executare activitate după terminarea Expertului**. 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 Consolei Web, selectează **Devices** → **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe butonul **Adăugare**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Configurarea setările generale ale activității

Configurați setările generale pentru activitate:

1. În lista verticală **Aplicație**, selectați **Kaspersky Security Center**.
2. În lista verticală **Tip activitate**, selectați **Dezinstalare aplicație la distanță**.
3. În câmpul **Nume activitate**, introduceți o descriere succintă, de exemplu `Dezinstalare Kaspersky Endpoint Security de pe computerele Serviciului de asistență tehnică`.
4. În secțiunea **Select 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 **Eliminare aplicație gestionată**.
2. Selectați **Kaspersky Endpoint Security for Windows (11.6.0)**.
3. **Forțați descărcarea utilitarului de dezinstalare**. Selectați metoda de livrare a utilitarului:

   - **Utilizare Agent rețea**. 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.
   - **Utilizarea resurselor Microsoft Windows prin intermediul Serverului de administrare**. 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.
   - **Utilizarea resurse sistem de operare prin puncte de distribuire**. 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 distribuire, *consultați Ajutor pentru Kaspersky Security Center*.

4. În câmpul **Număr maxim de descărcări simultane**, setați o limită pentru numărul de solicitări trimise către Serverul de administrare pentru a descărca utilitarul de dezinstalare a aplicației. O limită pentru numărul de

solicitări va ajuta la prevenirea supraîncărcării rețelei.

5. În câmpul **Număr de încercări de dezinstalare**, setează 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 **Se verifică versiunea sistemului de operare înainte de instalare**. 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 **Pornire**. 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, introduceți parola contului KLAdmin în proprietățile activității *Dezinstalare aplicație de la distanță* . Fără parolă, activitatea nu va fi executată.

Pentru a utiliza parola contului KLAdmin în activitatea Dezinstalare aplicație de la distanță:

1. În fereastra principală a Consolei Web, selectează **Devices** → **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe activitatea Kaspersky Security Center **Dezinstalare aplicație de la distanță** .

   Se va deschide fereastra de proprietăți a activității.

3. Selectați fila **Setări aplicație**.

4. Bifați caseta de selectare **Utilizare parolă dezinstalare**.

5. Introduceți parola contului KLAdmin.

6. Faceți clic pe butonul **Save**.

Dezinstalarea aplicației folosind Expertul

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.

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.

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.
- **Stocare locală a 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.

Eliminarea aplicației din linia de comandă

Aplicația KaspEndpoint 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 dvs. în procesul de eliminare. 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. Deschideți directorul în care se află pachetul de distribuție Kaspersky Endpoint Security.
3. Executați următoare comandă:
   - Dacă procesul de eliminare nu este protejat cu parolă:

     ```
     setup_kes.exe /s /x
     ```

     sau

     ```
     msiexec.exe /x <GUID> /qn
     ```

<GUID> este identificatorul unic al aplicației. Puteți afla GUID-ul aplicației 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=<nume utilizator> /pKLPASSWD=<parolă> /s /x
  ```

  sau

  ```
  msiexec.exe /x <GUID> KLLOGIN=<nume utilizator> KLPASSWD=<parolă> /qn
  ```

Exemplu:

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin
KLPASSWD=!Password1 /qn
```

Licența aplicației

Această secțiune oferă informații despre conceptele generale legate de licențierea aplicației.

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 distribuire al aplicației și se găsește, de asemenea, în directorul de instalare a aplicației `%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Endpoint Security for Windows\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.

O licență validă îți dă dreptul la următoarele tipuri de servicii:

- Utilizarea aplicației în conformitate cu termenii Acordului de licență pentru utilizatorul final
- Asistență tehnică

Scopul serviciilor 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.

- *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.

Atunci când expiră licența comercială, caracteristicile principale ale aplicației sunt dezactivate. Pentru a continua utilizarea aplicației, trebuie să reînnoiești licența comercială. Dacă nu intenționezi să îți reînnoiești licența, trebuie să elimini 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:

- Cheia de licență 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.
- Tipul licenței.

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 se poate adăuga o cheie de licență 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.

Puteți 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 licență 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 primiți 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.

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

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, folosind Expertul de activare, puteți adăuga atât cheia activă, cât și o cheie de rezervă în acest mod.
- La distanță, cu suita software Kaspersky Security Center, creând și apoi pornind o activitate de adăugare a cheii de licență. În acest mod puteți adăuga atât cheia activă, cât și o cheie de rezervă.
- De la distanță, distribuind fișierele cheie și codurile de activare stocate în stocarea cheilor a Serverului de administrare Kaspersky Security Center către computerele client. Pentru mai multe detalii despre selectarea cheilor, *consultați Ghidul de ajutor pentru Kaspersky Security Center*. În acest mod puteți adăuga atât cheia activă, cât și o cheie de rezervă.

  > Codul de activare achiziționat în baza abonamentului este distribuit primul.

- 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.

Activarea aplicației prin Kaspersky Security Center

Puteți activa aplicația de la distanță prin Kaspersky Security Center în următoarele moduri:

- Utilizarea activității *Adăugare cheie*.

  Această metodă îți permite să adaugi o cheie unui anumit computer sau unor computere care fac parte dintr-un grup de administrare.

- 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 Serverul de administrare Kaspersky Security Center, consultați secțiunea *Ajutor pentru Kaspersky Security Center*.

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.

Poți monitoriza utilizarea licențelor în următoarele moduri:

- Vizualizează *Raport utilizare cheie* pentru infrastructura organizației (**Monitorizare și rapoarte** → **Rapoarte**).
- Vizualizează stările computerelor în fila **Dispozitive** → **Dispozitive gestionate**. Dacă aplicația nu este activată, computerul va avea starea ⚠ și descrierea stării **Aplicația nu este activată**.
- Vizualizează informațiile despre licență în proprietățile computerului.
- Vizualizează proprietățile cheii (**Operații** → **Licențiere**).

Cum să activați aplicația în Consola de administrare (MMC)

1. În Consola de administrare, accesați directorul **Server de administrare** → **Activități**.

   Lista activităților se deschide.

2. Faceți clic pe butonul **Activitate nouă**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Selectarea tipului activității

Selectați **Kaspersky Endpoint Security for Windows (11.6.0)** → **Adăugare 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 Ghid de 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 **Executare activitate după terminarea Expertului**. 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 Consolei Web, selectează **Devices** → **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe butonul **Adăugare**.

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**, selectați **Kaspersky Endpoint Security for Windows (11.6.0)**.
2. În lista verticală **Tip activitate**, selectați **Adăugare cheie**.
3. În câmpul **Nume activitate**, introdu o descriere succintă, de exemplu `Activare Kaspersky Endpoint Security for Windows`.
4. În secțiunea **Select devices to which the task will be assigned**, selectați domeniul activității. Faceți clic pe butonul **Next**.

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. Faceți clic pe butonul **Next**.

Puteți adăuga chei la Consola Web (**Operații** → **Licențiere**).

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 **Pornire**. Ca rezultat, aplicația Kaspersky Endpoint Security va fi activată pe computerele utilizatorilor în modul silențios.

În proprietățile activității *Adăugare cheie*, puteți adăuga o cheie de rezervă computerului. O *cheie de rezervă* devine activă atunci când cheia activă expiră sau este ștearsă. 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, accesați directorul **Server de administrare** → **Licențe Kaspersky**.

   Se deschide o listă de chei de licență.

2. Deschideți proprietățile cheii de licență.

3. În secțiunea **General**, bifați caseta de selectare **Cheie de licență distribuită automat**.

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 **Dispozitive**.

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 **Operații** → **Licențiere** → **Licențe Kaspersky**.

   Se deschide o listă de chei de licență.

2. Deschideți proprietățile cheii de licență.

3. În fila **General**, activați butonul de comutare **Instalare automată cheie**.

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 **Dispozitive**.

Utilizarea Expertului de activare pentru activarea aplicației

Pentru a activa Kaspersky Endpoint Security folosind Expertul de activare:

1. Faceți clic pe butonul **Licență** în partea de jos a ferestrei principale a aplicației.

2. În fereastra care se deschide, faceți clic pe butonul **Activați aplicația utilizând o licență nouă**.

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

Activarea aplicației din linia de comandă

Pentru a activa aplicația din linia de comandă,

tastează următorul șir în linia de comandă:

```
avp.com license /add <cod activare sau fișier cheie> [/login=<nume utilizator>
/password=<parolă>]
```

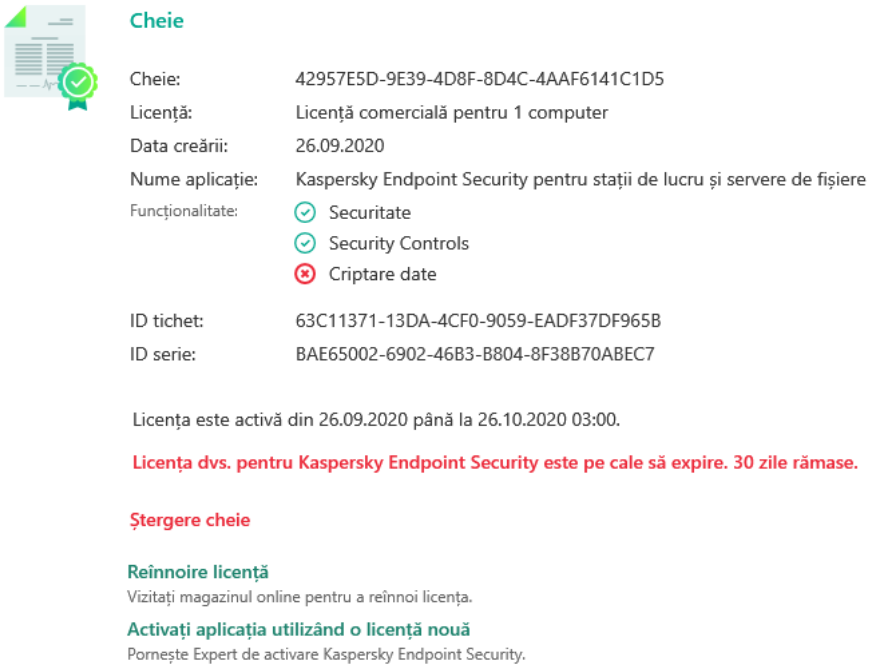
Trebuie să introduceți acreditările contului de utilizator (`/login=<nume utilizator> /password=<parolă>`) dacă funcția Protecție prin parolă este activată.

Vizualizarea informațiilor despre licență

Pentru a vizualiza informații despre o licență:

Faceți clic pe butonul **Licență** amplasat în partea de jos a ferestrei principale a aplicației.

Se va deschide fereastra **Licențiere**. Această fereastră afișează informații despre licență (vezi figura de mai jos).



Fereastra Licențiere

Următoarele informații sunt furnizate în fereastra **Licențiere**:

- **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 când expiră cheia activă sau după ce aceasta a fost ștearsă utilizând butonul .

- **Cheie**. O *cheie* este o secvență alfanumerică unică care este generată dintr-un cod de activare sau un fișier cheie.
- **Licențe**. Sunt disponibile următoarele tipuri de licențe: trial și comercială.
- **Nume aplicație**. Numele complet al aplicației Kaspersky achiziționată.
- **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**. Tipul de licență, numărul de computere care sunt acoperite de această licență, data de începere a licenței și data și ora expirării (numai pentru cheia activă).

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

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

- **Achiziționare licență/Reînnoire licență**. 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.
- **Activare aplicație cu 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, faceți clic pe butonul **Licență**.
2. În fereastra **Licențiere**, efectuează una dintre următoarele acțiuni:
   - Dacă nu au fost adăugate chei sau a fost adăugată o cheie pentru o licență pentru versiune trial, faceți clic pe butonul **Achiziționare licență**.
   - Dacă este adăugată cheia pentru o licență pentru versiune comercială, faceți clic pe butonul **Reînnoire licență**.

   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.

Îți poți reînnoi manual abonamentul în fereastra **Licențiere**. Acest lucru poate fi necesar dacă abonamentul a fost reînnoit după perioada de grație și aplicația nu a actualizat automat starea abonamentului.

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

1. În fereastra principală a aplicației, faceți clic pe butonul **Licență**.

2. În fereastra **Licențiere**, faceți clic pe **Contactează furnizorul abonamentului tău**.

Furnizarea de date 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-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 activă;
- cheia activă;
- termenii licenței Kaspersky Endpoint Security;
- starea curentă a licenței;
- tipul licenței active;
- 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 **Mod 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 **Mod KSN extins**, cât și caseta de selectare **Kaspersky Security Network**, în plus față de informațiile de mai sus, aplicația va 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 sistemul de operare (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.

Respectarea legislației Uniunii Europene (GDPR)

Kaspersky Endpoint Security poate transmite date către Kaspersky în următoarele scenarii:

- Despre 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
- Scrierea imaginilor

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 Private KSN sau dezactivați utilizarea KSN. Pentru mai multe detalii despre Private KSN, 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.

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 12 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 12 Web Console și Kaspersky Security Center Cloud Console

Kaspersky Security Center 12 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 12 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 12 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 12 Web Console. Spre deosebire de Plug-inul de gestionare pentru Consola de administrare Kaspersky Security Center, care este instalat pe stația de lucru a administratorului, plug-inul Web trebuie instalat pe un computer care are instalată Kaspersky Security Center 12 Web Console. 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 Consolă web: **Setări consolă** → **Plug-inuri**. Pentru mai multe detalii despre compatibilitatea versiunilor de plug-inuri Web și Consola Web, consultați *Ajutor pentru Kaspersky Security Center*.

Instalarea plug-inului Web

Poți instala plug-inul Web după cum urmează:

- Instalează plug-inul Web folosind Expertul de configurare inițială al Kaspersky Security Center 12 Web Console.

  Consola Web îți solicită automat să execuți Expertul de configurare inițială atunci când conectezi prima oară Consola Web la Serverul de administrare. Poți, de asemenea, să execuți Expertul de configurare inițială în interfața Consolei Web (**Descoperire dispozitive și implementare** → **Implementare și atribuire** → **Expert de configurare inițială**). Expertul de configurare inițială poate, de asemenea, să verifice dacă plug-inurile Web instalate sunt actualizate și să descarce actualizările necesare. Pentru mai multe detalii despre Expertul de configurare inițială pentru Kaspersky Security Center 12 Web Console, consultați *Ghidul de ajutor pentru Kaspersky Security Center*.

- Instalarea plug-inului Web folosind lista de pachete de distribuire disponibile din Consola Web.

  Pentru a instala plug-inul Web, selectați pachetul de distribuție al plug-inului Web Kaspersky Endpoint Security în interfața Consolei Web: **Setări Consolă** → **Plug-inuri**. 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 Consolei web: **Setări consolă** → **Plug-inuri**. Pachetul de distribuție al plug-inului Web poate fi descărcat, de exemplu, de pe site-ul Web Kaspersky.

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 *Sunt disponibile actualizări pentru plug-inurile utilizate*. 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 Consolei Web (**Setări consolă** → **Plug-inuri**). 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 Consolei Web (**Setări Consolă** → **Plug-inuri**). 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 selectați arhiva ZIP a pachetului de distribuție pentru plug-inul web Kaspersky Endpoint Security în interfața Consolei web: **Setări consolă** → **Plug-inuri**. 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.

Upgrade-ul Plug-inului de gestionare pentru Kaspersky Endpoint Security 10 for Windows

Dacă Plug-inul de gestionare pentru Kaspersky Endpoint Security 10 for Windows este instalat în Consola de administrare, ai în vedere următoarele atunci când instalezi Plug-inul de gestionare pentru Kaspersky Endpoint Security 11 for Windows:

- Plug-inul de gestionare pentru Kaspersky Endpoint Security 10 for Windows nu va fi eliminat și va fi disponibil pentru operare. Prin urmare, veți avea acces la două Plug-inuri de administrare pentru a lucra cu versiunile de

aplicații 10 și 11.

- Plug-inul de gestionare pentru Kaspersky Endpoint Security 11 for Windows nu acceptă gestionarea Plug-inului de gestionare pentru Kaspersky Endpoint Security 10 for Windows pe computerele utilizatorilor.
- Plug-inul de gestionare pentru Kaspersky Endpoint Security 11 for Windows nu acceptă elemente (de exemplu, politici sau activități) care au fost create utilizând Plug-inul de gestionare pentru Kaspersky Endpoint Security 10 for Windows.

  Puteți utiliza Expertul de conversie a loturilor de politici și sarcini pentru a converti politicile și acțiunile de la versiunea 10 la versiunea 11. Pentru mai multe detalii despre convertirea politicilor și activităților, consultați *Ghidul de ajutor pentru Kaspersky Security Center*.

Upgrade-ul Plug-inului de gestionare pentru Kaspersky Endpoint Security 11 for Windows

Dacă Plug-inul de gestionare pentru Kaspersky Endpoint Security 11 for Windows este instalat în Consola de administrare, ai în vedere următoarele atunci când instalezi o versiune nouă a Plug-inului de gestionare pentru Kaspersky Endpoint Security 11 for Windows:

- Versiunea anterioară a Plug-inului de gestionare pentru Kaspersky Endpoint Security 11 for Windows va fi eliminată.
- Versiunea nouă a Plug-inului de gestionare pentru Kaspersky Endpoint Security 11 for Windows acceptă gestionarea versiunii anterioare de Kaspersky Endpoint Security 11 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.
- Când actualizați Plug-inul de administrare la versiunea 11.2.0, trebuie să deschideți o politică pentru a-l converti automat. Atunci când faceți acest lucru, Kaspersky Endpoint Security vă va solicita confirmarea de a participa la KSN. Dacă ați făcut deja upgrade aplicației la versiunea 11.20 pe computerele organizației dvs., participarea la KSN va fi dezactivată până când acceptați condițiile de participare la KSN.

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 lucra cu serviciile externe ale Kaspersky. Kaspersky Endpoint Security utilizează servicii externe pentru următoarele funcții:

- Actualizarea bazelor de date și modulelor aplicației;
- Activarea aplicației cu un cod de activare (activare 2.0);
- Utilizarea Kaspersky Security Network.

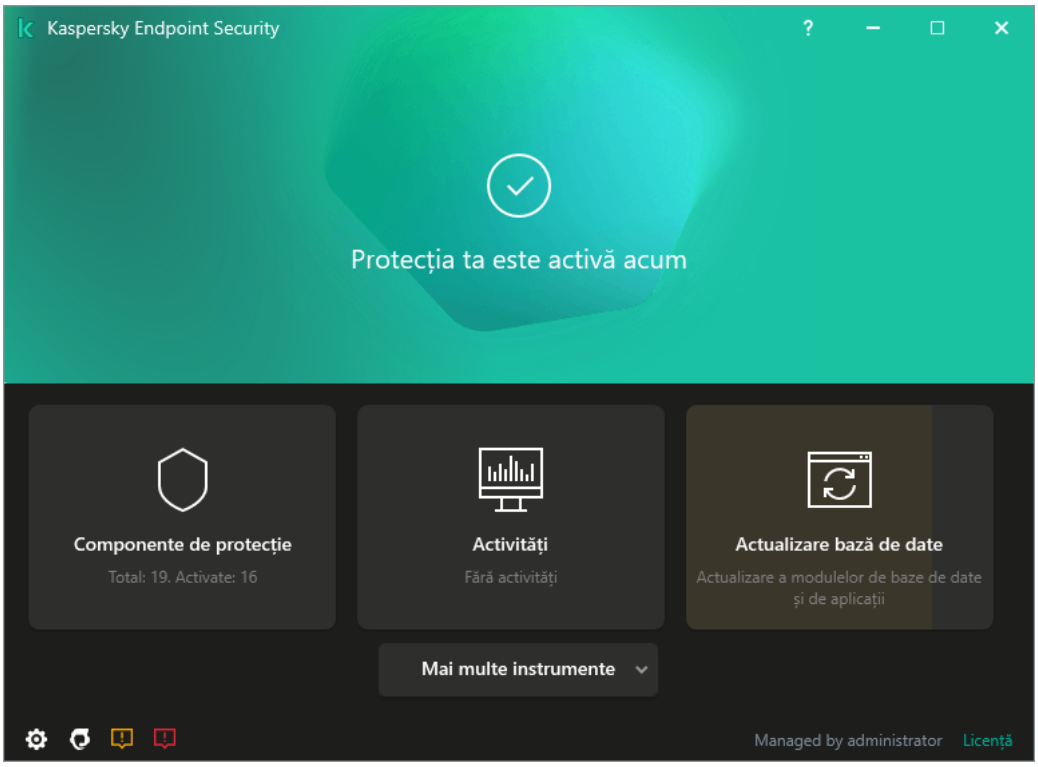
Utilizarea TLS securizează aplicația oferind următoarele caracteristici:

- 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. Pentru lucrul cu certificate este necesară o infrastructură cu cheie publică (PKI). 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 certificatelor autosemnate. 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

Componente protecție	Starea de funcționare a componentelor instalate. De asemenea, puteți continua să configurați oricare dintre componentele instalate, cu excepția componentelor de criptare.
Activități	Gestionați activitățile de scanare Kaspersky Endpoint Security. Puteți rula o scanare de viruși și o verificare a integrității aplicației. Un administrator poate ascunde sarcinile unui utilizator sau poate restricționa gestionarea sarcinilor.
Actualizare bază de date	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 sarcinile unui utilizator sau poate restricționa gestionarea sarcinilor.
Mai multe instrumente	Treceți la alte caracteristici ale aplicației. • **Rapoarte**. Vizualizați evenimentele care au avut loc în timpul funcționării aplicației, componentelor individuale și sarcinilor. • **Copie 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 oferă Kaspersky Endpoint Security informații despre categoria și reputația fișierelor scanate, precum și informații despre reputația adreselor web scanate. • **Monitorizare sistem**. Vizualizați informații despre funcționarea aplicațiilor instalate. Monitorizare sistem ține evidența evenimentelor (fișiere, registru și sistem 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.
⚙	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.
Licență	Licențierea aplicației. Puteți cumpăra o licență, puteți activa aplicația sau puteți reînnoi un abonament. De asemenea, puteți vizualiza informații despre licența curentă.

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.

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 / Repornire protecție**. 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, selectați **Reluare protecție și control** în meniul contextual al aplicației.

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

- **Dezactivare politică** / **Activare politică**. Dezactivează o politică 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 **Activare politică** în meniul contextual al aplicației.

- Setări. Deschide fereastra cu setările aplicației.

- **Asistență**. Deschide fereastra **Asistență**, care conține informațiile necesare pentru a contacta Serviciul de asistență tehnică al 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:

- **Dezactivare politică** / **Activare politică**. Dezactivează o politică 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 **Activare politică** în meniul contextual al aplicației.

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

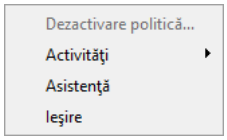
  - **Verificare integritate**.

  - **Derulare înapoi ultima actualizare**.

  - **Scanare completă**.

- **Scanare particularizată**.
- **Scanare zone critice**.
- **Actualizare**.

- **Asistență**. Deschide fereastra **Asistență**, care conține informațiile necesare pentru a contacta Serviciul de asistență tehnică al 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:

- **Cu 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, notificări deasupra pictogramei aplicației.
- **Cu interfață completă**. 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.
- **Fără interfață**. 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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Setări generale** → **Interfață**.
6. În secțiunea **Interacțiune cu utilizatorul**, efectuează una dintre următoarele acțiuni:
   - Bifați caseta de selectare **Afișare interfață aplicație** dacă dorești ca următoarele elemente ale interfeței să fie afișate pe computerul client:
     - Directorul care conține numele aplicației în meniul **Start**
     - Pictograma Kaspersky Endpoint Security în zona de notificări din bara de activități Microsoft Windows
     - Notificări pop-up

     Dacă această casetă de selectare este bifată, utilizatorul poate vedea și, dacă are drepturile corespunzătoare, poate modifica setările aplicației din interfața aplicației.
   - Debifați caseta de selectare **Afișare interfață aplicație** dacă vrei să ascunzi toate semnele funcționării aplicației Kaspersky Endpoint Security pe computerul client.
7. În secțiunea **Interacțiune cu utilizatorul**, bifați caseta de selectare **Interfață aplicație simplificată** dacă vrei să fie afișată interfața simplificată a aplicației pe un computer client pe care este instalată aplicația Kaspersky Endpoint Security.

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

1. În fereastra principală a Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security pentru computerele pe care doriți să activați asistența pentru modul portabil.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Selectați **Setări generale** → **Interfață**.
5. În secțiunea **Interacțiune cu utilizatorul**, configurați modul în care va fi afișată interfața aplicației:

   - **Cu 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, notificări deasupra pictogramei aplicației.
   - **Cu interfață completă**. 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.
   - **Fără interfață**. Pe un computer client, nu sunt afișate semne de funcționare a Kaspersky Endpoint Security. Pictograma din zona de notificare Windows și notificările sunt disponibile.
6. Faceți clic pe **OK**.

Noțiuni de bază

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. Expertul de configurare inițială al Kaspersky Security Center creează automat o politică pentru aplicația Kaspersky Endpoint Security.
- Creează activitățile *Actualizare* și *Scanare de viruși*.

  Activitatea *Actualizare* este necesară pentru menținerea actualizată a securității computerului. La efectuarea aceste activități, Kaspersky Endpoint Security actualizează bazele de date antivirus și modulele aplicației. Activitatea *Actualizare* este creată automat de Expertul de configurare inițială al Kaspersky Security Center. Pentru a crea activitatea *Actualizare*, instalați plug-inul web Kaspersky Endpoint Security for Windows în timp ce executați Expertul.

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

Cum se creează o activitate de scanare de viruși în Consola de administrare (MMC)

1. În Consola de administrare, accesați directorul **Server de administrare** → **Activități**.

   Lista activităților se deschide.

2. Faceți clic pe butonul **Activitate nouă**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Selectarea tipului activității

Selectați **Kaspersky Endpoint Security for Windows (11.6.0)** → **Scanare de viruși**.

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:

- **Dezinfectare; șterge dacă dezinfectarea nu reușește**. Dacă selectați această opțiune, Kaspersky Endpoint Security încearcă automat să dezinfecteze toate fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, Kaspersky Endpoint Security șterge fișierele.

- **Dezinfectare. Informează dacă dezinfectarea nu reușește**. Dacă selectați această opțiune, Kaspersky Endpoint Security încearcă automat să dezinfecteze toate fișierele infectate care sunt detectate. Dacă nu este posibilă dezinfectarea, Kaspersky Endpoint Security adaugă informațiile despre fișierele infectate detectate în lista de amenințări active.

- **Informare**. 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.

  Tehnologia de dezinfectare avansată 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.

Configurați modul de executare a activității utilizând caseta de selectare **Scanare doar când computerul este inactiv**. Această casetă de selectare activează/dezactivează funcția care suspendă activitatea *Scanare de viruși* când resursele computerului sunt limitate. Kaspersky Endpoint Security pune în pauză activitatea *Scanare de viruși* dacă economizorul de ecran este oprit și computerul este deblocat.

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 de viruși*. 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 **Executare activitate după terminarea Expertului**. Puteți monitoriza progresul activității în proprietățile activității. Ca rezultat, activitatea Scanare de viruși va fi executată pe computerele utilizatorilor în conformitate cu planificarea specificată.

[Cum se creează o activitate de scanare de viruși în Web Console]

1. În fereastra principală a Consolei Web, selectează **Devices** → **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe butonul **Adăugare**.

   Expertul de activitate pornește.

3. Configurați setările pentru activitate:

   a. În lista verticală **Application**, selectați **Kaspersky Endpoint Security for Windows (11.6.0)**.

   b. În lista verticală **Tip activitate**, selectați **Scanare de viruși**.

   c. În câmpul **Nume activitate**, introdu o descriere succintă, de exemplu `Scanare săptămânală`.

   d. În secțiunea **Select devices to which the task will be assigned**, selectați domeniul activității.

4. Selectați dispozitive în funcție de opțiunea selectată pentru domeniul activității. Faceți clic pe butonul **Next**.

5. Termină expertul făcând clic pe butonul **Finish**.

   Se va afișa o activitate nouă în lista de activități.

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

   Este recomandabil să configurezi o planificare care să execute activitatea cel puțin o dată pe săptămână.

7. Bifați caseta de selectare de lângă activitate.

8. Faceți clic pe butonul **Executare**.

   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 de viruși va fi executată pe computerele utilizatorilor în conformitate cu planificarea specificată.

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.

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.

Politică activă și inactivă

O politică este destinată unui grup de computere gestionate și poate fi activă sau inactivă. 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.

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.

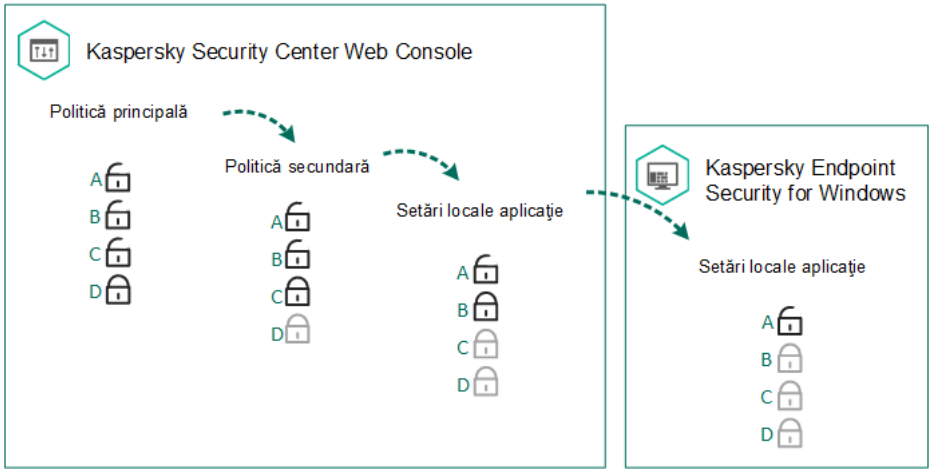
Politică Absent de la birou

O politică Absent de la birou se activează atunci când un computer părăsește perimetrul rețelei organizației.

Moștenire setări

Politicile, cum ar fi grupurile de administrare, sunt aranjate într-o ierarhie. În mod implicit, o politică secundară moștenește setările din politica principală. *Politica subordonată* este o politică pentru niveluri ierarhice imbricate, adică o politică pentru grupuri de administrare imbricate și Servere de administrare secundare. Puteți dezactiva moștenirea setărilor din politica principală.

Fiecare setare a politicii are atributul , care indică dacă setările pot fi modificate în politicile secundare sau în setările locale ale aplicației. Atributul este aplicabil numai dacă moștenirea setărilor pentru politica părinte este activată pentru politica subordonată. 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 **Securitate** din fereastra de proprietăți a serverului de administrare Kaspersky Security Center.

Crearea unei politici

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

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, selectați directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Faceți clic pe butonul **Politică nouă**.

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

Cum se creează o politică în Web Console și Cloud Console

1. În fereastra principală a Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.
2. Faceți clic pe butonul **Adăugare**.

   Expertul de politică pornește.
3. Selectați Kaspersky Endpoint Security și faceți clic pe **Următorul**.
4. Citește și acceptă condițiile din Declarația de Securitate a Rețelei Kaspersky (KSN) și faceți clic pe **Următorul**.
5. În fila **General** poți efectua următoarele acțiuni:
   - Schimbă numele politicii.
   - Selectați starea politicii:
     - **Activă**. După următoarea sincronizare, politica va fi folosită drept politica activă pe computer.
     - **Inactivă**. Faceți o copie de rezervă a politicii. Dacă este necesar, o politică inactivă poate fi comutată la starea Activă.
     - **Absent de la birou**. Politica este activată atunci când un computer părăsește perimetrul rețelei organizației.
   - Configurați moștenirea setărilor:
     - **Moștenire setări de la politica părinte**. 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.
     - **Forțați moștenirea setărilor pentru politicile secundare**. Dacă acest buton de comutare este pornit, valorile setărilor pentru politică se propagă în politicile subordonate. În proprietățile politicii secundare, butonul de comutare **Moștenire setări politică principală** 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.
6. În fila **Setări aplicație** poți configura setările pentru politici Kaspersky Endpoint Security.
7. Faceți clic pe butonul **Save**.

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 **Asistență** 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 *Ghidul de ajutor pentru Kaspersky Security Center*.

Indicator nivel de securitate

Indicatorul nivelului de securitate este afișat în partea de sus a ferestrei **Proprietăți: <nume politică>**. 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:
  - **Critic**. Această categorie include componentele următoare:
    - File Threat Protection.
    - Behavior Detection.
    - Exploit Prevention.
    - Remediation Engine.
  - **Important**. Această categorie include componentele următoare:
    - Kaspersky Security Network.
    - Web Threat Protection.
    - Mail Threat Protection.
    - Host Intrusion Prevention.
- **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.

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 de viruși**. Kaspersky Endpoint Security scanează de viruși și alte amenințări zonele din computer specificate în setările activității. Activitatea *Scanare de viruși* este necesară pentru funcționarea aplicației Kaspersky Endpoint Security și se creează în timpul executării Expertului de configurare inițială. Este recomandabil să configurezi o planificare care să execute activitatea cel puțin o dată pe săptămână.

- **Adăugare 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.

- **Change application components**. 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 *Inventariere* se efectuează de către componenta Application Control. Dacă nu este instalată componenta Application Control, activitatea se va termina cu o eroare.

- **Actualizare**. Kaspersky Endpoint Security actualizează bazele de date și modulele aplicației. Activitatea *Actualizare* este necesară pentru funcționarea aplicației Kaspersky Endpoint Security se creează în timpul executării Expertului de configurare inițială. Este recomandabil să configurezi o planificare care să execute activitatea cel puțin o dată zi.

- **Ștergere date**. 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**. 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.

Activitățile se execută pe un computer numai dacă aplicația Kaspersky Endpoint Security se execută.

Adăugați o activitate nouă

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. Faceți clic pe butonul **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 Consolei Web, selectează **Devices** → **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe butonul **Adăugare**.

   Expertul de activitate pornește.

3. Configurați setările pentru activitate:

   a. În lista verticală **Application**, selectați **Kaspersky Endpoint Security for Windows (11.6.0)**.

   b. În lista verticală **Task type**, selectați activitatea pe care dorești să o execuți pe computere ale utilizatorilor.

   c. În câmpul **Task name**, introdu o descriere succintă, de exemplu `Actualizare aplicație pentru contabilitate`.

   d. În secțiunea **Select devices to which the task will be assigned**, selectați domeniul activității.

4. Selectați dispozitive în funcție de opțiunea selectată pentru domeniul activității. Faceți clic pe butonul **Next**.

5. Termină expertul făcând clic pe butonul **Finish**.

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. Poți, de asemenea, să creezi o selecție de evenimente pentru monitorizarea finalizării activităților (**Monitorizare și rapoarte** → **Selectare evenimente**). Pentru mai multe detalii despre selectarea evenimentelor, *consultați Ghidul de ajutor pentru Kaspersky Security Center*. Rezultatele executării activității se salvează tot local, în jurnalul de evenimente Windows și în rapoartele aplicației Kaspersky Endpoint Security.

Controlul 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 accesule 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*.

Puteți 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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** 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 **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Activități locale** → **Gestionare activități**.
6. Configurați modul de gestionare a activităților (consultați tabelul de mai jos).
7. Salvați-vă modificările.

Cum se configurează modul de gestionare a activităților în interfața Kaspersky Endpoint Security prin Web Console

1. În fereastra principală a Consolei Web, selectați fila **Dispozitive** → **Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security pentru computerele pe care doriți să activați asistența pentru modul portabil.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Accesați **Local tasks** → **Task management**.
5. Configurați modul de gestionare a activităților (consultați tabelul de mai jos).
6. Faceți clic pe **OK**.
7. Confirmă modificările făcând clic pe **Salvare**.

Setări pentru Gestionare activități

Parametru	Descriere
Permite utilizarea activităților locale	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 rîmâne 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 de viruși a unui fișier sau director selectând opțiunea **Scanare de viruși** în meniul contextual al fișierului sau directorului respectiv. Activitatea de scanare este pornită cu valorile implicite pentru activitatea de scanare particularizată.

Permite afișarea activităților de grup	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.
Permitere gestionare activități de grup	În cazul în care caseta de selectare este bifată, utilizatorii pot porni și opri activitățile de grup specificate în 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 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 **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparține computerul client relevant.
3. În spațiul de lucru, selectați fila **Dispozitive**.
4. Selectați computerul pentru care dorești să configurezi setările Kaspersky Endpoint Security.
5. În meniul contextual al computerului client, selectează **Proprietăți**.

   Se deschide fereastra de proprietăți a computerului client.
6. În fereastra de proprietăți a computerului client, selectați secțiunea **Aplicații**.

   În dreapta ferestrei Proprietăți computer client apare o listă de aplicații Kaspersky instalate pe computerul client.
7. Selectați Kaspersky Endpoint Security.
8. Faceți clic pe butonul **Proprietăți** de sub lista de aplicații Kaspersky.

   Apare fereastra **de setări pentru aplicația Kaspersky Endpoint Security for Windows**.
9. În secțiunea **Setări generale**, configurați setările pentru Kaspersky Endpoint Security, precum și setările pentru rapoarte și stocare.

   Celelalte secțiuni din fereastra de **setări pentru aplicația Kaspersky Endpoint Security for Windows** sunt identice cu cele din secțiunile standard ale 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**.
10. Pentru a salva modificările, în fereastra **Setări pentru aplicația Kaspersky Endpoint Security for Windows**, faceți clic pe **OK**.

Cum se configurează setările locale pentru aplicație în Web Console și Cloud Console

1. În fereastra principală a Consolei Web. selectați **Dispozitive** → **Dispozitive gestionate**.
2. Selectează computerul pentru care dorești să configurezi setări locale pentru aplicație.
   Se vor deschide proprietățile computerului.
3. Selectați fila **Aplicații**.
4. Faceți clic pe **Kaspersky Endpoint Security for Windows**.
   Se vor deschide setările locale pentru aplicație.
5. Selectați fila **Setări aplicație**.
6. Configurați setările locale pentru aplicație.
7. 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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Setări generale** → **Setări aplicație**.
6. Folosește caseta de selectare **Pornire Kaspersky Endpoint Security for Windows la pornirea computerului** pentru a configura pornirea aplicației.
7. Salvați-vă modificările.

Cum se configurează pornirea Kaspersky Endpoint Security în Web Console

1. În fereastra principală a Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security pentru computerele pentru care dorești să configurezi pornirea aplicației.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Selectați **Setări generale**.
5. Faceți clic pe linkul **Setări aplicație**.
6. Folosește caseta de selectare **Pornire Kaspersky Endpoint Security for Windows la pornirea computerului** pentru a configura pornirea aplicației.
7. Faceți clic pe **OK**.
8. Confirmă modificările făcând clic pe **Salvare**.

Cum se configurează pornirea Kaspersky Endpoint Security în interfața aplicației

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra de setări a aplicației, selectați secțiunea **General**.
3. Utilizați caseta de selectare **Lansare la pornirea computerului** pentru a configura modul în care pornește aplicația.
4. Pentru a salva modificările, faceți clic pe butonul **Salvare**.

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 **Stare protecție**.

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 **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparține computerul client relevant.
3. În spațiul de lucru, selectați fila **Dispozitive**.
4. Selectează computerul pe care dorești să pornești sau să oprești aplicația.
5. Fă clic dreapta pentru a afișa meniul contextual al computerului client și selectează **Proprietăți**.
6. În fereastra de proprietăți a computerului client, selectați secțiunea **Aplicații**.

   În dreapta ferestrei Proprietăți computer client apare o listă de aplicații Kaspersky instalate pe computerul client.
7. Selectați Kaspersky Endpoint Security.
8. Efectuează 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 Consolei Web. selectați **Dispozitive** → **Dispozitive gestionate**.
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 **Aplicații**.
4. Bifați caseta de selectare din partea opusă a aplicației **Kaspersky Endpoint Security for Windows**.
5. Fă clic pe butonul **Pornire** sau **Oprire**.

Cum se pornește sau se oprește Kaspersky Endpoint Security din linia de comandă

Pentru a opri aplicația din linia de comandă, activați gestionarea externă a serviciilor de sistem.

Fișierul klpsm.exe, care este inclus în kitul de distribuire Kaspersky Endpoint Security, se folosește pentru pornirea sau oprirea aplicației 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. 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`.

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 se reiau 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. Faceți clic pe butonul **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 **Reluare protecție**.

Poți relua oricând protecția și controlul computerului, indiferent care este opțiunea de trecere în pauză a protecției și a controlului computerului selectată anterior.

Scanarea computerului

O scanare de viruși este esențială pentru securitatea computerului. Scanările de viruși executate regulat contribuie la eliminarea posibilității 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:

- Memorie 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 executarea 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 particularizată

Kaspersky Endpoint Security scanează obiectele selectate de utilizator. Poți scana orice obiect din următoarea listă:

- Memorie kernel
- Obiectele încărcate la pornirea sistemului de operare
- Crearea unei copii de rezervă a sistemului de operare

- Cutia poștală Microsoft Outlook
- Unități de hard disk, amovibile și de rețea
- Orice fișier selectat

Scanare în fundal

Scanare în fundal este un mod 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

Kaspersky Endpoint Security verifică modulele aplicației pentru a vedea dacă sunt deteriorate sau modificate.

Pornirea și oprirea unei activități de scanare

Indiferent de modul de executare a activității de scanare pe care îl selectezi, poți porni sau opri oricând o activitate de scanare.

Pentru a porni sau opri o activitate de scanare:

1. În fereastra principală a aplicației, faceți clic pe butonul **Activități**.
2. Faceți clic pe butonul **Pornire scanare** dacă vrei să execuți 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 **Oprire**.

Pentru a porni sau a opri o activitate de scanare atunci când este afișată interfața simplificată a aplicației:

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 scanare care nu se execută pentru a o porni
   - selectați o activitate de scanare care se execută pentru a o opri
   - selectați o activitate de scanare în pauză pentru a o relua sau a o porni

Schimbarea nivelului de securitate

Kaspersky Endpoint Security poate utiliza diferite grupuri de setări pentru executarea unei scanări. Aceste grupuri de setări salvate în aplicație sunt denumite *niveluri de securitate*: **Ridicat**, **Recomandat**, **Redus**. Setările pentru nivelul de securitate **Recomandat** sunt considerate optime. Ele sunt recomandate de experții Kaspersky. 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.

Pentru a modifica un nivel de securitate:

1. În fereastra principală a aplicației, faceți clic pe butonul **Activități**.
2. În fereastra deschisă, selectați activitatea de scanare și faceți clic pe butonul ⚙.
3. În secțiunea **Nivel de securitate**, efectuează una dintre următoarele acțiuni:
   - Dacă doriți să aplicați unul dintre nivelurile de securitate presetate, selectați-l folosind glisorul:
     - **Ridicat**. Kaspersky Endpoint Security scanează toate tipurile de fișiere. La scanarea fișierelor compuse, Kaspersky Endpoint Security scanează și fișierele multi-format.
     - **Recomandat**. Kaspersky Endpoint Security scanează numai formatele de fișiere specificate de pe toate unitățile de hard disk, de pe toate unitățile de rețea și de pe toate suporturile de stocare amovibile ale computerului, dar și de pe obiecte OLE încorporate. Kaspersky Endpoint Security nu scanează arhivele și pachetele de instalare.
     - **Redus**. Kaspersky Endpoint Security scanează numai fișierele noi sau modificate, cu extensii specificate de pe toate unitățile de hard disk, unitățile amovibile și unitățile de rețea ale computerului. Kaspersky Endpoint Security nu scanează fișierele compuse.
   - Dacă doriți să configurați un nivel de securitate personalizat, faceți clic pe butonul **Setări avansate** și definiți propriile setări pentru componentă.

     Puteți restabili valorile nivelurilor de securitate presetate făcând clic pe butonul **Restaurare nivel recomandat de securitate** din partea superioară a ferestrei.
4. Salvați-vă modificările.

Schimbarea acțiunii de efectuat asupra fișierelor infectate

În mod implicit, la detectarea unor fișiere infectate, Kaspersky Endpoint Security încearcă să le dezinfecteze sau le șterge, dacă dezinfectarea nu este posibilă.

Pentru a schimba acțiunea de efectuat asupra fișierelor infectate:

1. În fereastra principală a aplicației, faceți clic pe butonul **Activități**.
2. În fereastra deschisă, selectați activitatea de scanare și faceți clic pe butonul ⚙.
3. În blocul **Acțiune la detectarea amenințării**, selectați una dintre următoarele opțiuni:
   - **Dezinfectare; șterge dacă dezinfectarea nu reușește**. Dacă selectați această opțiune, Kaspersky Endpoint Security încearcă automat să dezinfecteze toate fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, Kaspersky Endpoint Security șterge fișierele.

- **Dezinfectare. Blochează dacă dezinfectarea nu reușește**. Dacă selectați această opțiune, Kaspersky Endpoint Security încearcă automat să dezinfecteze toate fișierele infectate care sunt detectate. Dacă nu este posibilă dezinfectarea, Kaspersky Endpoint Security adaugă informațiile despre fișierele infectate detectate în lista de amenințări active.

- **Informare**. 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, Kaspersky Endpoint Security 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.

4. Salvați-vă modificările.

Generarea unei liste de obiecte de scanat

Pentru a genera o listă de obiecte de scanat:

1. În fereastra principală a aplicației, faceți clic pe butonul **Activități**.
2. În fereastra deschisă, selectați activitatea de scanare și faceți clic pe butonul ⚙.
3. Faceți clic pe linkul **Editare domeniu de scanare**.
4. În fereastra deschisă, selectați obiectele pe care doriți să le adăugați la domeniul de scanare sau să le excludeți din acesta.

   Nu poți șterge sau edita obiecte care sunt incluse în domeniul de scanare implicit.

5. Dacă dorești să adaugi un obiect nou la domeniul de scanare:

   a. Faceți clic pe butonul **Adăugare**.

      Se deschide arborele de directoare.

   b. Selectați obiectul și apăsați pe **Selectare**.

   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.

6. Salvați-vă modificările.

Selectarea unui tip de fișiere de scanat

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 selecta un tip de fișiere de scanat:

1. În fereastra principală a aplicației, faceți clic pe butonul **Activități**.

2. În fereastra deschisă, selectați activitatea de scanare și faceți clic pe butonul ⚙.

3. Faceți clic pe butonul **Setări avansate**.

4. În secțiunea **Tipuri de fișiere**, specifică tipurile de fișiere care dorești să fie scanate la executarea activității de scanare selectate:

   - **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, Kaspersky Endpoint Security 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, Kaspersky Endpoint Security scanează numai fișierele infectabile. Formatul fișierului se determină în funcție de extensia sa.

   Kaspersky Endpoint Security consideră fișierele fără extensie ca fiind fișiere executabile. Kaspersky Endpoint Security scanează întotdeauna fișierele executabile, indiferent de tipurile de fișiere selectate pentru scanare.

5. Salvați-vă modificările.

Optimizarea scanării de fișiere

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).

De asemenea, puteți activa utilizarea tehnologiilor 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.

Pentru a optimiza scanarea de fișiere:

1. În fereastra principală a aplicației, faceți clic pe butonul **Activități**.
2. În fereastra deschisă, selectați activitatea de scanare și faceți clic pe butonul ⚙.
3. Faceți clic pe butonul **Setări avansate**.
4. În blocul **Optimizare scanare**, configurați setările de scanare:
   - **Scanare 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.
   - **Omitere fișiere scanate mai mult de N secunde**. Limitează durata scanării unui singur obiect. După scurgerea duratei specificate, Kaspersky Endpoint Security oprește scanarea fișierului. Acest lucru reduce durata unei scanări.
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.

Pentru a configura scanarea fișierelor compuse:

1. În fereastra principală a aplicației, faceți clic pe butonul **Activități**.
2. În fereastra deschisă, selectați activitatea de scanare și faceți clic pe butonul ⚙.
3. Faceți clic pe butonul **Setări avansate**.
4. În secțiunea **Scanare fișiere compuse**, specifică fișierele compuse pe care dorești să le scanezi: arhive, pachete de instalare, fișiere în formate Office, fișiere în format corespondență și arhive protejate prin parolă.
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. În blocul **Limită dimensiune**, efectuați una dintre următoarele acțiuni:
   - Dacă nu dorești să dezarhivezi fișierele compuse de dimensiuni mari, bifați caseta de selectare **Nu dezarhiva fișiere compuse mari** și specifică valoarea necesară în câmpul **Dimensiune maximă fișier**.
   - Dacă dorești să dezarhivezi fișiere compuse de dimensiuni mari, indiferent de dimensiunea lor, debifați caseta de selectare **Nu dezarhiva fișiere compuse mari**.

Kaspersky Endpoint Security scanează fișierele de dimensiuni mari extrase din arhive indiferent dacă este bifată sau nu caseta de selectare **Nu dezarhiva fișiere compuse mari**.

7. 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 utiliza metode de scanare:

1. În fereastra principală a aplicației, faceți clic pe butonul **Activități**.
2. În fereastra deschisă, selectați activitatea de scanare și faceți clic pe butonul ⚙.
3. Faceți clic pe butonul **Setări avansate**.
4. Dacă doriți ca aplicația să utilizeze analiza euristică atunci când rulează activitatea de scanare, bifați caseta de selectare **Analiză euristică** din blocul **Metode de scanare**. Apoi utilizați cursorul pentru a seta nivelul analizei euristice: **Scanare rapidă**, **Scanare normală** sau **Scanare riguroasă**.
5. Salvați-vă modificările.

Utilizarea tehnologiilor de scanare

Pentru a utiliza tehnologii de scanare:

1. În fereastra principală a aplicației, faceți clic pe butonul **Activități**.
2. În fereastra deschisă, selectați activitatea de scanare și faceți clic pe butonul ⚙.
3. Faceți clic pe butonul **Setări avansate**.
4. În blocul **Tehnologii de scanare**, bifați casetele de selectare de lângă numele tehnologiilor care doriți să fie utilizate în timpul unei scanări:

   - **Tehnologie iSwift**. Această tehnologie permite creșterea vitezei de scanare excluzând de la scanare anumite fișiere. Fișierele sunt excluse de la scanare 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.

- **Tehnologie 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.

Selectarea modului de executare pentru activitatea de scanare

Dacă nu se poate executa activitatea de scanare dintr-un anumit motiv (de exemplu, computerul este oprit la momentul respectiv), poți configura activitatea omisă pentru executare automată atunci când este posibil.

Poți amâna începerea activității de scanare dacă ora de pornire a acesteia corespunde cu ora de pornire a Kaspersky Endpoint Security. Activitatea de scanare 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 scanare:

1. În fereastra principală a aplicației, faceți clic pe butonul **Activități**.
2. În fereastra deschisă, selectați activitatea de scanare și faceți clic pe butonul ⚙.
3. Faceți clic pe butonul **Planificare scanare**.
4. În fereastra deschisă, configurați programul de rulare a activității de scanare.
5. În funcție de frecvența selectată, configurați setările avansate pentru a specifica planificare de executare a activității.
   a. Selectați **Executare scanare planificată în ziua următoare dacă computerul este închis** dacă doriți ca Kaspersky Endpoint Security să execute sarcinile de scanare ratate cu prima ocazie.

      Dacă este selectat elementul **La fiecare minut**, **La fiecare oră**, **După pornirea aplicației** sau **După fiecare actualizare** în lista verticală **Executare scanare**, caseta de selectare **Executare scanare planificată în ziua următoare dacă computerul este închis** nu este disponibilă.

   b. Dacă dorești ca aplicația Kaspersky Endpoint Security să suspende o activitate atunci când resursele computerului sunt limitate, bifează caseta de selectare **Execută doar atunci când computerul este inactiv**. Kaspersky Endpoint Security pornește activitatea de scanare dacă computerul este blocat sau dacă economizorul de ecran este pornit.

      Această opțiune de planificare ajută la conservarea resurselor computerului.

6. Salvați-vă modificările.

Pornirea unei activități de scanare din contul altui utilizator

În mod implicit, o activitate de scanare se execută cu permisiunile contului în care utilizatorul s-a conectat la sistemul de operare. Cu toate acestea, este posibil să fie necesar să execuți o activitate de scanare din alt cont de utilizator. Poți să specifici un utilizator care are drepturile corespunzătoare în setările pentru activitatea de scanare și să execuți activitatea de scanare din contul acestui utilizator.

Pentru a configura pornirea unei activități de scanare din contul altui utilizator:

1. În fereastra principală a aplicației, faceți clic pe butonul **Activități**.
2. În fereastra deschisă, selectați activitatea de scanare și faceți clic pe butonul ⚙.
3. Faceți clic pe **Setări avansate** → **Executare scanare ca**.
4. În fereastra deschisă, selectați utilizatorul care solicită drepturile pentru a începe activitatea de scanare.
5. Salvați-vă modificările.

Scanarea unităților amovibile atunci când sunt conectate la computer

Kaspersky Endpoint Security scanează toate fișierele pe care le executați sau le copiați, 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 (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.

Pentru a configura scanarea unităților amovibile atunci când acestea sunt conectate:

1. În fereastra principală a aplicației, faceți clic pe butonul **Activități**.
2. În fereastra deschisă, selectați sarcina de scanare a unității amovibile și faceți clic pe butonul ⚙.
3. Utilizați comutatorul **Scanare unități amovibile** pentru a activa sau a dezactiva scanările unităților amovibile la conectarea la computer.
4. Selectați modul de scanare a unităților amovibile la conectare:
   - **Scanare detaliată** Dacă este selectat acestă opțiune, atunci când este conectată o unitate amovibilă, Kaspersky Endpoint Security scanează toate fișierele de pe unitatea 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.
   - **Scanare rapidă** Dacă această opțiune este selectată, atunci când o unitate amovibilă este conectată, Kaspersky Endpoint Security va scana numai fișierele cu anumite formate care sunt cele mai vulnerabile să fie infectate și nu va dezarhiva obiectele compuse.
5. Dacă dorești ca aplicația Kaspersky Endpoint Security să scaneze doar acele unități amovibile a căror capacitate nu depășește valoarea specificată, bifați caseta de selectare **Dimensiune maximă unitate amovibilă** și specifică în câmpul alăturat valoarea (în megaocteți).
6. Configurați modul în care va fi afișat progresul scanării unui disc amovibil. Efectuează una dintre următoarele acțiuni:

- Dacă doriți ca aplicația Kaspersky Endpoint Security să afișeze progresul scanării unității amovibile într-o fereastră separată, bifați caseta de selectare **Afișare progres scanare**.

  În fereastra de scanare a unității amovibile, utilizatorul poate opri scanarea. Pentru ca scanările unității amovibile să fie obligatorii și să se împiedice utilizatorul să oprească o scanare, bifați caseta de selectare **Blochează oprirea activității de scanare** .

- Dacă dorești ca aplicația Kaspersky Endpoint Security să execute în fundal o scanare a unității amovibile, debifați caseta de selectare **Afișare progres scanare**.

7. Pentru a salva modificările, faceți clic pe butonul **Salvare**.

Scanare în fundal

Scanare în fundal este un mod 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. 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.

Pentru a activa scanări în fundal ale computerului:

1. În fereastra principală a aplicației, faceți clic pe butonul **Activități**.
2. În fereastra deschisă, selectați activitatea de scanare și faceți clic pe butonul ⚙.
3. Utilizați comutatorul **Scanare în fundal** pentru a activa sau dezactiva scanările în fundal.
4. Salvați-vă modificările.

Verificarea integrității aplicației

Kaspersky Endpoint Security verifică fișierele aplicației din directorul de instalare a 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* este destinată scanării fișierelor aplicațiilor. Executați activitatea *Verificare integritate* dacă Kaspersky Endpoint Security a detectat un obiect rău intenționat, dar nu l-a neutralizat.

Puteți crea activitatea *Verificare integritate* atât în Kaspersky Security Center 12 Web Console, cât și în Consola de administrare. Nu este posibilă crearea unei activități în Kaspersky Security Center Cloud Console.

Cum se rulează o verificare a integrității aplicației prin Consola de administrare (MMC)

1. În Consola de administrare, accesați directorul **Server de administrare** → **Activități**.

   Lista activităților se deschide.

2. Faceți clic pe butonul **Activitate nouă**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Selectarea tipului activității

Selectați **Kaspersky Endpoint Security for Windows (11.6.0)** → **Verificare integritate**.

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 **Executare activitate după terminarea Expertului**. 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.

[Cum se rulează o verificare a integrității aplicației prin Web Console]

1. În fereastra principală a Consolei Web, selectează **Devices** → **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe butonul **Adăugare**.

   Expertul de activitate pornește.

3. Configurați setările pentru activitate:

   a. În lista verticală **Application**, selectați **Kaspersky Endpoint Security for Windows (11.6.0)**.

   b. În lista verticală **Tip activitate**, selectați **Verificare integritate**.

   c. În câmpul **Nume activitate**, introduceți o descriere succintă, de exemplu, `Verifică integritatea aplicației după o infectare a computerului`.

   d. În secțiunea **Select devices to which the task will be assigned**, selectați domeniul activității.

4. Selectați dispozitive în funcție de opțiunea selectată pentru domeniul activității. Faceți clic pe butonul **Next**.

5. Termină expertul făcând clic pe butonul **Finish**.

   Se va afișa o activitate nouă în lista de activități.

6. 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.

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.

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.

Actualizările regulate necesită o licență activă. Dacă nu există nicio licență curentă, vei avea posibilitatea să efectuezi doar o singură actualizare.

Sursa principală de actualizare a aplicației Kaspersky Endpoint Security o reprezintă serverele de actualizare Kaspersky.

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.

Fișierele de ajutor contextual pentru aplicație pot fi actualizate odată cu actualizările modulelor aplicației.

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 secțiunea **Actualizare** din fereastra **Activități**.

Informațiile despre rezultatele actualizărilor și despre toate evenimentele care apar în timpul funcționării activității de actualizare sunt înregistrate în Raportul Kaspersky Endpoint Security.

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:

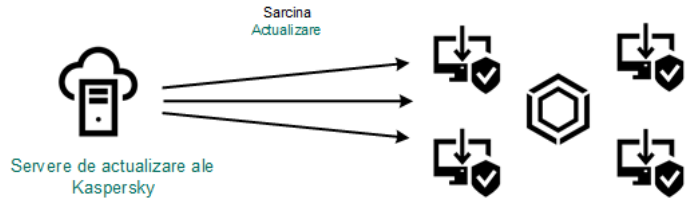
- Bazele de date antivirus. Bazele de date antivirus includ baze de date cu semnături de programe malware, descrieri ale atacurilor de rețea, baze de date de adrese Web rău intenționate și phishing, baze de date de bannere, baze de date de mesaje spam și alte date.

- 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 servere 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 *Descărcare actualizări în depozitul Serverului de administrare*.

  2. Descărcați pachetul de actualizare într-un director partajat (opțional).

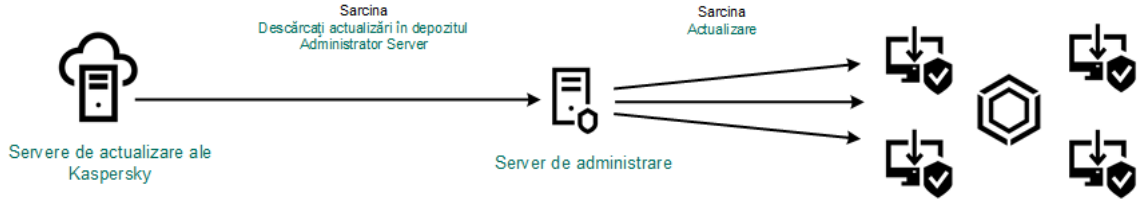
     Puteți descărca pachetul de actualizare într-un director partajat folosind următoarele metode:

     - Utilizând activitatea *Actualizare* din aplicația Kaspersky Endpoint Security. Activitatea este destinată unuia dintre computerele din rețeaua locală a companiei.

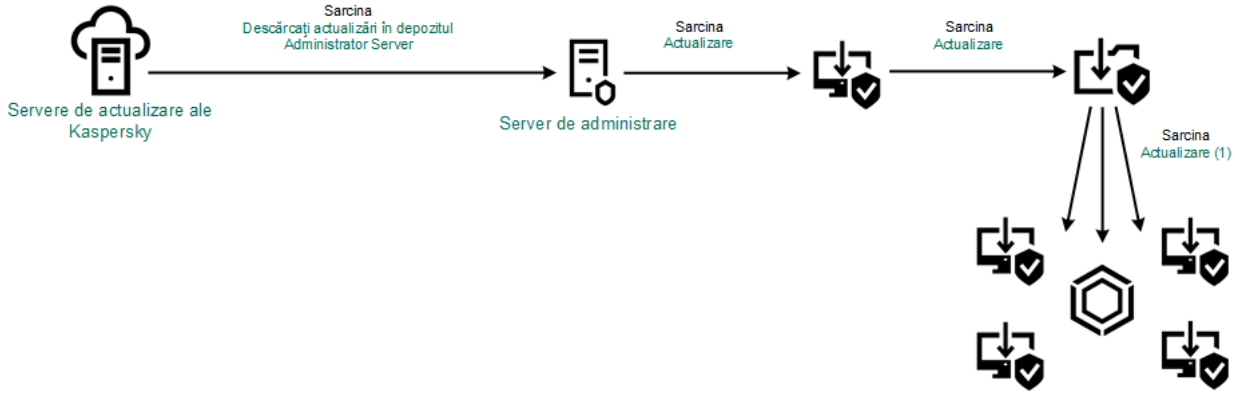
     - Folosirea Utilitarului de actualizare Kaspersky. Pentru informații detaliate despre Utilitarul de actualizare Kaspersky, *consultați* Baza de cunoștințe Kaspersky.

  3. Distribuirea pachetului de actualizare către computere client.

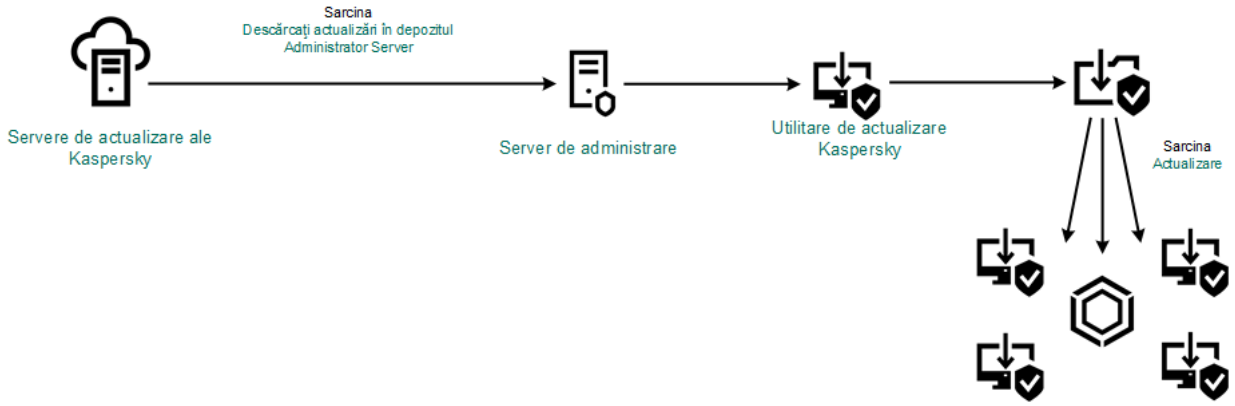
Pachetul de actualizare este distribuit către computere client prin intermediul activității *Actualizare* a aplicației Kaspersky Endpoint Security. Poți crea un număr nelimitat de activități de actualizare pentru fiecare grup de administrare.



Actualizarea din depozitul unui server



Actualizarea dintr-un director partajat



Actualizarea folosind Utilitarul de actualizare Kaspersky

Pentru Web Console, lista implicită de surse 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 *Ajutor pentru Kaspersky Security Center Cloud Console*. Poți adăuga la listă alte surse de actualizare. Poți 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.

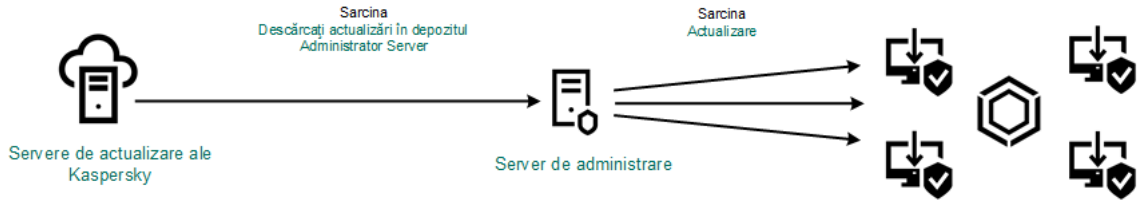
Actualizarea din depozitul unui server

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. Configurarea descărcării unui pachet de actualizare în depozitul Serverului de administrare (activitatea *Descărcare actualizări în depozitul Serverului de administrare*).

2. Configurarea actualizărilor pentru bazele de date și modulele aplicației din depozitul serverului specificat pe celelalte computere din rețeaua locală a organizației (activitatea *Actualizare*).



Actualizarea din depozitul unui server

Pentru a configura descărcarea unui pachet de actualizare în depozitul serverului:

1. În fereastra principală a Consolei Web, selectează **Devices** → **Tasks**.

   Lista activităților se deschide.

2. Selectați activitatea **Descărcare actualizări în depozit** a Serverului de administrare.

   Se va deschide fereastra de proprietăți a activității.

   Activitatea *Descărcare actualizări în depozit* a Serverului de administrare se creează automat de către Expertul de configurare inițială din Kaspersky Security Center 12 Web Console și această activitate poate avea numai o singură instanțiere.

3. Selectați fila **Setări aplicație**.

4. În secțiunea **Alte setări**, faceți clic pe **Configurare**.

5. În câmpul **Director de stocare actualizare**, specifică adresa serverului FTP sau HTTP, directorul de rețea ori directorul local unde Kaspersky Security Center copiază pachetul de actualizare primit de la servere de actualizare Kaspersky.

   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://<nume utilizator>:<parolă>@<nod>:<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\AVP11\Update distribution\`.

6. Salvați-vă modificările.

Pentru a configura actualizarea pentru Kaspersky Endpoint Security din zona de stocare a serverului specificat:

1. În fereastra principală a Consolei Web, selectează **Devices** → **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe activitatea **Actualizare** pentru Kaspersky Endpoint Security.

   Se va deschide fereastra de proprietăți a activității.

   Activitatea *Actualizare* este creată automat de Expertul de configurare inițială al Kaspersky Security Center. Pentru a crea activitatea *Actualizare*, instalați plug-inul web Kaspersky Endpoint Security for Windows în timp ce executați Expertul.

3. Selectați fila **Setări aplicație** → **Mod local**.

4. În lista de surse de actualizări, faceți clic pe butonul **Adăugare**.

5. În câmpul **Sursă**, 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 actualizări trebuie să se potrivească cu adresa pe care ai specificat-o în câmpul **Director pentru stocare actualizări** atunci când ai configurat copierea pachetului de actualizare în spațiul de stocare al serverului (vezi *instrucțiunii de mai sus*).

6. În secțiunea **Stare**, selectați **Activat**.

7. Faceți clic pe **OK**.

8. Configurați prioritățile surselor de actualizări folosind butoanele **Sus** și **Jos**.

9. Faceți clic pe butonul **Save**.

Dacă o actualizare nu poate fi efectuată din prima sursă de actualizare, Kaspersky Endpoint Security comută automat la sursa următoare.

Actualizarea dintr-un director partajat

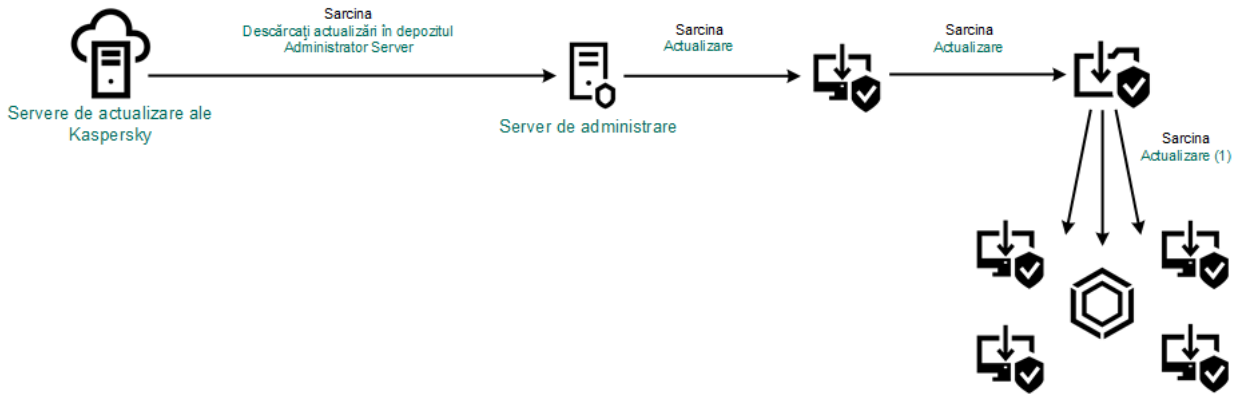
Pentru a conserva traficul pe Internet, poți configura actualizări ale bazelor de date și modulelor aplicației pe computere din rețeaua locală a organizației dintr-un director partajat. În acest scop, unul dintre computerele din rețeaua locală a organizației trebuie să primească pachete de actualizare 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.

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. Permiteți copierea unui pachet de actualizare într-un director partajat pe unul dintre computerele din rețeaua LAN a întreprinderii (consultați instrucțiunile de mai jos).

3. Configurarea actualizărilor pentru bazele de date și modulele aplicației din directorul partajat specificat pe celelalte computere din rețeaua LAN a întreprinderii (consultați instrucțiunile de mai jos).



Actualizarea dintr-un director partajat

Pentru a permite copierea pachetului de actualizare în directorul partajat:

1. În fereastra principală a Consolei Web, selectează **Devices** → **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe activitatea **Actualizare** pentru Kaspersky Endpoint Security.

   Se va deschide fereastra de proprietăți a activității.

   Activitatea *Actualizare* este creată automat de Expertul de configurare inițială al Kaspersky Security Center. Pentru a crea activitatea *Actualizare*, instalați plug-inul web Kaspersky Endpoint Security for Windows în timp ce executați Expertul.

3. Selectați fila **Setări aplicație** → **Mod local**.

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 **Copiere actualizări în folder**.

6. În câmpul **Cale**, introduceți calea UNC către directorului partajat (de exemplu, `\\Server\Partajare\Actualizare distribuție`).

   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\AVP11\Update distribution\`.

7. Faceți clic pe butonul **Save**.

Activitatea *Actualizare* trebuie atribuită unui computer care va servi drept sursă de actualizări.

Pentru a configura actualizările dintr-un director partajat:

1. În fereastra principală a Consolei Web, selectează **Devices** → **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe butonul **Adăugare**.

   Expertul de activitate pornește.

3. Configurați setările pentru activitate:

   a. În lista verticală **Application**, selectați **Kaspersky Endpoint Security for Windows (11.6.0)**.

   b. În lista verticală **Tip activitate**, selectați **Actualizare**.

   c. În câmpul **Nume activitate**, introdu o descriere succintă, de exemplu `Actualizare din director partajat`.

   d. În secțiunea **Select devices to which the task will be assigned**, selectați domeniul activității.

   > Activitatea *Actualizare* 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 fă clic pe **Următorul**.

5. Termină expertul făcând clic pe butonul **Creare**.

   Se va afișa o activitate nouă în tabelul cu activități.

6. Faceți clic pe activitatea *Actualizare* nou creată.

   Se va deschide fereastra de proprietăți a activității.

7. Accesează secțiunea **Setări aplicație**.

8. Selectați fila **Mod Local**.

9. În secțiunea **Sursă actualizare**, faceți clic pe butonul **Adăugare**.

10. În câmpul **Sursă**, introdu calea către directorul partajat.

    > Adresa sursă trebuie să se potrivească cu adresa specificată anterior de dvs. în câmpul **Cale**, atunci când ați configurat copierea pachetului de actualizare în directorul partajat (consultați *instrucțiunile de mai sus*).

11. Faceți clic pe **OK**.

12. Configurați prioritățile surselor de actualizări folosind butoanele **Sus** și **Jos**.

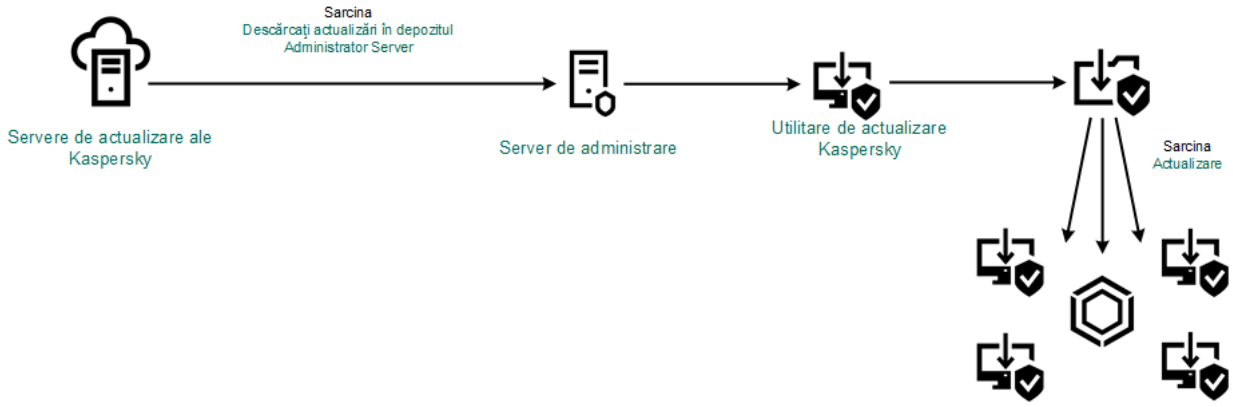
13. Faceți clic pe butonul **Save**.

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.

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.
4. Configurarea actualizărilor pentru bazele de date și modulele aplicației din directorul partajat specificat pe celelalte computere din rețeaua locală a organizației.



Actualizarea folosind Utilitarul 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 Utilitarul de actualizare Kaspersky, *consultați Baza de cunoștințe Kaspersky*.

Pentru a configura actualizările dintr-un director partajat:

1. În fereastra principală a Consolei Web, selectează **Devices** → **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe activitatea **Actualizare** pentru Kaspersky Endpoint Security.

   Se va deschide fereastra de proprietăți a activității.

   Activitatea *Actualizare* este creată automat de Expertul de configurare inițială al Kaspersky Security Center. Pentru a crea activitatea *Actualizare*, instalați plug-inul web Kaspersky Endpoint Security for Windows în timp ce executați Expertul.

3. Selectați fila **Setări aplicație** → **Mod local**.
4. În lista de surse de actualizări, faceți clic pe butonul **Adăugare**.
5. În câmpul **Sursa**, introduceți calea UNC în directorul partajat (de exemplu, `\\Server\Partajare\Actualizare distribuție`).

   Adresa sursă trebuie să se potrivească cu adresa indicată în setările Utilitarului de actualizare Kaspersky.

6. Faceți clic pe **OK**.
7. Configurați prioritățile surselor de actualizări folosind butoanele **Sus** și **Jos**.
8. Faceți clic pe butonul **Save**.

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.

Pentru a configura actualizarea setărilor pentru modul Mobil:

1. În fereastra principală a Consolei Web, selectează **Devices** → **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe activitatea **Actualizare** pentru Kaspersky Endpoint Security.

   Se va deschide fereastra de proprietăți a activității.

   Activitatea *Actualizare* este creată automat de Expertul de configurare inițială al Kaspersky Security Center. Pentru a crea activitatea *Actualizare*, instalați plug-inul web Kaspersky Endpoint Security for Windows în timp ce executați Expertul.

   Selectați fila **Setări aplicație** → **Mod mobil**.

3. Configurarea surselor de actualizări. Sursele de actualizări pot fi servere de actualizare Kaspersky, alte servere FTP și HTTP, directoare locale sau directoare de rețea.

4. Faceți clic pe butonul **Save**.

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, faceți clic pe butonul **Actualizare bază de date**.

2. În blocul **Actualizare a modulelor de baze de date și de aplicații**, faceți clic pe butonul **Actualizare** 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 face clic pe butonul ◻ pentru a opri această activitate în orice moment.

Pentru a începe sau a opri activitatea de actualizare atunci când este afișată interfața de aplicație 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 Kaspersky Endpoint Security, 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:

1. În fereastra principală a aplicației, faceți clic pe butonul **Actualizare bază de date**.
2. Selectați activitatea *Actualizare* și faceți clic pe linkul **Mod executare: <mod>**.
   Se deschid proprietățile activității *Actualizare*.
3. Faceți clic pe butonul **Setări cont utilizator**.
4. În fereastra deschisă, selectați opțiunea **Executare actualizări bază de date cu drepturi de 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 **După planificare** 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:

1. În fereastra principală a aplicației, faceți clic pe butonul **Actualizare bază de date**.

2. Selectați activitatea *Actualizare* și faceți clic pe linkul **Mod executare: <mod>**.

   Se deschid proprietățile activității *Actualizare*.

3. Faceți clic pe butonul **Configurează modul de actualizare a bazei de date**.

4. În fereastra deschisă, 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 de pornire a activității de actualizare, selectați <**După planificare**>. Configurați setările avansate pentru a începe activitatea de actualizare:

     - În câmpul **Amânare executare după pornirea aplicației timp de**, specifică intervalul de timp cu care să fie amânată pornirea activității de actualizare după pornirea aplicației Kaspersky Endpoint Security.

     - Dacă dorești ca aplicația Kaspersky Endpoint Security să execute cât mai curând posibil activitățile de actualizare omise, bifați caseta de selectare **Executare activități omise**.

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.

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.

Pentru a adăuga o sursă de actualizare:

1. În fereastra principală a aplicației, faceți clic pe butonul **Actualizare bază de date**.

2. Selectați activitatea *Actualizare* și faceți clic pe linkul **Mod executare: <mod>**.

   Se deschid proprietățile activității *Actualizare*.

3. Faceți clic pe butonul **Selectare sursă actualizare**.

4. În fereastră, faceți clic pe butonul **Adăugare**.

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://<nume utilizator>:<parolă>@<nod>:<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\AVP11\Update distribution\`.

6. Faceți clic pe butonul **Selectare**.

7. Configurați prioritățile surselor de actualizări folosind butoanele **Sus** și **Jos**.

8. Salvați-vă modificările.

Configurarea actualizărilor 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.

Configurarea actualizărilor pentru bazele de date și modulele aplicației dintr-un director partajat constă din următorii pași:

1. Permiterea copierii unui pachet de actualizare într-un director partajat de pe unul dintre computerele din rețeaua locală.

2. Configurarea actualizărilor pentru bazele de date și modulele aplicației din directorul partajat specificat pe celelalte computere din rețeaua locală a organizației.

Pentru a permite copierea pachetului de actualizare în directorul partajat:

1. În fereastra principală a aplicației, faceți clic pe butonul **Actualizare bază de date**.

2. Selectați activitatea *Actualizare* și faceți clic pe linkul **Mod executare: <mod>**.

   Se deschid proprietățile activității *Actualizare*.

3. În blocul **Se distribuie actualizările**, bifați caseta de selectare **Copiere actualizări în folder**.

4. Introduceți calea UNC în dosarul partajat (de exemplu, `\\Server\Partajare\Actualizare distribuție`).
5. Salvați-vă modificările.

Pentru a configura actualizările dintr-un director partajat:

1. În fereastra principală a aplicației, faceți clic pe butonul **Actualizare bază de date**.
2. Selectați activitatea *Actualizare* și faceți clic pe linkul **Mod executare: <mod>**.
   Se deschid proprietățile activității *Actualizare*.
3. Faceți clic pe butonul **Selectare sursă actualizare**.
4. În fereastră, faceți clic pe butonul **Adăugare**.
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. Faceți clic pe butonul **Selectare**.
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. Când o actualizare devine disponibilă, aplicația va afișa una dintre următoarele notificări în fereastra principală a Kaspersky Endpoint Security: actualizare importantă () sau actualizare critică (). 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. Pentru detalii despre urmărirea actualizărilor modulelor aplicației și confirmarea unei actualizări în Kaspersky Security Center, *consultați Centrul de ajutor Kaspersky Security Center*.

După instalarea unei actualizări a aplicației, este posibil să vi se solicite să reporniți computerul.

Pentru a configura actualizările pentru modulele aplicației:

1. În fereastra principală a aplicației, faceți clic pe butonul **Actualizare bază de date**.
2. Selectați activitatea *Actualizare* și faceți clic pe linkul **Mod executare: <mod>**.
   Se deschid proprietățile activității *Actualizare*.
3. În blocul **Descărcarea și instalarea actualizărilor modulelor aplicației**, bifați caseta de selectare **Descărcare actualizări ale modulelor aplicației**.

4. Selectați actualizările modulelor aplicației pe care doriți să le instalați.

   - **Instalare actualizări 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.

   - **Instalare numai actualizări 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 Consolei Web, faceți clic pe ⚙.

   Se deschide fereastra de proprietăți a Serverului de administrare.

2. Accesează secțiunea **Setări acces la Internet**.

3. Bifați caseta de selectare **Utilizare server proxy**.

4. Configurați setările pentru conexiunea la serverul proxy: adresa serverului proxy, portul și setările de autentificare (numele de utilizator și parola).

5. Faceți clic pe butonul **Save**.

Pentru a dezactiva utilizarea unui server proxy pentru un anumit grup de administrare:

1. În fereastra principală a Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security pentru computerele pe care dorești să dezactivezi utilizarea unui server proxy.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Setări aplicație**.

4. Accesează secțiunea **Setări generale** → **Setări rețea**.

5. În secțiunea **Setări server proxy**, selectați **Nu se utilizează server proxy**.

6. Faceți clic pe **OK**.

7. Confirmă modificările făcând clic pe **Salvare**.

Pentru a configura setările serverului proxy în interfața aplicației:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Setări de rețea**.
3. În blocul **Server proxy**, faceți clic pe linkul **Setări server proxy**.
4. În fereastra deschisă, selectați una dintre opțiunile următoare pentru a stabili adresa serverului proxy:
   - **Detectare automată setări server proxy**.

     Această opțiune este selectată în mod implicit. Kaspersky Endpoint Security utilizează setările serverului proxy definite în setările sistemului de operare.
   - **Utilizare setări server proxy specificate**.

     Dacă ați selectat această opțiune, configurați setările pentru conectarea la serverul proxy: adresa și portul serverului proxy.
5. Dacă doriți să activați autentificarea pe serverul proxy, bifați caseta de selectare **Utilizare autentificare server proxy** și introduceți acreditările contului dvs. de utilizator.
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 **Se 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, atunci când versiunea nouă a bazei de date conține o semnătură nevalidă care determină aplicația Kaspersky Endpoint Security să blocheze o aplicație sigură.

Pentru a derula înapoi cea mai recentă actualizare:

1. În fereastra principală a aplicației, faceți clic pe butonul **Actualizare bază de date**.
2. În blocul **Derularea înapoi a bazelor de date la versiunea anterioară**, faceți clic pe butonul **Derulare 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 face clic pe butonul ◻ pentru a opri această activitate în orice moment.

Pentru a începe sau a opri o activitate de restaurare atunci când este afișată interfața de aplicație 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 restaurare care nu se execută pentru a o porni.
   - Selectați o activitate de restaurare care se execută pentru a o opri.
   - Selectați o activitate de restaurare pusă în pauză pentru a o relua sau a o reporni.

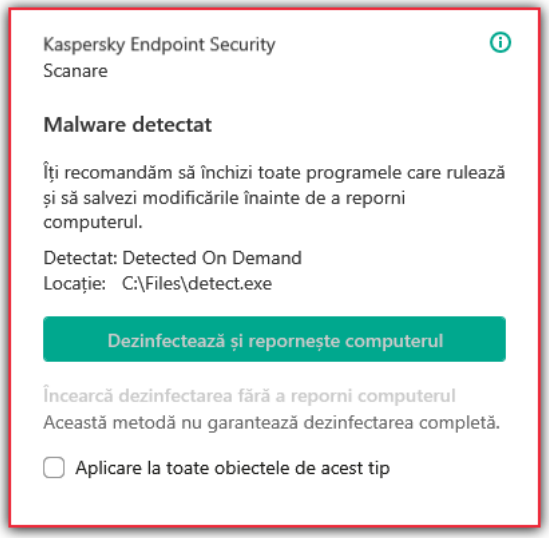
Cum se lucrează cu amenințările active

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. 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. Puteți configura tehnologia Dezinfectare avansată în setările activității *Scanare de viruși* și în setările aplicației.

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 de viruși*. Există o casetă de selectare în proprietățile activității, denumită **Activare Dezinfectare avansată imediată**. 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 de viruși*.

Dacă Kaspersky Endpoint Security este instalat pe un computer care rulează Windows Server, Kaspersky Endpoint Security nu va afișa notificarea. Prin urmare, utilizatorul nu poate selecta o activitate pentru a îndepărta o amenințare activă. Pentru a îndepărta o amenințare, este necesar să activați tehnologia Dezinfectare avansată în setările aplicației și să activați Dezinfectarea avansată imediată în proprietățile *activității Scanare de viruși*. Apoi, este necesar să porniți activitatea *Scanare de viruși*.

Procesarea amenințărilor active

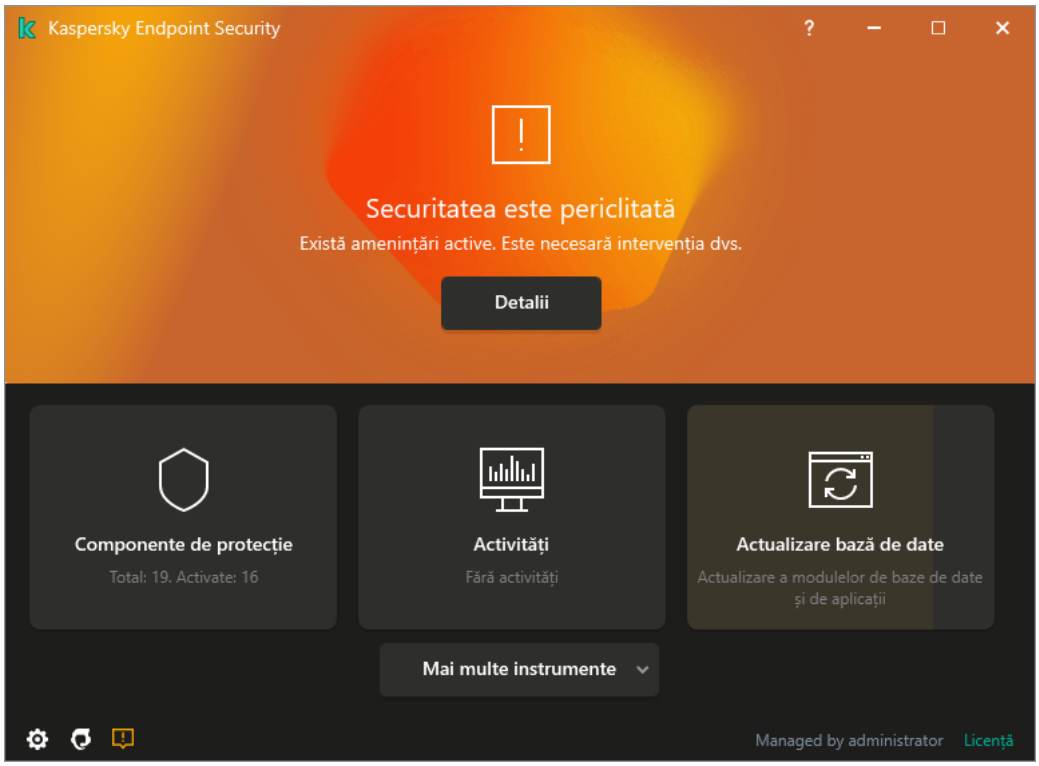
Un fișier infectat este considerat *procesat*, dacă Kaspersky Endpoint Security execută una dintre următoarele acțiuni asupra acestui fișier, în conformitate cu setările de aplicație specificate în cursul scanării computerului după viruși și alte amenințări:

- Dezinfectare.
- Eliminare.
- Ștergere dacă dezinfectarea nu reușește.

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).
- Acțiunea selectată în secțiunea **Acțiune la detectarea amenințării** pentru activitățile de scanare este **Informare**, iar utilizatorul selectați acțiunea **Omitere** atunci când este afișată o notificare despre fișierul infectat.



Fereastra principală a aplicației când este detectată o amenințare

Pentru a procesa amenințările active:

1. În fereastra principală a aplicației, faceți clic pe butonul **Detalii**.

   Se deschide lista amenințărilor active.

2. Selectați obiectul pe care doriți să îl procesați.

3. Alegeți cum doriți să gestionați amenințarea:

   - **Rezolvare**. Dacă selectați această opțiune, Kaspersky Endpoint Security încearcă automat să dezinfecteze toate fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, Kaspersky Endpoint Security șterge fișierele.

   - **Ignorare**. 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 selectați această opțiune, Kaspersky Endpoint Security deschide site-ul web al Enciclopediei de viruși a Kaspersky.

File Threat Protection

Componenta File Threat Protection îți permite să împiedici infectarea sistemului de fișiere al computerului. În mod implicit, componenta File Threat Protection de își are originea permanentă în memoria RAM a computerului. Componenta scanează fișierele de pe toate unitățile computerului, precum și 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 utilizator sau 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 încercați să accesați un fișier al cărui conținut este stocat în stocarea 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 salvate 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.

Pentru a activa sau a dezactiva componenta File Threat Protection:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **File Threat Protection**.
3. Utilizați comutatorul **File Threat Protection** pentru a activa sau dezactiva componenta.
4. Dacă ați activat componenta, efectuați una dintre următoarele acțiuni în secțiunea **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. Valorile setărilor pentru nivelul de securitate recomandat sunt furnizate în tabelul de mai jos.

- **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 avansate** și definiți propriile setări pentru componentă.

  Puteți restabili valorile nivelurilor de securitate presetate făcând clic pe butonul **Restaurare nivel recomandat de securitate** din partea superioară a ferestrei.

5. 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, Kaspersky Endpoint Security 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.
Scanare numai fișiere noi și modificate	**Activat**	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.
Tehnologie iSwift	**Activat**	Această tehnologie permite creșterea vitezei de scanare excluzând de la scanare anumite fișiere. Fișierele sunt excluse de la scanare 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.
Tehnologie iChecker	**Activat**	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).
Scanare fișiere în	**Activat**	Scanează fișierele Microsoft Office (DOC, DOCX, XLS, PPT și alte extensii Microsoft). Fișierele în format Office includ și obiecte OLE.

formate Microsoft Office		
Mod 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	**Dezinfectare, dacă nu este posibil – ștergere**	Dacă selectați această opțiune, Kaspersky Endpoint Security încearcă automat să dezinfecteze toate fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, Kaspersky Endpoint Security șterge fișierele.

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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **File Threat Protection**.
3. Faceți clic pe butonul **Setări avansate**.
4. În blocul **Punere în pauză File Threat Protection**, faceți clic pe linkul **Punere în pauză File Threat Protection**.
5. În fereastra deschisă, configurați setările pentru întreruperea 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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **File Threat Protection**.
3. În secțiunea **Acțiune la detectarea amenințării**, selectați opțiunea necesară:
   - **Dezinfectare; șterge dacă dezinfectarea nu reușește**. Dacă selectați această opțiune, Kaspersky Endpoint Security încearcă automat să dezinfecteze toate fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, Kaspersky Endpoint Security șterge fișierele.
   - **Dezinfectare. Blochează dacă dezinfectarea nu reușește**. Dacă selectați această opțiune, Kaspersky Endpoint Security încearcă automat să dezinfecteze toate fișierele infectate care sunt detectate. Dacă nu este posibilă dezinfectarea, Kaspersky Endpoint Security adaugă informațiile despre fișierele infectate detectate în lista de amenințări active.
   - **Blocare**. Dacă selectezi această opțiune, componenta File Threat Protection blochează automat toate fișierele infectate, fără a încerca să le dezinfecteze.

   Înainte de a încerca să dezinfectați sau să ștergeți un fișier infectat, Kaspersky Endpoint Security 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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **File Threat Protection**.
3. Faceți clic pe butonul **Setări avansate**.
4. În secțiunea **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, Kaspersky Endpoint Security 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, Kaspersky Endpoint Security scanează numai fișierele infectabile. Formatul fișierului se determină în funcție de extensia sa.
5. Faceți clic pe linkul **Editare domeniu de protecție**.
6. În fereastra deschisă, selectați obiectele pe care doriți să le adăugați la domeniul de protecție sau să le excludeți 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. Faceți clic pe butonul **Adăugare**.
      Se deschide arborele de directoare.
   b. Selectați obiectul și apăsați pe **Selectare**.

   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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul .
2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **File Threat Protection**.
3. Faceți clic pe butonul **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 cursorul pentru a seta nivelul analizei euristice: **Scanare rapidă**, **Scanare normală** sau **Scanare riguroasă**.
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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul .
2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **File Threat Protection**.
3. Faceți clic pe butonul **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:
   - **Tehnologie iSwift**. Această tehnologie permite creșterea vitezei de scanare excluzând de la scanare anumite fișiere. Fișierele sunt excluse de la scanare 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.
   - **Tehnologie 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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **File Threat Protection**.
3. Faceți clic pe butonul **Setări avansate**.
4. În secțiunea **Optimizare scanare**, bifați caseta de selectare **Scanare numai fișiere 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 RAR, ARJ, ZIP, CAB și LHA și șterge fișiere în toate celelalte formate (exceptând bazele de date de e-mail).

Pentru a configura scanarea fișierelor compuse:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **File Threat Protection**.
3. Faceți clic pe butonul **Setări avansate**.
4. În secțiunea **Scanare fișiere compuse**, specifică tipurile de fișiere compuse pe care dorești să le scanezi: arhive, pachete de instalare sau fișiere în formate 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 fișiere 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 fișiere compuse mari**.

- **Dezarhivare fișiere 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 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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **File Threat Protection**.
3. Faceți clic pe butonul **Setări avansate**.
4. În secțiunea **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.

Web Threat Protection

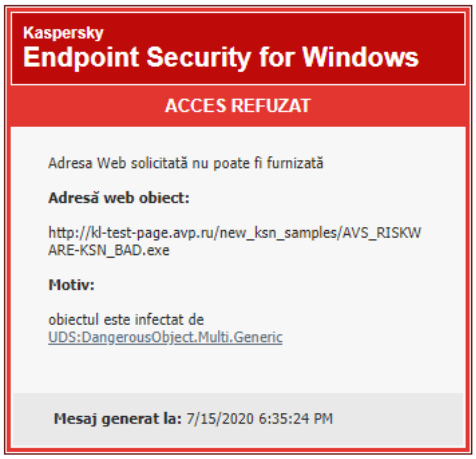
Această componentă este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Windows pentru stații de lucru. Această componentă nu este disponibilă dacă aplicația Kaspersky Endpoint Security este instalată pe un computer pe care se execută Windows pentru servere.

Componenta Web Threat Protection previne descărcarea de pe Internet a fișierelor dăunătoare și, de asemenea, blochează site-urile web dăunătoare 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. Puteți specifica porturile pe care Kaspersky Endpoint Security le va monitoriza sau puteți selecta toate porturile.

Pentru monitorizarea traficului HTTPS, trebuie să activați scanarea conexiunilor securizate.

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 (vedeți figura de mai jos).



Mesaj privind respingerea accesului la site-ul web

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, Kaspersky Endpoint Security poate aplica diferite grupuri de setări. Aceste grupuri de setări salvate 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.

Pentru a activa sau a dezactiva componenta Web Threat Protection:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Protecție** → **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 secțiunea **Nivel de securitate**:

   - Dacă doriți să aplicați unul dintre nivelurile de securitate presetate, selectați-l folosind glisorul:

     - **Ridicat**. Nivelul de securitate în care componenta Web Threat Protection efectuează un control maxim asupra scanării traficului Web primit de computer 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 Kaspersky Endpoint Security și securitatea traficului Web. Componenta Web Threat Protection efectuează analiza euristică la nivelul **Scanare normală**. 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 avansate** și definiți propriile setări pentru componentă.

     Puteți restabili valorile nivelurilor de securitate presetate făcând clic pe butonul **Restaurare nivel recomandat de securitate** din partea superioară a ferestrei.

5. Salvați-vă modificările.

Setări Web Threat Protection recomandate de experții Kaspersky (nivel de securitate recomandat)

Parametru	Valoare	Descriere
Verifică dacă linkurile sunt listate în baza de date de linkuri periculoase	**Activat**	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 URL în baza de date cu adrese URL de phishing	**Activat**	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.
Utilizare analiză 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.
Utilizare analiză euristică (Anti-Phishing)	**Activat**	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	**Blocare descărcare**	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.

Schimbarea acțiunii de efectuat asupra obiectelor de trafic Web rău intenționate

În mod implicit, la detectarea unui obiect infectat în traficul Web, componenta Web Threat Protection blochează accesul la obiectul respectiv și afișează o notificare despre acțiune.

Pentru a schimba acțiunea de efectuat asupra obiectelor de trafic Web rău intenționate:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **Web Threat Protection**.
3. În secțiunea **Acțiune la detectarea amenințării**, selectați acțiunea pe care aplicația Kaspersky Endpoint Security să o efectueze asupra obiectelor de trafic Web rău intenționate:
   - **Blochează descărcarea**. 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.
   - **Informare**. 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.
4. Salvați-vă modificările.

Scanarea adreselor URL în bazele de date de phishing și adrese URL rău intenționate

Scanarea linkurilor pentru a vedea dacă acestea sunt incluse în lista de adrese Web de phishing permite evitarea *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 mesajele ICQ, 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. Listele de adrese URL de phishing sunt incluse în kitul de distribuire Kaspersky Endpoint Security.

Pentru a configura componenta Web Threat Protection să verifice linkurile în bazele de date cu adrese Web de phishing și periculoase:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **Web Threat Protection**.
3. Faceți clic pe butonul **Setări avansate**.
4. Efectuează următoarele acțiuni:
   - Dacă dorești ca componenta Web Threat Protection să verifice linkurile în bazele de date cu adrese Web periculoase, în secțiunea **Metode de scanare**, bifați caseta de selectare **Verifică adresa URL în baza de date cu adrese URL 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 scanează toate linkurile pentru a determina dacă acestea sunt listate în baze de date de adrese URL dăunătoare. Setările de scanare a conexiunii securizate ale aplicației nu afectează funcționalitatea de scanare a linkurilor. Cu alte cuvinte, dacă scanările de conexiune criptate sunt dezactivate, Kaspersky Endpoint Security verifică legăturile cu bazele de date de adrese URL dăunătoare, chiar dacă traficul de rețea este transmis printr-o conexiune criptată.

   - Dacă doriți ca componenta Web Threat Protection să verifice linkurile în bazele de date cu adrese URL de phishing, bifați caseta de selectare **Verifică adresa URL în baza de date cu adrese URL de phishing** din 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.

     De asemenea, poți să verifici linkurile în bazele de date de reputație din Kaspersky Security Network.

5. Salvați-vă modificările.

Folosirea analizei euristice în funcționarea componentei Web Threat Protection

Pentru a spori eficiența protecției, poți utiliza analiza 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.

Pentru a configura utilizarea analizei euristice:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **Web Threat Protection**.
3. Faceți clic pe butonul **Setări avansate**.
4. În blocul **Metode de scanare**, bifați caseta de selectare **Utilizare analiză euristică** dacă doriți ca aplicația să utilizeze analize euristice atunci când scanează traficul web pentru viruși și alte programe malware. Apoi utilizați cursorul pentru a seta nivelul analizei euristice: **Scanare rapidă**, **Scanare normală** sau **Scanare riguroasă**.
5. În blocul **Anti-Phishing**, bifați caseta de selectare **Utilizare analiză euristică** dacă doriți ca aplicația să utilizeze analize euristice atunci când scanează pagini web pentru linkuri de phishing.
6. Salvați-vă modificările.

Crearea listei de adrese web de încredere

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.

Pentru a crea o listă de adrese URL de încredere:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **Web Threat Protection**.
3. Faceți clic pe butonul **Setări avansate**.
4. Bifați caseta de selectare **Nu se scanează traficul Web de la adresele URL de încredere**.

   Dacă această casetă de selectare este bifată, 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.
6. Salvați-vă modificările.

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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **Web Threat Protection**.
6. Fă clic pe butonul **Setări**.
7. În fereastra deschisă, selectați fila **Adrese URL de încredere**.
8. 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 **Exportare**.
   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. Faceți clic pe butonul **Save**.
      Kaspersky Endpoint Security exportă întreaga listă de adrese URL de încredere în fișierul XML.
9. Pentru a importa lista de adrese de încredere:
   a. Faceți clic pe linkul **Importare**.
      În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de adrese de încredere.
   b. Faceți clic pe butonul **Deschidere**.
      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.
10. 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 Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security pentru computerele pe care doriți să exportați sau să importați o listă de adrese URL de încredere.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Selectați **Essential Threat Protection** → **Web Threat Protection**.
5. Pentru a exporta lista excluderilor din blocul **Adrese URL de încredere**:
   a. Selectați adresele URL de încredere pe care doriți să le exportați.
   b. Faceți clic pe linkul **Exportare**.
   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. Faceți clic pe butonul **Save**.

      Kaspersky Endpoint Security exportă întreaga listă de adrese URL de încredere în fișierul XML.
6. Pentru a importa o listă de excluderi în blocul **Adrese URL de încredere**:
   a. Faceți clic pe linkul **Importare**.

      În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de adrese de încredere.
   b. Faceți clic pe butonul **Deschidere**.

      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.
7. Salvați-vă modificările.

Mail Threat Protection

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 Mail Threat Protection scanează atașările mesajelor de e-mail primite și trimise în vederea detectării virușilor și a altor amenințări. Componenta scanează, de asemenea, mesajele pentru detectarea link-urilor periculoase și de phishing. În mod implicit, componenta Mail Threat Protection își are originea permanent în memoria RAM a computerului și scanează toate mesajele primite sau trimise utilizând protocoalele POP3, SMTP, IMAP sau NNTP sau clientul de mail Microsoft Office Outlook (MAPI). Componenta oferă protecție computerului cu ajutorul bazelor de date antivirus, a [serviciului cloud Kaspersky Security Network] și a analizei euristice.

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 redenumește subiectul mesajului după cum urmează: `[Mesajul este infectat] <subiect mesaj>` sau `[Obiectul infectat a fost șters] <subiect mesaj>`.

Această componentă interacționează cu clienții de e-mail instalați pe computer. Pentru clientul de mail Microsoft Office Outlook, este furnizată o extensie cu parametri suplimentari. Extensia Mail Threat Protection este încorporată în clientul de e-mail Microsoft Office Outlook în cursul instalării aplicației Kaspersky Endpoint Security.

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, Kaspersky Endpoint Security poate aplica diferite grupuri de setări. Aceste grupuri de setări salvate 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.

Pentru a activa sau a dezactiva componenta Mail Threat Protection:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **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 secțiunea **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 Kaspersky Endpoint Security 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 de securitate pentru e-mail **Redus** 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 avansate** și definiți propriile setări pentru componentă.

  Puteți restabili valorile nivelurilor de securitate presetate făcând clic pe butonul **Restaurare nivel recomandat de securitate** din partea superioară a ferestrei.

5. Salvați-vă modificările.

Setări Mail Threat Protection recomandate de experții Kaspersky (nivel de securitate recomandat)

Parametru	Valoare	Descriere
Domeniu de protecție	**Mesaje 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.
Conectare extensie Microsoft Outlook	**Activat**	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 Exchange în cache. Pentru informații mai detaliate despre modul Cached Exchange și recomandări privind utilizarea sa, consultați Baza de cunoștințe Microsoft.
Scanare arhive atașate	**Activat**	Scanează arhivele în următoarele formate: RAR, ARJ, ZIP, CAB, LHA, JAR, și ICE.
Scanare formate Office atașate	**Activat**	Scanează fișierele Microsoft Office (DOC, DOCX, XLS, PPT și alte extensii Microsoft). Fișierele în format Office includ și obiecte OLE.
Filtrare atașare	**Redenumire atașări 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	**Dezinfectare, dacă nu este posibil – ștergere**	Când un obiect infectat este detectat într-un mesaj de intrare sau de ieșire, Kaspersky Endpoint Security încearcă să dezinfecteze obiectul detectat. Utilizatorul va putea accesa mesajul cu o atașare sigură. Dacă obiectul nu poate fi dezinfectat, Kaspersky Endpoint Security șterge

		obiectul infectat. Kaspersky Endpoint Security adaugă informații despre acțiunea efectuată la subiectul mesajului: `[Obiectul infectat a fost șters] <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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **Mail Threat Protection**.
3. În secțiunea **Acțiune la detectarea amenințării**, selectați acțiunea pe care aplicația Kaspersky Endpoint Security să o efectueze atunci când este detectat un mesaj infectat:
   - **Dezinfectare; șterge dacă dezinfectarea nu reușește**. Când un obiect infectat este detectat într-un mesaj de intrare sau de ieșire, Kaspersky Endpoint Security încearcă să dezinfecteze obiectul detectat. Utilizatorul va putea accesa mesajul cu o atașare sigură. Dacă obiectul nu poate fi dezinfectat, Kaspersky Endpoint Security șterge obiectul infectat. Kaspersky Endpoint Security adaugă informații despre acțiunea efectuată la subiectul mesajului: `[Obiectul infectat a fost șters] <subiect mesaj>`.
   - **Dezinfectare. Blochează dacă dezinfectarea nu reușește**. Când un obiect infectat este detectat într-un mesaj de intrare, Kaspersky Endpoint Security încearcă să dezinfecteze obiectul detectat. Utilizatorul va putea accesa mesajul cu o atașare sigură. Dacă obiectul nu poate fi dezinfectat, Kaspersky Endpoint Security adaugă un avertisment la subiectul mesajului: `[Mesaj infectat] <subiect mesaj>`. Utilizatorul va putea accesa mesajul cu atașarea originală. Când un obiect infectat este detectat într-un mesaj de ieșire, Kaspersky Endpoint Security încearcă să dezinfecteze obiectul detectat. Dacă obiectul nu poate fi dezinfectat, Kaspersky Endpoint Security blochează transmiterea mesajului, iar clientul de e-mail afișează o eroare.
   - **Blocare**. Dacă un obiect infectat este detectat într-un mesaj de intrare, Kaspersky Endpoint Security adaugă un avertisment la subiectul mesajului: `[Mesaj infectat] <subiect mesaj>`. Utilizatorul va putea accesa mesajul cu atașarea originală. Dacă un obiect infectat este detectat într-un mesaj de ieșire, Kaspersky Endpoint Security 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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **Mail Threat Protection**.
3. Faceți clic pe butonul **Setări avansate**.
4. În blocul **Domeniu de protecție**, selectați mesajele de scanat:
   - **Mesaje primite și trimise**.
   - **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.

   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 secțiunea **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 **Scanare trafic POP3 / SMTP / NNTP / 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 **Scanare trafic POP3 / SMTP / NNTP / 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 **Conectare extensie Microsoft Outlook**.

     Dacă utilizați un alt client de e-mail decât Microsoft Office Outlook, mesajele de e-mail transmise prin protocoalele POP3, SMTP, NNTP și IMAP nu sunt scanate de către componenta Mail Threat Protection atunci când caseta de selectare **Scanare trafic POP3 / SMTP / NNTP / IMAP** nu este bifată.

   - 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 **Conectare extensie 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 **Conectare extensie 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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **Mail Threat Protection**.
3. Faceți clic pe butonul **Setări avansate**.
4. În secțiunea **Scanare fișiere compuse**, configurați setările de scanare:
   - **Scanare fișiere atașate cu formate Microsoft Office**. Scanează fișierele Microsoft Office (DOC, DOCX, XLS, PPT și alte extensii Microsoft). Fișierele în format Office includ și obiecte OLE.
   - **Scanare arhive atașate**. Scanează arhivele în următoarele formate: RAR, ARJ, ZIP, CAB, LHA, JAR, și ICE.

     Dacă în timpul scanării, Kaspersky Endpoint Security 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. Arhiva 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 arhive 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.
   - **Limitați timpul de scanare a arhivei la N secunde**. 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 la mesaje de e-mail

Funcționalitatea de filtrare a 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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **Mail Threat Protection**.
3. Faceți clic pe butonul **Setări avansate**.
4. În secțiunea **Filtrare atașare**, efectuați una dintre următoarele acțiuni:
   - Dacă nu dorești ca componenta Mail Threat Protection să filtreze atașările mesajelor, selectați opțiunea **Dezactivare filtrare**.
   - Dacă dorești ca componenta Mail Threat Protection să redenumească atașările mesajelor cu tipurile specificate, selectați opțiunea **Redenumire tipuri de atașări selectate**.
   - Dacă dorești ca componenta Mail Threat Protection să șteargă atașările mesajelor cu tipurile de fișiere specificate, selectați opțiunea **Ștergere atașări de tipurile selectate**.
5. Dacă ai selectat opțiunea **Redenumire tipuri de atașări selectate** sau opțiunea **Ștergere tipuri de atașări 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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **Mail Threat Protection**.
6. În secțiunea **Nivel de securitate**, faceți clic pe butonul **Setări**.
7. În fereastra deschisă, selectați fila **Filtrare atașări**.
8. 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 **Exportare**.
   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. Faceți clic pe butonul **Save**.
      Kaspersky Endpoint Security exportă întreaga listă de extensii în fișierul XML.
9. Pentru a importa lista de extensii:
   a. Faceți clic pe linkul **Importare**.
   b. În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de extensii.
   c. Faceți clic pe butonul **Deschidere**.
      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.
10. Salvați-vă modificările.

Cum se exportă și se importă o listă de extensii pentru filtrarea atașamentelor în Consola Web și Cloud Console

1. În fereastra principală a Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security pentru computerele pe care doriți să exportați sau să importați o listă de excluderi.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Selectați **Essential Threat Protection** → **Mail Threat Protection**.
5. Pentru a exporta lista extensiilor din blocul **Filtrare atașări**:
   a. Selectați extensiile pe care doriți să le exportați.
   b. Faceți clic pe linkul **Exportare**.
   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. Faceți clic pe butonul **Save**.

      Kaspersky Endpoint Security exportă întreaga listă de extensii în fișierul XML.
6. Pentru a importa o listă de extensii în blocul **Filtrare atașări**:
   a. Faceți clic pe linkul **Importare**.
   b. În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de extensii.
   c. Faceți clic pe butonul **Deschidere**.

      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.

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). Acesta permite deschiderea setărilor componentei Mail Threat Protection din Outlook și specificarea momentului în care mesajele de e-mail trebuie scanate de viruși și alte amenințări. Extensia Mail Threat Protection pentru Outlook poate scana mesaje primite și trimise transmise prin protocoalele POP3, SMTP, NNTP, IMAP și MAPI. Kaspersky Endpoint Security acceptă, de asemenea, colaborarea cu alți clienți de e-mail (inclusiv Microsoft Outlook Express®, Windows Mail și Mozilla™ Thunderbird™).

Extensia Mail Threat Protection acceptă funcționarea cu Outlook 2010, 2013, 2016 și 2019.

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**.

În Outlook, mesajele primite sunt întâi scanate de componenta Mail Threat Protection (dacă este bifată caseta de selectare Trafic POP3/SMTP/NNTP/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.

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 folosind Kaspersky Security Center:

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **Mail Threat Protection**.
6. În secțiunea **Nivel de securitate**, faceți clic pe butonul **Setări**.

   Se deschide fereastra **Mail Threat Protection**.
7. În secțiunea **Conectivitate**, faceți clic pe butonul **Setări**.
8. În fereastra **Protecție e-mail**:
   - Bifați caseta de selectare **Scanare 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 **Scanare la citire** dacă dorești ca extensia Mail Threat Protection pentru Outlook să scaneze mesajele primite atunci când utilizatorul le deschide.
   - Bifați caseta de selectare **Scanare la trimitere** dacă dorești ca extensia Mail Threat Protection pentru Outlook să scaneze mesajele trimise atunci când acestea sunt expediate.
9. Salvați-vă modificările.

Network Threat Protection

Componenta Network Threat Protection scanează traficul de rețea de la intrare, căutând activitate tipică atacurilor de rețea. Când Kaspersky Endpoint Security detectează o încercare de atac asupra rețelei pe computerul utilizatorului, acesta 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 Kaspersky Endpoint Security. 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. Dacă este necesar, poți dezactiva componenta Network Threat Protection.

Pentru a activa sau a dezactiva componenta Network Threat Protection:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Network Threat Protection**.
3. Utilizați comutatorul **Network Threat Protection** pentru a activa sau a dezactiva componenta.
4. Salvați-vă modificările.

Drept urmare, dacă Network Threat Protection este activat, Kaspersky Endpoint Security scanează traficul de rețea de intrare pentru activități tipice atacurilor de rețea. Când Kaspersky Endpoint Security detectează o încercare de atac asupra rețelei pe computerul utilizatorului, acesta blochează conexiunea la rețea cu respectivul computer atacator.

Blocarea unui computer atacator

Pentru a bloca un computer atacator:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Network Threat Protection**.
3. Bifați caseta de selectare **Adăugare computer agresor la lista de computere blocate pentru N minute**.

   Dacă această casetă de selectare este bifată, componenta Network Threat Protection adaugă computerul agresor 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.

   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.

4. În câmpul de lângă caseta de selectare **Adăugare computer agresor la lista de computere blocate pentru N minute** puteți schimba perioada de timp în decursul căreia computerul agresor să fie blocat.

5. Salvați-vă modificările.

Prin urmare, atunci când Kaspersky Endpoint Security detectează o tentativă de atac de rețea lansată împotriva computerului utilizatorului, aceasta va bloca toate conexiunile cu computerul atacator.

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.

Pentru a configura adresele de excluderi de la blocare:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Protecție** → **Network Threat Protection**.

3. Faceți clic pe linkul **Gestionare excluderi**.

4. În fereastră, faceți clic pe butonul **Adăugare**.

5. Introdu adresa IP a computerului de la care nu trebuie blocate atacurile de rețea.

6. Salvați-vă modificările.

Prin urmare, Kaspersky Endpoint Security nu urmărește activitatea de pe dispozitivele din lista de excluderi.

Exportul și importul listei de dispozitive de încredere

Puteți 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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **Network Threat Protection**.
6. În blocul **Setări Network Threat Protection**, faceți clic pe butonul **Excluderi**.
7. 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. Faceți clic pe linkul **Exportare**.
   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. Faceți clic pe butonul **Save**.
      Kaspersky Endpoint Security exportă întreaga listă de excluderi în fișierul XML.
8. Pentru a importa lista de excluderi:
   a. Faceți clic pe butonul **Import**.
   b. În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de excluderi.
   c. Faceți clic pe butonul **Deschidere**.
      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.
9. Salvați-vă modificările.

[Cum se exportă și se importă o listă de excluderi în Consola Web și Cloud Console]

1. În fereastra principală a Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security pentru computerele pe care doriți să exportați sau să importați o listă de excluderi.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Selectați **Essential Threat Protection** → **Network Threat Protection**.
5. În blocul **Setări Network Threat Protection**, faceți clic pe linkul **Excluderi**.

   Se deschide lista cu excluderi.
6. Pentru a exporta lista de reguli:
   a. Selectați excluderile pe care doriți să le exportați.
   b. Faceți clic pe butonul **Export**.
   c. Confirmați că doriți să exportați numai excluderile selectate sau exportați întreaga listă de excluderi.
   d. 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.
   e. Faceți clic pe butonul **Save**.

      Kaspersky Endpoint Security exportă întreaga listă de excluderi în fișierul XML.
7. Pentru a importa lista de excluderi:
   a. Faceți clic pe butonul **Import**.
   b. În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de excluderi.
   c. Faceți clic pe butonul **Deschidere**.

      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.
8. Salvați-vă modificările.

Configurarea protecției împotriva atacurilor din rețea după 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.

Pentru a configura protecția împotriva atacurilor de rețea după tip:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Network Threat Protection**.
3. Uilizați butonul **Tratează scanarea porturilor și supraîncărcarea rețelei ca atacuri** pentru a activa sau dezactiva aceste atacuri.
4. Utilizați comutatorul **Protecție falsificare MAC**.
5. În blocul **La detectarea unui atac de falsificare MAC**, selectați una dintre următoarele opțiuni:
   - **Numai notificare**.
   - **Notificare și blocare**.
6. Salvați-vă modificările.

Firewall

Firewall blochează conexiunile neautorizate la computer în timp ce lucrați pe Internet sau în rețeaua 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, consultați *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 rețea ale aplicației*. 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 din *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 puteți schimba grupul de încredere numai pentru 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 după cum urmează: o regulă de rețea pentru aplicații include reguli de acces bazate pe starea rețelei: *publică*, *locală* sau *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.

Stările conexiunii de rețea

Firewall-ul vă permite să controlați activitatea rețelei în funcție de starea conexiunii de rețea. Kaspersky Endpoint Security primește starea conexiunii de rețea de la sistemul de operare al computerului. Starea conexiunii de rețea în sistemul de operare este setată de utilizator atunci când configurează conexiunea. Puteți schimba starea conexiunii de rețea în setările Kaspersky Endpoint Security. Firewall-ul va monitoriza activitatea rețelei în funcție de starea rețelei în setările Kaspersky Endpoint Security și nu în sistemul de operare.

Conexiunea de rețea poate avea una dintre următoarele patru tipuri de stare:

- **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 starea *Rețea publică* întregului Internet. Nu poți modifica starea 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.

Pentru a activa sau a dezactiva componenta Firewall:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **Firewall**.
3. Utilizați comutatorul de **Firewall** pentru a activa sau a dezactiva componenta.
4. Salvați-vă modificările.

Modificarea stării conexiunii de rețea

Firewall atribuie în mod implicit starea *Rețea publică* întregului Internet. Nu poți modifica starea pentru Internet.

Pentru a schimba starea unei conexiuni de rețea:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **Firewall**.
3. Faceți clic pe butonul **Rețele disponibile**.
4. Selectați conexiunea de rețea a cărei stare dorești să o modifici.
5. În coloana **Tip de rețea**, selectați starea conexiunii de 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

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.

La crearea de reguli pentru pachete de rețea, reține faptul că acestea au o prioritate mai mare decât regulile de rețea pentru aplicații.

Cum se utilizează instrumentul Monitor rețea pentru a crea o regulă pentru pachetul de rețea în interfața aplicației

1. În fereastra principală a aplicației, faceți clic pe **Mai multe instrumente** → **Monitorizare rețea**.
2. Selectați fila **Activitate rețea**.

   Fila **Activitate rețea** afișează toate conexiunile de rețea active în prezent pe computer. Se afișează atât conexiunile de rețea la ieșire, cât și cele la intrare.
3. În meniul contextual al unei conexiuni la rețea, selectați **Creare regulă pachet**.

   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 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 **Înregistrare evenimente în jurnal**.
8. Faceți clic pe butonul **Save**.

   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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **Firewall**.
3. Faceți clic pe butonul **Reguli pachet**.

   Aceasta deschide o listă de reguli implicite setate de componenta Firewall.
4. Faceți clic pe butonul **Adăugare**.

   Aceasta deschide proprietățile regulii pentru rețea.
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 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 **Înregistrare evenimente în jurnal**.
9. Faceți clic pe butonul **Save**.

   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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **Firewall**.
6. În blocul **Setări Firewall**, faceți clic pe butonul **Setări**.

   Aceasta deschide lista cu regulile pentru pachetele de rețea și lista regulilor de rețea pentru aplicații.
7. Selectați fila **Reguli pentru pachetele de rețea**.

   Aceasta deschide o listă de reguli implicite setate de componenta Firewall.
8. Faceți clic pe butonul **Adăugare**.

   Aceasta deschide proprietățile regulii de pachete.
9. Introdu manual numele serviciului de rețea în câmpul **Nume**.
10. 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.
11. Dacă dorești ca acțiunile regulii de rețea să fie reflectate în raport, bifați caseta de selectare **Înregistrare evenimente în jurnal**.
12. Faceți clic pe butonul **Save**.

    Noua regulă de rețea va fi adăugată în listă.
13. Utilizați butoanele **Sus**/**Jos** pentru a seta prioritatea regulii de rețea.
14. 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 Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Selectați **Essential Threat Protection** → **Firewall**.
5. În blocul **Setări Firewall**, faceți clic pe linkul **Reguli pentru pachetele de rețea**.

   Aceasta deschide o listă de reguli implicite setate de componenta Firewall.
6. Faceți clic pe butonul **Adăugare**.

   Aceasta deschide proprietățile regulii de pachete.
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 linkul **Selectare șablon**. 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 **Înregistrare evenimente în jurnal**.
10. Faceți clic pe butonul **Save**.

    Noua regulă de rețea va fi adăugată în listă.
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. Utilizați comutatorul din coloana **Stare** pentru a activa sau a dezactiva regula pentru pachet.

Setări Reguli pentru pachetele de rețea

Parametru	Descriere
Acțiune	**Permitere**. **Blocare**. **După regulile de aplicații**. Dacă este setată această opțiune, componenta Firewall aplică regulile de rețea pentru aplicații conexiunii la rețea.
Protocol	Controlează activitatea rețelei 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, delimitate prin virgulă, pentru computerul local și computerul la distanță între care urmează să fie monitorizată conexiunea.
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 atât pachetelor de rețea de intrare, cât și celor de ieșire, indiferent dacă computerul utilizatorului sau un computer la distanță a inițiat conexiunea la rețea. **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. Protocolul TCP stabilește o conexiune. Utilizați direcțiile **Intrare**, **Ieșire** și **Intrare/Ieșire** pentru TCP. Toate protocoalele celelalte nu stabilesc conexiuni, dar trimit pachete. Pentru toate protocoalele celelalte utilizează direcțiile **(pachet) Intrare**, **(pachete) Ieșire** sau **Intrare/Ieșire**.
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)	Restricționează controlul pachetelor de rețea pe baza timpului de viață (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 sau puteți selecta o subrețea (Rețele de încredere, Rețele locale, Rețele publice).
Adrese locale	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 locale. Puteți include toate adresele Ip într-o regulă de rețea sau puteți crea o listă separată de adrese IP. 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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **Firewall**.
3. Faceți clic pe butonul **Reguli 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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **Firewall**.

3. Faceți clic pe butonul **Reguli 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 **Editare**.

5. În lista verticală **Acțiune**, selectați acțiunea de efectuat de componenta Firewall la detectarea acestui tip de activitate de rețea:

   - **Permitere**.
   - **Blocare**.
   - **După regulile de aplicații**.

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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **Firewall**.

3. Faceți clic pe butonul **Reguli 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. Utilizează butoanele **Sus** și **Jos** pentru a muta regula pachetului de rețea în poziția dorită din lista de reguli pentru pachete 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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **Firewall**.
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 **Exportare**.
   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. Faceți clic pe butonul **Save**.
      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 **Importare**.
      În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de reguli.
   b. Faceți clic pe butonul **Deschidere**.
      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 Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security pentru computerele pe care doriți să exportați sau să importați lista de reguli.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Selectați **Essential Threat Protection** → **Firewall**.
5. Faceți clic pe linkul **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.
   b. Faceți clic pe butonul **Export**.
   c. Confirmați că doriți să exportați numai regulile selectate sau să exportați întreaga listă.
   d. Faceți clic pe butonul **Export**.

      Kaspersky Endpoint Security exportă lista de reguli într-un fișier XML în directorul de descărcări implicit.
7. Pentru a importa o listă de reguli de pachete de rețea:
   a. Faceți clic pe linkul **Importare**.

      În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de reguli.
   b. Faceți clic pe butonul **Deschidere**.

      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.

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, faceți clic pe **Mai multe instrumente** → **Monitorizare rețea**.
2. Selectați fila **Activitate rețea** sau **Porturi deschise**.

   Fila **Activitate rețea** afișează toate conexiunile de rețea active în prezent pe computer. Se afișează atât conexiunile de 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 **Creare regulă de aplicație**.

   Se deschide fereastra de reguli și proprietăți a aplicației.
4. Selectați fila **Reguli rețea**.

   Aceasta deschide o listă de reguli implicite setate de componenta Firewall.
5. Faceți clic pe butonul **Adăugare**.

   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 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 **Înregistrare evenimente în jurnal**.
9. Faceți clic pe butonul **Save**.

   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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **Firewall**.
3. Faceți clic pe butonul **Reguli de 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 rețea**.
7. Faceți clic pe butonul **Adăugare**.

   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 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 **Înregistrare evenimente în jurnal**.
11. Faceți clic pe butonul **Save**.

    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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra cu setările aplicației, selectați **Essential Threat Protection** → **Firewall**.
6. În blocul **Setări Firewall**, faceți clic pe butonul **Setări**.

   Aceasta deschide lista cu regulile pentru pachetele de rețea și lista regulilor de rețea pentru aplicații.
7. Selectați fila **Reguli de rețea pentru aplicații**.
8. Faceți clic pe butonul **Adăugare**.
9. În fereastra deschisă, selectați 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.
10. Faceți clic pe butonul **Împrospătare**.

    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.
11. Selectați aplicația necesară.
12. În lista verticală **Adaugă aplicațiile selectate la grupul <grup de încredere>**, selectați **Grupuri implicite** și faceți clic pe **OK**.

    Aplicația va fi adăugată la grupul implicit.
13. Selectați aplicația relevantă și apoi selectați **Drepturi aplicație** din meniul contextual al aplicației.

    Se deschide fereastra de reguli și proprietăți a aplicației.
14. Selectați fila **Reguli rețea**.

    Aceasta deschide o listă de reguli implicite setate de componenta Firewall.
15. Faceți clic pe butonul **Adăugare**.

    Aceasta deschide proprietățile regulii pentru rețea.
16. Introdu manual numele serviciului de rețea în câmpul **Nume**.
17. 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.
18. Dacă dorești ca acțiunile regulii de rețea să fie reflectate în raport, bifați caseta de selectare **Înregistrare evenimente în jurnal**.

19. Faceți clic pe butonul **Save**.

    Noua regulă de rețea va fi adăugată în listă.

20. Utilizați butoanele **Sus**/**Jos** pentru a seta prioritatea regulii de rețea.

21. Salvați-vă modificările.

[Cum se creează o regulă de rețea pentru aplicații în Web Console și Cloud Console]

1. În fereastra principală a Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Selectați **Essential Threat Protection** → **Firewall**.
5. În blocul **Setări Firewall**, faceți clic pe linkul **Reguli de rețea pentru aplicații**.

   Tastfel se deschide fereastra de configurare a drepturilor aplicațiilor și lista resurselor protejate.
6. Selectați fila **Drepturi aplicații**.

   Veți vedea o listă cu grupurile de încredere în partea stângă a ferestrei, iar proprietățile acestora în partea dreaptă.
7. Faceți clic pe butonul **Adăugare**.

   Aceasta pornește Expertul pentru adăugarea unei aplicații la un grup de încredere.
8. Faceți clic pe linkul **Grup țintă selectat** pentru a selecta grupul de încredere relevant pentru aplicație.
9. Selectați **Tip aplicație**. Faceți clic pe butonul **Next**.

   Dacă doriți să creați o regulă de rețea pentru mai multe aplicații, selectați tipul pentru **Grup** 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. Finalizați Expertul, făcând clic pe **OK**.

    Aplicația va fi adăugată în grupul de încredere.
12. În partea stângă a ferestrei, selectați aplicația relevantă.
13. În partea dreaptă a ferestrei, selectați **Reguli rețea** din lista verticală.

    Aceasta deschide o listă de reguli implicite setate de componenta Firewall.
14. Faceți clic pe butonul **Adăugare**.

    Aceasta deschide proprietățile regulii pentru aplicație.
15. Introdu manual numele serviciului de rețea în câmpul **Nume**.
16. Configurați setările regulii de rețea (consultați tabelul de mai jos).

    Puteți selecta un șablon de regulă predefinit făcând clic pe linkul **Selectare șablon**. 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 **Înregistrare evenimente în jurnal**.
18. Faceți clic pe butonul **Save**.

Noua regulă de rețea va fi adăugată în listă.

19. Utilizați butoanele **Sus**/**Jos** pentru a seta prioritatea regulii de rețea.

20. Salvați-vă modificările.

Setări Regulă de rețea pentru aplicație

Parametru	Descriere
Acțiune	**Permitere**. **Blocare**.
Protocol	Controlează activitatea rețelei 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, delimitate prin virgulă, pentru computerul local și computerul la distanță între care urmează să fie monitorizată conexiunea.
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 sau puteți selecta o subrețea (Rețele de încredere, Rețele locale, Rețele publice).
Adrese locale	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 locale. Puteți include toate adresele Ip într-o regulă de rețea sau puteți crea o listă separată de adrese IP. 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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **Firewall**.

3. Faceți clic pe butonul **Reguli de 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 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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **Firewall**.

3. Faceți clic pe butonul **Reguli de 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 rețea**, apoi selectați acțiunea pe care doriți să o atribuiți:

   - **Moștenire**.
   - **Permitere**.
   - **Blocare**.

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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **Firewall**.

3. Faceți clic pe butonul **Reguli de 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 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:

   - **Moștenire.**
   - **Permitere**.
   - **Blocare**.
   - **Înregistrare evenimente 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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **Firewall**.

3. Faceți clic pe butonul **Reguli de 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 rețea**.

7. Selectați regula de rețea a cărei prioritate dorești să o modifici.

8. Utilizează butoanele **Sus** și **Jos** pentru a muta regula de rețea în poziția dorită din lista de reguli 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, faceți clic pe **Mai multe instrumente** → **Monitorizare rețea**.

Se deschide fereastra **Monitorizare rețea**. Informațiile despre activitatea de rețea a computerului sunt afișate în cele patru file ale acestei ferestre:

- Fila **Activitate rețea** afișează toate conexiunile de rețea active în prezent pe computer. Se afișează atât conexiunile de 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 de 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.

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 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 virtuală dacă este disponibilă (consultați figura de mai jos). Această procedură este cunoscută sub numele de Autorizare tastatură.

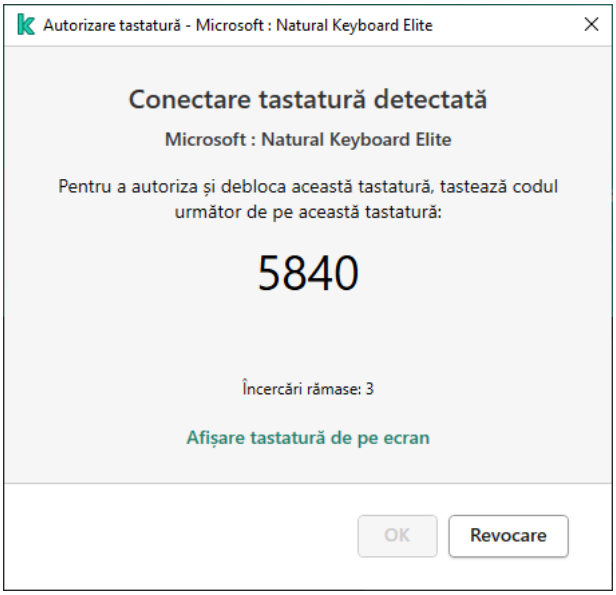
Dacă a fost introdus corect codul, aplicația salvează parametrii de identificare – VID/PID pentru tastatură și numărul portului la care a fost conectată – în lista de tastaturi autorizate. Autorizarea nu trebuie repetată atunci când tastatura este reconectată sau după repornirea sistemului de operare.

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. Sunt disponibile trei încercări pentru introducerea codului numeric. Dacă este introdus în mod incorect codul numeric de trei ori la rând sau dacă fereastra **<Nume tastatură> autorizare tastatură** este închisă, aplicația blochează introducerea de la această tastatură. Atunci când tastatura este reconectată 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.

Pentru a activa sau a dezactiva componenta BadUSB Attack Prevention:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **BadUSB Attack Prevention**.
3. Utilizați comutatorul **BadUSB Attack Prevention** pentru a activa sau a dezactiva componenta.
4. 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 (de exemplu, scanere de coduri de bare). Nu se recomandă folosirea tastaturii virtuale pentru autorizarea dispozitivelor USB necunoscute.

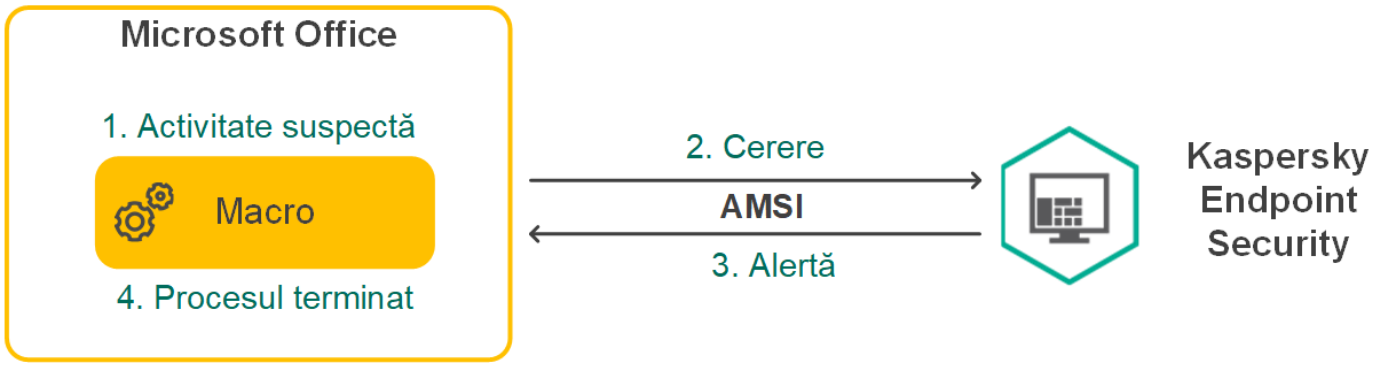
Pentru a permite sau a interzice utilizarea tastaturii virtuale pentru autorizare:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **BadUSB Attack Prevention**.
3. Utilizați caseta de selectare **Interzicere utilizare tastatură vizuală pentru autorizarea dispozitivelor USB** pentru a bloca sau a permite utilizarea tastaturii vizuale pentru autorizare.
4. Salvați-vă modificările.

Protecție AMSI

Componenta Protecție AMSI are rol de suport pentru 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. Aplicația terță, după primirea unei notificări despre o amenințare, nu permite efectuarea de acțiuni rău intenționate (de exemplu, terminări).



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 Protecție AMSI nu refuză solicitări de la aplicațiile terțe pentru care caseta de selectare **Nu se blochează interacțiunea cu Furnizorul de protecție AMSI** este bifată

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;
- Windows Server 2016 Essentials/Standard/Datacenter;
- Windows Server 2019 Essentials/Standard/Datacenter.

Activarea și dezactivarea componentei Protecție AMSI

În mod implicit, componenta Protecție AMSI este activată.

Pentru a activa sau a dezactiva componenta Protecție AMSI:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **Protecție AMSI**.
3. Utilizați comutatorul **Protecție AMSI** pentru a activa sau dezactiva componenta.
4. Salvați-vă modificările.

Utilizarea Protecției AMSI pentru a scana fișiere compuse

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.

Pentru a configura scanarea fișierelor compuse cu Protecție AMSI:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Essential Threat Protection** → **Protecție AMSI**.
3. În secțiunea **Scanare fișiere compuse**, specifică tipurile de fișiere compuse pe care dorești să le scanezi: arhive, pachete de distribuție sau fișiere în formate Office.
4. În secțiunea **Limită dimensiune**, efectuează una dintre următoarele acțiuni:
   - Pentru a bloca componenta Protecție AMSI să dezarhiveze fișierele compuse de dimensiuni mari, bifați caseta de selectare **Nu dezarhiva fișiere compuse mari** și specifică valoarea necesară în câmpul **Dimensiune maximă fișier**. 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 fișiere compuse mari**.

Componenta Protecție AMSI scanează fișierele mari extrase din arhive, indiferent dacă este bifată sau nu caseta de selectare **Nu dezarhiva fișiere compuse mari**.

5. Salvați-vă modificările.

Exploit Prevention

Componenta Exploit Prevention detectează codul programului care profită de vulnerabilitățile de pe 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.

Activarea și dezactivarea componentei Exploit Prevention

În mod implicit, componenta Exploit Prevention este activată și se execută în modul recomandat de experții Kaspersky. Dacă este necesar, poți dezactiva componenta Exploit Prevention.

Pentru a activa sau a dezactiva componenta Exploit Prevention:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Advanced Threat Protection** → **Exploit Prevention**.
3. Utilizați comutatorul **Exploit Prevention** pentru a activa sau a dezactiva componenta.
4. Salvați-vă modificările.

Ca urmare, dacă Exploit Prevention este activat, Kaspersky Endpoint Security va monitoriza fișierele executabile care sunt rulate de aplicații 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).

Selectarea unei acțiuni de efectuat la detectarea unui exploit

În mod implicit, la detectarea unui exploit Kaspersky Endpoint Security blochează operațiunile încercate de exploit.

Pentru a alege o acțiune de efectuat la detectarea unui exploit:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Advanced Threat Protection** → **Exploit Prevention**.
3. Selectați acțiunea relevantă în blocul **La detectarea exploatării**:

- **Blocare operațiune**. 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.

- **Informare**. Dacă este selectat acest element, atunci când Kaspersky Endpoint Security detectează un exploit, înregistrează în jurnal informațiile despre exploit și adaugă informațiile despre acest exploit în lista amenințărilor active.

4. Salvați-vă modificările.

Protecție memorie pentru procese de sistem

În mod implicit, protecția memoriei pentru procese de sistem este activată.

Pentru a activa sau a dezactiva protecția memoriei pentru procese de sistem:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Advanced Threat Protection** → **Exploit Prevention**.
3. Utilizați comutatorul **Activează protecția memoriei pentru procese de sistem** pentru a activa sau a dezactiva această caracteristică.
4. Salvați-vă modificările.

Drept urmare, Kaspersky Endpoint Security va bloca procesele externe care încearcă să acceseze procesele sistemului.

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. Pe baza semnăturilor de flux de comportamental, Kaspersky Endpoint Security oferă o apărare proactivă pentru computer.

Activarea și dezactivarea componentei Behavior Detection

În mod implicit, componenta Behavior Detection este activată și se execută în modul recomandat de experții Kaspersky. Dacă este necesar, poți dezactiva componenta Behavior Detection.

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.

Pentru a activa sau a dezactiva componenta Behavior Detection:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Advanced Threat Protection** → **Behavior Detection**.
3. Utilizați comutatorul **Behavior Detection** pentru a activa sau a dezactiva componenta.
4. 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.

Selectarea acțiunii de urmat la detectarea activității programelor malware

Pentru a alege ce trebuie făcut dacă o aplicație efectuează o activitate rău intenționată, parcurge următorii pași:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Advanced Threat Protection** → **Behavior Detection**.
3. Selectați acțiunea relevantă în blocul **La detectarea activității programelor malware**:
   - **Ștergere fișier**. 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.
   - **Oprește forțat aplicația**. Dacă este selectat acest element, la detectarea unei activități rău intenționate Kaspersky Endpoint Security termină această aplicație.
   - **Informare**. 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.
4. Salvați-vă modificările.

Protecția directoarelor partajate împotriva criptării externe

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.

Protecția directoarelor partajate împotriva criptării externe asigură analiza activității în directoare partajate. Dacă această activitate corespunde unei semnături de flux comportamental care este tipică pentru criptare externă, Kaspersky Endpoint Security execută acțiunea selectată.

În mod implicit, protecția directoarelor partajate împotriva criptării externe este dezactivată.

După instalarea Kaspersky Endpoint Security, protecția directoarelor partajate împotriva criptării externe va fi limitată până la repornirea computerului.

Activarea sau dezactivarea protecției directoarelor partajate împotriva criptării externe

După instalarea Kaspersky Endpoint Security, protecția directoarelor partajate împotriva criptării externe va fi limitată până la repornirea computerului.

Pentru a activa sau a dezactiva protecția directoarelor partajate împotriva criptării externe:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Advanced Threat Protection** → **Behavior Detection**.
3. Utilizați comutatorul **Activează protecția directoarelor partajate împotriva criptării externe** pentru a activa sau a dezactiva detectarea activității tipice criptării externe.
4. Salvați-vă modificările.

Selectarea acțiunii de luat atunci când este detectată criptarea externă a directoarelor partajate

Pentru a selecta acțiunea de luat atunci când este detectată criptarea externă a directoarelor partajate:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Advanced Threat Protection** → **Behavior Detection**.
3. Selectați acțiunea relevantă în blocul **Protecția directoarelor partajate împotriva criptării externe**:
   - **Blochează conexiunea pentru N min**. Dacă această opțiune este selectată și Kaspersky Endpoint Security detectează o încercare de modificare a fișierelor din directoarele partajate, aceasta efectuează următoarele acțiuni:
     - Blochează activitatea de rețea a computerului care încearcă modificarea.
     - Creează copii de rezervă ale fișierelor care sunt modificate.
     - Adaugă o intrare în rapoartele de interfață ale aplicațiilor locale.
     - Trimite informații despre activitatea dăunătoare detectată către Kaspersky Security Center.

     De asemenea, în cazul în care componenta Remediation Engine este activată, fișierele modificate sunt restaurate din copii de rezervă.
   - **Informare**. Dacă această opțiune este selectată și Kaspersky Endpoint Security detectează o încercare de modificare a fișierelor din directoarele partajate, aceasta efectuează următoarele acțiuni:
     - Adaugă o intrare în rapoartele de interfață ale aplicațiilor locale.

- Adaugă o intrare în lista cu amenințări active.
- Trimite informații despre activitatea dăunătoare detectată către Kaspersky Security Center.

4. Salvați-vă modificările.

Crearea unei excluderi pentru protecția directoarelor partajate împotriva criptării externe

Excluderea unui director 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.

Cum se creează o excludere pentru protejarea directoarelor partajate utilizând Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Setări generale** → **Excluderi**.
6. În secțiunea **Scan exclusions and trusted applications**, fă clic pe butonul **Settings**.
7. În fereastra care se deschide, selectează fila **Excluderi de la scanare**.

   Acest lucru va deschide o fereastră care conține lista excluderilor.
8. Bifați caseta de selectare **Îmbinare valori 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.
9. Bifați caseta de selectare **Permite utilizarea aplicațiilor de încredere 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. Dacă a fost generată o listă locală, după dezactivarea acestei funcționalități, Kaspersky Endpoint Security continuă să excludă din scanări fișierele listate.
10. Faceți clic pe butonul **Adăugare**.
11. În secțiunea **Proprietăți**, bifați caseta de selectare **Fișier sau director**.
12. Faceți clic pe linkul **Selectare fișier sau director** din secțiunea **Descriere excludere de la scanare (faceți clic pe elementele subliniate pentru a le edita)** pentru a deschide fereastra **Nume al fișierului sau al directorului**.
13. Faceți clic pe **Răsfoire** și selectați directorul partajat.

    De asemenea, puteți introduce manual calea. 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 `Director`, cu excepția `Directorului` în sine. Masca trebuie să includă cel puțin un nivel de imbricare. Masca `C:\**\*.txt` nu este o mască validă.

- Caracterul `?` (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.

14. Dacă este necesar, în câmpul **Comentariu**, introdu o descriere succintă a excluderii de la scanare pe care o creezi.

15. Dacă faci clic pe linkul **oricare** din secțiunea **Descriere excludere de la scanare (fă clic pe elementele subliniate pentru a le edita)** pentru a activa linkul **Selectare componente**.

16. Faceți clic pe linkul **Selectare componente** pentru a deschide fereastra **Componente protecție**.

17. Bifează caseta de selectare de lângă componenta **Behavior Detection**.

18. Salvați-vă modificările.

Cum se creează o excludere pentru protejarea directoarelor partajate utilizând Web Console și Cloud Console

1. În fereastra principală a Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Selectați **General settings** → **Exclusions**.
5. În blocul **Excluderi de la scanare și aplicații de încredere**, faceți clic pe linkul **Excluderi de la scanare**.
6. Bifați caseta de selectare **Îmbinare valori 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.
7. Bifați caseta de selectare **Permite utilizarea aplicațiilor de încredere 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. Dacă a fost generată o listă locală, după dezactivarea acestei funcționalități, Kaspersky Endpoint Security continuă să excludă din scanări fișierele listate.
8. Faceți clic pe butonul **Adăugare**.
9. Selectați modul în care doriți să adăugați excluderea **File or folder**.
10. Faceți clic pe **Răsfoire** și selectați directorul partajat.

    De asemenea, puteți introduce manual calea. 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 `Director`, cu excepția `Directorului` în sine. Masca trebuie să includă cel puțin un nivel de imbricare. Masca `C:\**\*.txt` nu este o mască validă.
    - Caracterul `?` (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.
11. În blocul **Componente protecție**, selectează componenta **Behavior Detection**.

12. Dacă este necesar, în câmpul **Comentariu**, introdu o descriere succintă a excluderii de la scanare pe care o creezi.

13. Selectați starea **Activă** pentru excludere.

    Puteți utiliza comutatorul pentru a opri o excludere în orice moment.

14. Salvați-vă modificările.

[Cum se creează o excludere pentru protejarea directoarelor partajate în interfața aplicației]

1. În fereastra principală a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Setări generale** → **Amenințări și excluderi**.

3. În blocul **Excluderi**, faceți clic pe linkul **Gestionare excluderi**.

4. Faceți clic pe butonul **Adăugare**.

5. Faceți clic pe **Răsfoire** și selectați directorul partajat.

   De asemenea, puteți introduce manual calea. 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 `Director`, cu excepția `Directorului` în sine. Masca trebuie să includă cel puțin un nivel de imbricare. Masca `C:\**\*.txt` nu este o mască validă.

   - Caracterul `?` (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.

6. În blocul **Componente protecție**, selectează 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 opri o excludere în orice moment.

9. Salvați-vă modificările.

Configurarea adreselor de excluderi de la protecția directoarelor partajate împotriva criptării externe

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.

Pentru a exclude computere aflate la distanță care efectuează criptarea externă a directoarelor partajate:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul .
2. În fereastra cu setările aplicației, selectați **Protecție** → **Advanced Threat Protection** → **Behavior Detection**.
3. În blocul **Excluderi**, faceți clic pe linkul **Configurare adrese de excluderi**.
4. Dacă vrei să adaugi o adresă IP sau numele unui computer în lista de excluderi, faceți clic pe butonul **Adăugare**.
5. Introdu adresa IP sau numele computerului de unde nu trebuie gestionate încercările de criptare externă.
6. Salvați-vă modificările.

Exportarea și importarea unei liste de excluderi de la protecția directoarelor partajate împotriva criptării externe

Puteți 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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Advanced Threat Protection** → **Behavior Detection**.
6. În secțiunea **Protecția directoarelor partajate împotriva criptării externe**, apasă pe butonul **Excluderi**.
7. 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. Faceți clic pe linkul **Exportare**.
   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. Faceți clic pe butonul **Save**.
      Kaspersky Endpoint Security exportă întreaga listă de excluderi în fișierul XML.
8. Pentru a importa lista de excluderi:
   a. Faceți clic pe butonul **Import**.
   b. În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de excluderi.
   c. Faceți clic pe butonul **Deschidere**.
      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.
9. Salvați-vă modificările.

[Cum se exportă și se importă o listă de excluderi în Consola Web și Cloud Console]

1. În fereastra principală a Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security pentru computerele pe care doriți să exportați sau să importați o listă de excluderi.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Selectați **Advanced Threat Protection** → **Behavior Detection**.
5. Pentru a exporta lista excluderilor din blocul **Excluderi**:
   a. Selectați excluderile pe care doriți să le exportați.
   b. Faceți clic pe butonul **Export**.
   c. Confirmați că doriți să exportați numai excluderile selectate sau exportați întreaga listă de excluderi.
   d. 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.
   e. Faceți clic pe butonul **Save**.

      Kaspersky Endpoint Security exportă întreaga listă de excluderi în fișierul XML.
6. Pentru a importa lista excluderilor din blocul **Excluderi**:
   a. Faceți clic pe butonul **Import**.
   b. În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de excluderi.
   c. Faceți clic pe butonul **Deschidere**.

      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.

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 (cum ar fi fișiere și aplicații)

Activitatea de rețea a aplicațiilor este controlată de 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 din *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 puteți schimba grupul de încredere numai pentru 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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Advanced Threat Protection → Host Intrusion Prevention**.
6. Utilizați caseta de selectare **Host Intrusion Prevention** pentru a activa sau a dezactiva componenta.
7. Salvați-vă modificările.

Cum se activează sau dezactivează componenta Host Intrusion Prevention în Web Console și Cloud Console

1. În fereastra principală a Consolei Web, selectați **Dispozitive → Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.
   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Selectați **Advanced Threat Protection → Host Intrusion Prevention**.
5. Utilizați comutatorul **Host Intrusion Prevention** 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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul .
2. În fereastra setărilor aplicației, selectați **Protecție → 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 căruia Kaspersky Endpoint Security trebuie să-i atribuie automat toate aplicațiile necunoscute. Aplicațiile care au fost pornite înainte de Kaspersky Endpoint Security sunt mutate automat în grupul de încredere definit 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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Advanced Threat Protection** → **Host Intrusion Prevention**.
6. În blocul **Drepturi aplicații**, faceți clic pe butonul **Setări**.

   Tastfel se deschide fereastra de configurare a drepturilor aplicațiilor și lista resurselor protejate.
7. Selectați fila **Drepturi aplicații**.
8. Faceți clic pe butonul **Adăugare**.
9. În fereastra deschisă, 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.
10. Faceți clic pe butonul **Împrospătare**.

    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.
11. Selectați aplicația necesară.
12. În lista verticală **Adaugă aplicațiile selectate la grupul <grup de încredere>**, selectați grupul de încredere necesar pentru aplicație.
13. Salvați-vă modificările.

[Cum se modifică grupul de încredere al unei aplicații în Web Console și Cloud Console]

1. În fereastra principală a Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Selectați **Advanced Threat Protection** → **Host Intrusion Prevention**.
5. În blocul **Drepturile aplicației și resursele protejate**, faceți clic pe linkul **Drepturile aplicației și resursele protejate**.

   Tastfel se deschide fereastra de configurare a drepturilor aplicațiilor și lista resurselor protejate.
6. Selectați fila **Drepturi aplicații**.

   Veți vedea o listă cu grupurile de încredere în partea stângă a ferestrei, iar proprietățile acestora în partea dreaptă.
7. Faceți clic pe butonul **Adăugare**.

   Aceasta pornește Expertul pentru adăugarea unei aplicații la un grup de încredere.
8. Faceți clic pe linkul **Grup țintă selectat** pentru a selecta grupul de încredere relevant pentru aplicație.
9. Selectați **Tip aplicație**. Faceți clic pe butonul **Next**.

   Dacă doriți să modificați grupul de încredere pentru mai multe aplicații, selectați **Tip grup** 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. Finalizați Expertul, făcând clic pe **OK**.

    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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul .
2. În fereastra setărilor aplicației, selectați **Protecție** → **Advanced Threat Protection** → **Host Intrusion Prevention**.
3. Faceți clic pe butonul **Gestionare aplicații**.

   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 *(definită 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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Advanced Threat Protection** → **Host Intrusion Prevention**.
6. În blocul **Drepturi aplicații**, faceți clic pe butonul **Setări**.

   Tastfel se deschide fereastra de configurare a drepturilor aplicațiilor și lista resurselor protejate.
7. Selectați fila **Drepturi aplicații**.
8. Selectați grupul de încredere necesar.
9. Selectați **Drepturi grup** din meniul contextual al grupului de încredere.

   Aceasta deschide proprietățile grupului de încredere.
10. Efectuează una dintre următoarele acțiuni:

    - Dacă dorești să editezi drepturi unui grup de încredere care guvernează operațiile cu registry-ul sistemului de operare, fișierele utilizatorului și setările aplicațiilor, selectați fila **Fișiere și registry sistem**.
    - Dacă doriți să editați drepturile grupului de încredere care reglementează accesul la procesele și obiectele sistemului de operare, selectați fila **Drepturi**.

    Activitatea de rețea a aplicațiilor este controlată de Firewall folosind *regulile de rețea* .
11. Pentru resursa relevantă, în coloana acțiunii corespunzătoare, faceți clic dreapta pentru a se deschide meniul contextual și selectați opțiunea necesară: **Moștenire**, **Permitere** (✓) sau **Interzicere** (⊘).
12. Dacă doriți să monitorizați utilizarea resurselor computerului, selectați **Scriere în raport** (✓ / ⊘).

    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.
13. Salvați-vă modificările.

Cum se modifică drepturile grupului de încredere în Web Console și Cloud Console

1. În fereastra principală a Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Selectați **Advanced Threat Protection** → **Host Intrusion Prevention**.
5. În blocul **Drepturile aplicației și resursele protejate**, faceți clic pe linkul **Drepturile aplicației și resursele protejate**.

   Tastfel se deschide fereastra de configurare a drepturilor aplicațiilor și lista resurselor protejate.
6. Selectați fila **Drepturi aplicații**.

   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 **Fișiere și registry sistem**.
   - Dacă doriți să editați drepturile grupului de încredere care reglementează accesul la procesele și obiectele sistemului de operare, selectați **Drepturi**.

   Activitatea de rețea a aplicațiilor este controlată de Firewall folosind *regulile de rețea* .
9. Pentru resursa relevantă, în coloana acțiunii corespunzătoare, selectați opțiunea necesară: **Moștenire**, **Permitere** ( ) sau **Interzicere** ( ).
10. Dacă doriți să monitorizați utilizarea resurselor computerului, selectați **Scriere în raport** (/).

    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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul .
2. În fereastra setărilor aplicației, selectați **Protecție** → **Advanced Threat Protection** → **Host Intrusion Prevention**.
3. Faceți clic pe butonul **Gestionare aplicații**.

   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 dorești să editezi drepturi unui grup de încredere care guvernează operațiile cu registry-ul sistemului de operare, fișierele utilizatorului și setările aplicațiilor, selectați fila **Fișiere și registry sistem**.
   - Dacă doriți să editați drepturile grupului de încredere care reglementează accesul la procesele și obiectele sistemului de operare, selectați fila **Drepturi**.

   Activitatea de rețea a aplicațiilor este controlată de 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: **Moștenire**, **Permitere** ( ) sau **Interzicere** ( ).
8. Dacă doriți să monitorizați utilizarea resurselor computerului, selectați **Scriere în raport** ( ).

   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 utilizator*) 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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Advanced Threat Protection → Host Intrusion Prevention**.
6. În blocul **Drepturi aplicație**, faceți clic pe butonul **Editare**.
7. Selectați grupul de încredere necesar pentru setarea **Aplicațiile lansate înaintea componentei Kaspersky Endpoint Security for Windows sunt mutate automat în grupul de încredere <grup de încredere>**.
8. Salvați-vă 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 Consolei Web, selectați **Dispozitive → Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.
   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Selectați **Advanced Threat Protection → Host Intrusion Prevention**.
5. Selectați grupul de încredere necesar pentru setarea **Aplicațiile lansate înaintea componentei Kaspersky Endpoint Security for Windows sunt mutate automat în grupul de încredere <grup de încredere>**.
6. Salvați-vă modificările.

Cum se selectează un grup de încredere pentru aplicații pornite înaintea componentei Kaspersky Endpoint Security în interfața aplicației

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra setărilor aplicației, selectați **Protecție → Advanced Threat Protection → Host Intrusion Prevention**.
3. Selectați grupul de încredere necesar în blocul **Aplicațiile lansate înaintea componentei Kaspersky Endpoint Security for Windows sunt mutate automat în grupul de încredere <grup de încredere>**.
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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Advanced Threat Protection** → **Host Intrusion Prevention**.
6. În blocul **Reguli de procesare a aplicațiilor**, utilizați lista verticală **Grup de încredere pentru aplicațiile care nu au putut fi alocate în alte grupuri** 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.
7. Utilizați caseta de selectare **Actualizare drepturi pentru aplicații necunoscute anterior de la baza de date KSN** pentru a configura actualizarea automată a drepturilor pentru aplicațiile necunoscute.
8. Salvați-vă modificările.

Cum se selectează un grup de încredere pentru aplicații necunoscute în Web Console și Cloud Console

1. În fereastra principală a Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Selectați **Advanced Threat Protection** → **Host Intrusion Prevention**.
5. În blocul **Reguli de procesare a aplicațiilor**, utilizați lista verticală **Grup de încredere pentru aplicațiile care nu au putut fi alocate în alte grupuri** 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 **Actualizare drepturi pentru aplicații necunoscute anterior de la baza de date KSN** 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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul .
2. În fereastra setărilor aplicației, selectați **Protecție** → **Advanced Threat Protection** → **Host Intrusion Prevention**.
3. În blocul **Grup de încredere pentru aplicații necunoscute**, selectați grupul de încredere relevant.

   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 **Actualizare drepturi pentru aplicații necunoscute anterior de la baza de date 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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Advanced Threat Protection → Host Intrusion Prevention**.
6. În blocul **Reguli de procesare a aplicațiilor**, utilizați caseta de selectare **Aplicații de încredere care au o semnătură digitală** pentru a activa sau dezactiva atribuirea automată în Grupul de încredere pentru aplicațiile care conțin semnătura digitală a producătorilor de încredere.

   Producătorii de încredere 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.
7. Salvați-vă modificările.

Cum se selectează un grup de încredere pentru aplicații semnate digital în Web Console și Cloud Console

1. În fereastra principală a Consolei Web, selectați **Dispozitive → Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Selectați **Advanced Threat Protection → Host Intrusion Prevention**.
5. În blocul **Reguli de procesare a aplicațiilor**, utilizați caseta de selectare **Aplicații de încredere care au o semnătură digitală** pentru a activa sau dezactiva atribuirea automată în Grupul de încredere pentru aplicațiile care conțin semnătura digitală a producătorilor de încredere.

   Producătorii de încredere 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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra setărilor aplicației, selectați **Protecție** → **Advanced Threat Protection** → **Host Intrusion Prevention**.
3. În blocul **Reguli de procesare a aplicațiilor**, utilizați caseta de selectare **Aplicații de încredere care au o semnătură digitală** pentru a activa sau dezactiva atribuirea automată în Grupul de încredere pentru aplicațiile care conțin semnătura digitală a producătorilor de încredere.

   Producătorii de încredere 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. Dacă o aplicație este pornită indirect de altă aplicație, dar 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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Advanced Threat Protection** → **Host Intrusion Prevention**.
6. În blocul **Drepturi aplicații**, faceți clic pe butonul **Setări**.

   Tastfel se deschide fereastra de configurare a drepturilor aplicațiilor și lista resurselor protejate.
7. Selectați fila **Drepturi aplicații**.
8. Faceți clic pe butonul **Adăugare**.
9. În fereastra deschisă, introduceți criteriul de căutare a aplicației 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.
10. Faceți clic pe butonul **Împrospătare**.

    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.
11. Selectați aplicația necesară.
12. În lista verticală **Adaugă aplicațiile selectate la grupul <grup de încredere>**, selectați **Grupuri implicite** și faceți clic pe **OK**.

    Aplicația va fi adăugată la grupul implicit.
13. Selectați aplicația relevantă și apoi selectați **Drepturi aplicație** din meniul contextual al aplicației.

    Aceasta deschide proprietățile aplicației.
14. Efectuează una dintre următoarele acțiuni:

    - Dacă dorești să editezi drepturi unui grup de încredere care guvernează operațiile cu registry-ul sistemului de operare, fișierele utilizatorului și setările aplicațiilor, selectați fila **Fișiere și registry sistem**.
    - Dacă doriți să editați drepturile grupului de încredere care reglementează accesul la procesele și obiectele sistemului de operare, selectați fila **Drepturi**.

    Activitatea de rețea a aplicațiilor este controlată de Firewall folosind *regulile de rețea* .
15. Pentru resursa relevantă, în coloana acțiunii corespunzătoare, faceți clic dreapta pentru a se deschide meniul contextual și selectați opțiunea necesară: **Moștenire**, **Permitere** (✓) sau **Interzicere** (⊘).
16. Dacă doriți să monitorizați utilizarea resurselor computerului, selectați **Scriere în raport** (✓ / ⊘).

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.

17. Salvați-vă modificările.

Cum se modifică drepturile pentru aplicații în Web Console și Cloud Console

1. În fereastra principală a Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Selectați **Advanced Threat Protection** → **Host Intrusion Prevention**.
5. În blocul **Drepturile aplicației și resursele protejate**, faceți clic pe linkul **Drepturile aplicației și resursele protejate**.

   Tastfel se deschide fereastra de configurare a drepturilor aplicațiilor și lista resurselor protejate.
6. Selectați fila **Drepturi aplicații**.

   Veți vedea o listă cu grupurile de încredere în partea stângă a ferestrei, iar proprietățile acestora în partea dreaptă.
7. Faceți clic pe butonul **Adăugare**.

   Aceasta pornește Expertul pentru adăugarea unei aplicații la un grup de încredere.
8. Faceți clic pe linkul **Grup țintă selectat** pentru a selecta grupul de încredere relevant pentru aplicație.
9. Selectați **Tip aplicație**. Faceți clic pe butonul **Next**.

   Dacă doriți să modificați grupul de încredere pentru mai multe aplicații, selectați **Tip grup** 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. Finalizați Expertul, făcând clic pe **OK**.

    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 **Fișiere și registry sistem**.
    - Dacă doriți să editați drepturile grupului de încredere care reglementează accesul la procesele și obiectele sistemului de operare, selectați **Drepturi**.

    Activitatea de rețea a aplicațiilor este controlată de Firewall folosind *regulile de rețea* .
14. Pentru resursa relevantă, în coloana acțiunii corespunzătoare, selectați opțiunea necesară: **Moștenire**, **Permitere** ( ) sau **Interzicere** ( ).
15. Dacă doriți să monitorizați utilizarea resurselor computerului, selectați **Scriere în raport** (/).

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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul .
2. În fereastra setărilor aplicației, selectați **Protecție** → **Advanced Threat Protection** → **Host Intrusion Prevention**.
3. Faceți clic pe butonul **Gestionare aplicații**.

   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 dorești să editezi drepturi unui grup de încredere care guvernează operațiile cu registry-ul sistemului de operare, fișierele utilizatorului și setările aplicațiilor, selectați fila **Fișiere și registry sistem**.
   - Dacă doriți să editați drepturile grupului de încredere care reglementează accesul la procesele și obiectele sistemului de operare, selectați fila **Drepturi**.
7. Pentru resursa relevantă, în coloana acțiunii corespunzătoare, faceți clic dreapta pentru a se deschide meniul contextual și selectați opțiunea necesară: **Moștenire**, **Permitere** () sau **Interzicere** ().
8. Dacă doriți să monitorizați utilizarea resurselor computerului, selectați **Scriere în raport** ().

   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 fișiere deschise	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. Activitatea aplicației este monitorizată prin următoarele componente: Behavior Detection, Exploit Prevention, Host Intrusion Prevention, Remediation Engine și Firewall.
Nu moșteni restricții de la procesul părinte (aplicație)	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 aplicațiilor secundare	Kaspersky Endpoint Security nu va monitoriza activitatea fișierelor sau activitatea de rețea a aplicațiilor care sunt pornite de această aplicație.

Permitere interacțiune 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.

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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Advanced Threat Protection** → **Host Intrusion Prevention**.
6. În blocul **Drepturi aplicații**, faceți clic pe butonul **Setări**.

   Tastfel se deschide fereastra de configurare a drepturilor aplicațiilor și lista resurselor protejate.
7. Selectați 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.
8. Selectați categoria de resurse protejate la care doriți să adăugați o nouă resursă protejată.

   Dacă doriți să adăugați o subcategorie, faceți clic pe **Adăugare** → **Categorie**.
9. Faceți clic pe butonul **Adăugare**. În lista verticală, selectați tipul de resursă pe care dorești s-o adaugi: **Fișier sau director** sau **Cheie de registry**.
10. În fereastra deschisă, selectați un fișier, director sau 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.
11. Salvați-vă modificările.

Cum se adaugă o resursă protejată în Web Console și Cloud Console

1. În fereastra principală a Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Selectați **Advanced Threat Protection** → **Host Intrusion Prevention**.
5. În blocul **Drepturile aplicației și resursele protejate**, faceți clic pe linkul **Drepturile aplicației și resursele protejate**.

   Tastfel se deschide fereastra de configurare a drepturilor aplicațiilor și lista resurselor protejate.
6. Selectați 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.
7. Faceți clic pe butonul **Adăugare**.

   Funcția Expert pentru resursă nouă pornește.
8. Faceți clic pe linkul **Nume grup** pentru a selecta categoria de resurse protejate la care doriți să adăugați o nouă resursă protejată.

   Dacă doriți să adăugați o subcategorie, selectați opțiunea **Categorie de resurse protejate**.
9. Selectați tipul de resursă pe care dorești s-o adaugi: **Fișier sau director** sau **Cheie de registry**.
10. Selectați un fișier, un dosar sau o cheie de registry.
11. Finalizați Expertul, făcând clic pe **OK**.

    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 **Stare** pentru a dezactiva controlul activității aplicației cu resursele.
12. Salvați-vă modificările.

Cum se adaugă o resursă protejată în interfața aplicației

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra setărilor aplicației, selectați **Protecție** → **Advanced Threat Protection** → **Host Intrusion Prevention**.
3. Faceți clic pe butonul **Gestionare resurse**.

   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 **Adăugare** → **Categorie**.
5. Faceți clic pe butonul **Adăugare**. În lista verticală, selectați tipul de resursă pe care dorești s-o adaugi: **Fișier sau director** sau **Cheie de registry**.
6. În fereastra deschisă, selectați un fișier, director sau 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 **Dezactivare 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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Advanced Threat Protection** → **Host Intrusion Prevention**.
6. În blocul **Reguli de procesare a aplicațiilor**, efectuați una dintre următoarele acțiuni:
   - Dacă doriți să configurați ștergerea automată, bifați caseta de selectare **Reguli de ștergere pentru aplicațiile care nu au fost lansate pentru o perioadă mai mare de N zile** și specificați numărul necesar 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 validare **Reguli de ștergere pentru aplicațiile care nu au fost lansate pentru o perioadă mai mare de N 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 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.
7. Salvați-vă modificările.

[Cum se configurează ștergerea automată a informațiilor despre aplicațiile neutilizate în Web Console și Cloud Console]

1. În fereastra principală a Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Selectați **Advanced Threat Protection** → **Host Intrusion Prevention**.
5. În blocul **Reguli de procesare a aplicațiilor**, efectuați una dintre următoarele acțiuni:

   - Dacă doriți să configurați ștergerea automată, bifați caseta de selectare **Reguli de ștergere pentru aplicațiile care nu au fost lansate pentru o perioadă mai mare de N zile** și specificați numărul necesar 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 validare **Reguli de ștergere pentru aplicațiile care nu au fost lansate pentru o perioadă mai mare de N 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 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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra setărilor aplicației, selectați **Protecție** → **Advanced Threat Protection** → **Host Intrusion Prevention**.
3. În blocul **Reguli de procesare a aplicațiilor**, efectuați una dintre următoarele acțiuni:
   - Dacă doriți să configurați ștergerea automată, bifați caseta de selectare **Reguli de ștergere pentru aplicațiile care nu au fost lansate pentru o perioadă mai mare de N zile** și specificați numărul necesar 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 validare **Reguli de ștergere pentru aplicațiile care nu au fost lansate pentru o perioadă mai mare de N 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 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

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 controlează accesul aplicațiilor la fluxul audio și la fluxul video în funcție de categoria aplicației:

- Aplicațiile De încredere sau Restricționate la nivel inferior pot primi, în mod implicit, fluxuri audio și video de la dispozitive.
- Aplicațiile Restricționate la nivel superior și aplicațiile care nu sunt de încredere nu pot primi, în mod implicit, fluxuri audio și 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 nicio notificare.
- 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.

Remediation Engine

Componenta Remediation Engine permite Kaspersky Endpoint Security să restaureze 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 registru**

  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 de 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 a acțiunilor unui malware poate fi pornită de componenta File Threat Protection sau Behavior Detection ori în cursul unei scanări de viruși.

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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Advanced Threat Protection → Remediation Engine**.
6. Utilizați caseta de selectare **Remediation Engine** pentru a activa sau a dezactiva componenta.
7. Salvați-vă modificările.

Cum se activează sau dezactivează componenta Remediation Engine în Web Console și Cloud Console

1. În fereastra principală a Consolei Web, selectați **Dispozitive → Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Selectați **Advanced Threat Protection → Remediation Engine**.
5. Utilizați comutatorul **Remediation Engine** pentru a activa sau a dezactiva componenta.
6. Salvați-vă modificările.

[Cum se activează sau dezactivează componenta Remediation Engine în interfața aplicației]

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra setărilor aplicației, selectați **Protecție** → **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.

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 oferă Kaspersky Endpoint Security informații despre categoria și reputația fișierelor scanate, precum și informații despre reputația adreselor web scanate.

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.

Pentru a reduce încărcarea serverelor KSN, experții Kaspersky pot să lanseze actualizări ale aplicațiilor care dezactivează temporar sau restricționează parțial solicitările către Kaspersky Security Network. În acest caz, starea conexiunii la KSN în interfața locală a aplicației este *Activată cu restricții*.

Infrastructura KSN

Kaspersky Endpoint Security acceptă următoarele soluții de infrastructură KSN:

- *Global KSN* este soluția folosită de majoritatea aplicațiilor Kaspersky. Participanții KSN primesc informații de la Kaspersky Security Network și trimit informațiile Kaspersky despre obiecte detectate pe computerul utilizatorului pentru a fi analizate suplimentar de analiștii Kaspersky pentru a fi incluse în bazele de date privind reputația și în cele statistice ale Kaspersky Security Network.
- *Private KSN* este o soluție care permite utilizatorilor de computere care găzduiesc Kaspersky Endpoint Security sau alte aplicații Kaspersky să obțină acces la bazele de date de renume ale Kaspersky Security Network și la alte date statistice, fără a trimite date către KSN de la propriile lor computere. Private KSN 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.

În mod implicit, Kaspersky Security Center utilizează Global KSN. Puteți configura utilizarea tehnologiei Private KSN în Consola de administrare (MMC), în Kaspersky Security Center 12 Web Console și în linia de comandă. Nu este posibil să configurați utilizarea tehnologiei Private KSN în Kaspersky Security Center Cloud Console.

Pentru mai multe detalii despre Private KSN, consultați *documentația cu privire la Kaspersky Private Security Network*.

Proxy KSN

Computerele utilizatorilor administrate de Serverul de administrare Kaspersky Security Center pot interacționa cu KSN prin serviciul Proxy KSN.

Serviciul Proxy KSN oferă următoarele funcționalități:

- Computerul utilizatorului poate interoga KSN și poate trimite informații către KSN, chiar și fără acces direct la Internet.
- Serviciul Proxy KSN stochează în memoria cache datele procesate, reducând astfel încărcarea asupra canalului de comunicare în rețeaua externă și accelerând recepția informațiilor solicitate de computerul utilizatorului.

Pentru mai multe detalii despre serviciul KSN Proxy, consultați *Ghidul de ajutor pentru Kaspersky Security Center*.

Activarea și dezactivarea utilizării Kaspersky Security Network

Pentru a activa sau a dezactiva utilizarea Kaspersky Security Network:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **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. Citiți și acceptați condițiile din Declarația Kaspersky Security Network (KSN) dacă sunteți de acord cu acestea.

   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.
4. Dacă este necesar, debifați caseta de selectare **Activare mod KSN extins**.
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.

Limitările Private KSN

Private KSN (denumit în continuare KPSN) vă permite să utilizați propria bază de date locală a reputației 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.

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.

Pentru a activa sau a dezactiva modul cloud pentru componentele protecției:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul .

2. În fereastra cu setările aplicației, selectați **Protecție** → **Advanced Threat Protection** → **Kaspersky Security Network**.

3. Utilizați comutatorul **Activare mod cloud** pentru a activa sau 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.

Verificarea conexiunii la serviciul Kaspersky Security Network

Conexiunea dvs. la Kaspersky Security Network se poate pierde din unul dintre motivele următoare:

- Nu participați la Kaspersky Security Network.
- Computerul nu este conectat la internet.
- Starea cheii curente nu permite conectarea la Kaspersky Security Network. De exemplu, o conexiune la KSN poate fi indisponibilă din următoarele motive:
  - Aplicația nu este activată.
  - Licența sau abonamentul a expirat.
  - Problemele legate de cheia de licență au fost identificate (de exemplu, cheia a fost adăugată la lista de chei interzise).

Pentru a verifica o conexiune la serviciul Kaspersky Security Network:

În fereastra principală a aplicației, faceți clic pe **Mai multe instrumente** → **Kaspersky Security Network**.

Aceasta deschide fereastra **Kaspersky Security Network**, care afișează informații despre activitatea Kaspersky Security Network. Aplicația primește statistici de utilizare KSN când se deschide fereastra **Kaspersky Security Network**. Statisticile globale ale infrastructurii serviciilor cloud Kaspersky Security Network și momentul sincronizării nu se reîmprospătează în timp real.

Partea din stânga a ferestrei **Kaspersky Security Network** afișează una dintre următoarele stări pentru conexiunea dintre computer și Kaspersky Security Network:

- *Activat.*

  Această stare înseamnă că produsul Kaspersky Security Network este folosit în operațiunile Kaspersky Endpoint Security și că serverele KSN sunt disponibile.

- *Activat. Disponibilă cu restricții.*

  Această stare înseamnă că produsul Kaspersky Security Network este folosit în operațiunile Kaspersky Endpoint Security și că serverele KSN sunt indisponibile.

Este posibil ca serverele KSN să nu fie disponibile din următoarele motive:

- Serviciul KSN Proxy (ksnproxy) rulează pe computer.
- Firewallul blochează portul 13111.

Dacă durata care a trecut de la ultima sincronizare cu serverele KSN depășește 15 minute sau arată starea *Necunoscut*, starea conexiunii Kaspersky Endpoint Security la Kaspersky Security Network preia *valoarea Activat. Indisponibil.*

- *Oprit.*

  Această stare înseamnă că produsul Kaspersky Security Network nu este folosit în operațiunile Kaspersky Endpoint Security.

Dacă nu se poate reface conexiunea la serverele Kaspersky Security Network, îți recomandăm să contactezi Asistența tehnică sau furnizorul de servicii.

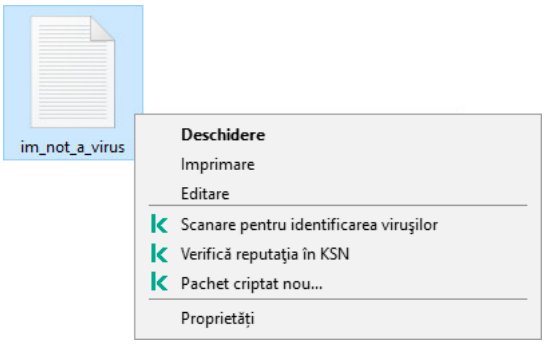
Verificarea reputației unui fișier în Kaspersky Security Network

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 **Verifică reputația în KSN** (consultați figura de mai jos).



Meniu contextual fișier

Kaspersky Endpoint Security afișează reputația fișierului:

De încredere. Majoritatea utilizatorilor Kaspersky Security Network au confirmat că fișierul este de încredere.

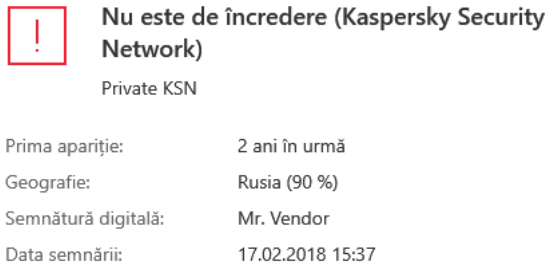
Software legal care ar putea fi exploatat pentru a dăuna computerului sau datelor cu caracter personal. Cu toate că nu au funcții rău intenționate, astfel de aplicații pot fi exploatate de intruși. Pentru detalii despre software-urile legale care pot fi folosite de infractori pentru a prejudicia computerul 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. Un virus sau o altă aplicație care reprezintă o amenințare.

Necunoscută. Kaspersky Security Network nu are informații despre fișier. Puteți scana un fișier utilizând bazele de date antivirus (opțiunea **Scanare pentru identificarea virușilor** din meniul contextual).

Kaspersky Endpoint Security afișează soluția KSN care a fost utilizată pentru a determina reputația fișierului: *Global KSN* sau *Private KSN*.

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

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.

După instalare, Kaspersky Endpoint Security adaugă certificatul Kaspersky la stocarea de sistem a certificatelor de încredere (depozitul de certificate Windows). 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 și Web Threat Protection pot decripta și scana trafic 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.

Configurarea setărilor pentru scanarea conexiunilor criptate

Pentru a configura setările pentru scanarea conexiunilor criptate:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Setări de rețea**.
3. În secțiunea Scanare conexiuni criptate, selectați modul de scanare a conexiunilor criptate:
   - **Nu se scanează conexiunile criptate** Kaspersky Endpoint Security nu va avea acces la conținutul site-urilor web ale căror adrese încep cu `https://`.
   - **Se scanează conexiunile criptate la cererea componentelor de protecție**. Kaspersky Endpoint Security va scana traficul criptat numai la solicitarea componentelor File Threat Protection, Mail Threat Protection și Control web.
   - **Se 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. Faceți clic pe butonul **Setări avansate**.
6. Configurați setările pentru scanarea conexiunilor criptate (consultați tabelul de mai jos).
7. Salvați-vă modificările.

Setări scanare conexiuni criptate

Parametru	Descriere
La vizitarea unui domeniu cu un certificat care nu este de încredere	• **Permitere**. Dacă este selectată această opțiune, atunci când se vizitează un domeniu cu un certificat neautorizat, 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. 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. • **Blocare conexiune**. Dacă este selectată această opțiune, atunci când se vizitează un domeniu cu un certificat neautorizat, Kaspersky Endpoint Security permite 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.

Când apar erori la scanarea conexiunilor criptate	• **Blocare conexiune**. Dacă acest element este selectat, atunci când apare o eroare la scanare în cadrul unei conexiuni criptate, Kaspersky Endpoint Security blochează conexiunea la rețea. • **Adăugare domeniu la excluderi**. Dacă acest element este selectat, atunci când apare o eroare la scanare în cadrul unei conexiuni 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 **Blocare conexiune**.
Blocare conexiuni SSL 2.0	Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security blochează conexiunile la rețea stabilite prin protocolul SSL 2.0. Dacă această casetă de selectare nu este bifată, Kaspersky Endpoint Security nu blochează conexiunile la rețea stabilite prin protocolul SSL 2.0 și nu monitorizează traficul de rețea transmis prin aceste conexiuni.
Decriptarea conexiunilor criptate cu site-urile web care utilizează certificate EV	Certificatele EV (certificate cu validare extinsă) 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, Kaspersky Endpoint Security decriptează și monitorizează conexiunile criptate cu site-uri web care utilizează un certificat EV. În cazul în care caseta de selectare este debifată, Kaspersky Endpoint Security nu are acces la conținutul traficului HTTPS. Din acest motiv, aplicația monitorizează traficul HTTPS doar pe baza adresei site-ului web, de exemplu, `https://facebook.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.

Scanarea conexiunilor criptate în Firefox și Thunderbird

După instalare, Kaspersky Endpoint Security adaugă certificatul Kaspersky la stocarea de sistem a certificatelor de încredere (depozitul de certificate Windows). În mod implicit, Firefox și Thunderbird folosesc propriul depozit de certificate, proprietate a Mozilla, în locul depozitului de certificate Windows. Dacă Kaspersky Security Center este implementat în organizația dvs. și o politică este aplicată unui computer, Kaspersky Endpoint Security permite automat utilizarea depozitului de certificate Windows în Firefox și Thunderbird pentru a scana traficul acestor aplicații. Dacă nu este aplicată o politică pe computer, puteți alege depozitul de certificate care va fi utilizat de aplicațiile Mozilla. Dacă ați selectat depozitul de certificate Mozilla, adăugați manual un certificat Kaspersky. 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, Kaspersky Endpoint Security nu scanează traficul din browserul Mozilla Firefox și clientul de e-mail Thunderbird.

Înainte de a adăuga un certificat în depozitul Mozilla, exportați certificatul Kaspersky din Panoul de control Windows (proprietăți browser). Pentru detalii despre exportul certificatului Kaspersky, consultați Baza de cunoștințe a Suportului tehnic. Pentru detalii despre adăugarea unui certificat în depozit, accesați *site-ul web de asistență tehnică Mozilla*.

Puteți alege depozitul de certificate numai în interfața locală a aplicației.

Pentru a alege un depozit de certificate pentru scanarea conexiunilor criptate în Firefox și Thunderbird:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Setări de rețea**.
3. În blocul **Mozilla Firefox și Thunderbird**, bifați caseta de selectare **Scanează traficul sigur în aplicațiile Mozilla**.
4. Selectați un depozit de certificate:
   - **Utilizează depozitul de certificate Windows**. Certificatul rădăcină Kaspersky este adăugat la acest depozit în timpul instalării Kaspersky Endpoint Security.
   - **Utilizează depozitul de certificate Mozilla**. 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.
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 legată de muncă, puteți adăuga un site web la excluderile considerate *adrese de încredere*. 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.

Pentru a exclude o adresă Web de la scanarea conexiunilor criptate:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Setări de rețea**.
3. În secțiunea **Scanare conexiuni criptate**, faceți clic pe butonul **Adrese de încredere**.
4. Faceți clic pe butonul **Adăugare**.
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 `*` când introduceți masca unui nume de domeniu.

   Kaspersky Endpoint Security nu acceptă măști pentru adresele IP.

   Exemple:

   - `domain.com` – această intrare include următoarele adrese: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Această intrare include subdomenii (de

exemplu, `subdomain.domain.com`).

- `subdomain.domain.com` – această intrare include următoarele subdomenii: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Intrarea include domeniul `domain.com`.

- `*.domain.com` – această intrare include următoarele adrese: `https://movies.domain.com`, `https://images.domain.com/page123`. Intrarea include 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.

- 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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul .

2. În fereastra cu setările aplicației, selectați **Setări de rețea**.

3. În secțiunea **Scanare conexiuni criptate**, faceți 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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul .

2. În fereastra cu setările aplicației, selectați **Setări de rețea**.

3. În secțiunea **Scanare conexiuni criptate**, faceți clic pe linkul **site-uri web**.

   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.

Control Web

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 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).

Kaspersky Endpoint Security monitorizează doar traficul HTTP- și HTTPS.

Pentru monitorizarea traficului HTTPS, trebuie să activați scanarea conexiunilor securizate.

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 sociale” sau la alte categorii.
- **Tipul de date**. Puteți restricționa accesul utilizatorilor la datele de pe un site web și puteți ascunde imaginile grafice, 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 „Fișiere grafice”.

- **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, puteți restricționa accesul la tipul de date „Fișiere Office” doar pentru categoria de site-uri web „E-mail 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.

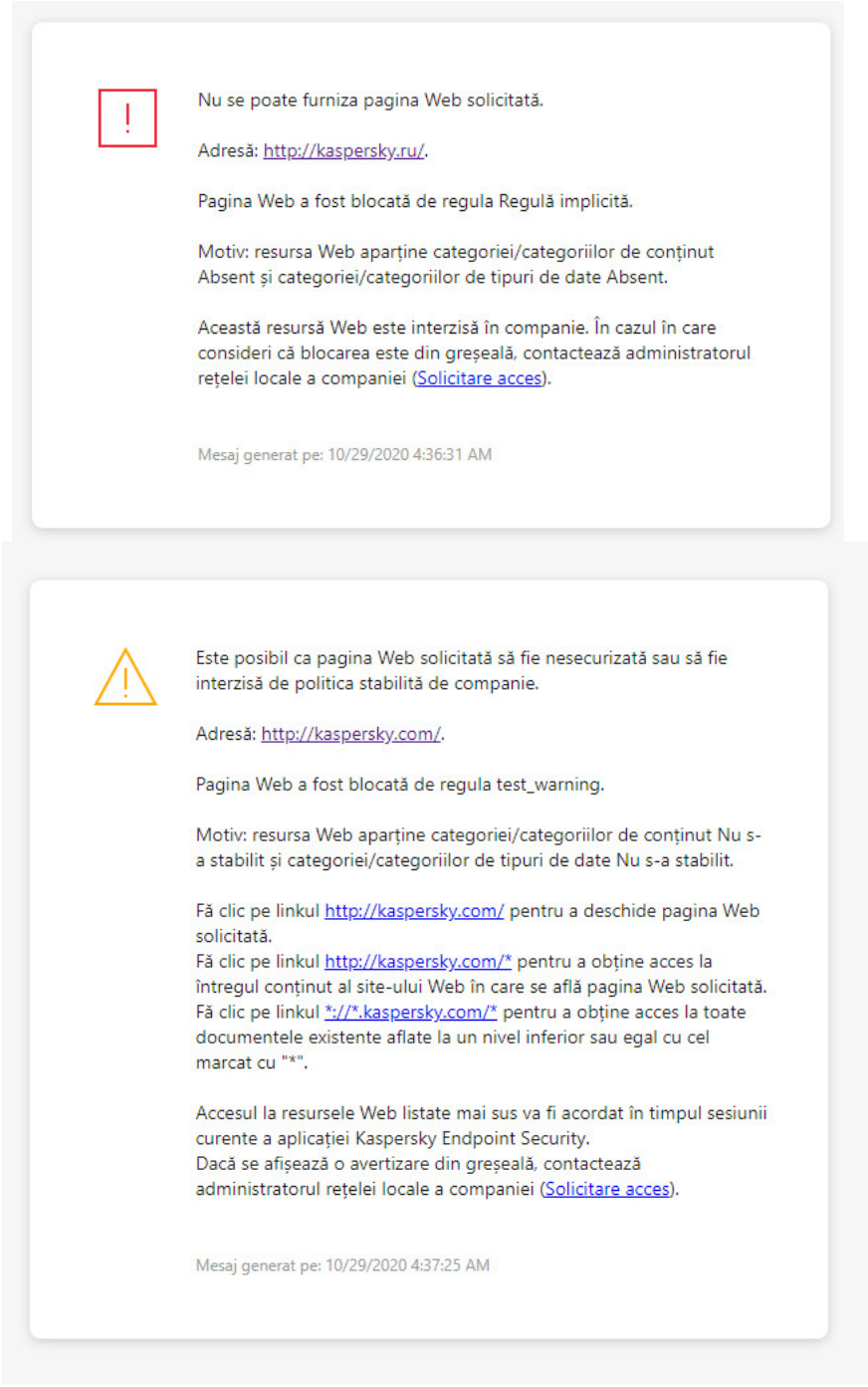
  De exemplu, puteți restricționa accesul la Internet printr-un browser pentru toți utilizatorii companiei, cu excepția departamentului IT.

- 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 sociale” 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

Activarea și dezactivarea componentei Control Web

Componenta Control Web este activată în mod implicit.

Pentru a activa sau a dezactiva componenta Control Web:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Control Web**.
3. Utilizați comutatorul de **Control Web** pentru a activa sau a dezactiva componenta.
4. Salvați-vă modificările.

Acțiuni asupra regulilor de acces la resurse Web

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. Două reguli sunt presetate:

- Regula Scripturi și foi de stil, care asigură tuturor utilizatorilor accesul permanent la resursele Web ale căror adrese conțin nume de fișiere cu extensia CSS, JS sau VBS. De exemplu: http://www.example.com/style.css, http://www.example.com/style.css?mode=normal.

- Regula implicită. 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.

Adăugarea unei reguli de acces la resursele web

Pentru a adăuga sau a edita o regulă de acces la resurse Web:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Control Web**.
3. În blocul **Setări**, faceți clic pe butonul **Reguli de acces la resurse Web**.
4. În fereastră, faceți clic pe butonul **Adăugare**.

   Se deschide fereastra **Regulă de acces la resurse Web**.
5. În câmpul **Nume regulă**, introduceți numele regulii.
6. Selectați starea **Activă** pentru regula de acces la resursele web.

   Puteți utiliza comutatorul pentru a dezactiva regula de acces la resursele web în orice moment.
7. În blocul **Acțiune**, selectați opțiunea relevantă:

   - **Permitere**. Dacă este selectată această valoare, Kaspersky Endpoint Security permite accesul la resurse Web care se potrivesc cu parametrii regulii.
   - **Blocare**. Dacă este selectată această valoare, Kaspersky Endpoint Security blochează accesul la resurse Web care se potrivesc cu parametrii regulii.
   - **Avertizare**. Dacă se selectați această valoare, atunci când utilizatorul încearcă să acceseze o resursă Web care corespunde regulii, Kaspersky Endpoint Security afișează o avertizare că resursa Web respectivă nu este recomandată. Utilizând linkuri din mesajul de avertizare, utilizatorul poate obține acces la resursa Web solicitată.
8. În blocul **Tip filtru**, selectați filtrul de conținut relevant:

   - **După categorii de conținut**. Puteți controla accesul utilizatorilor la resursele web după categorie (de exemplu, categoria *Rețele sociale*).
   - **După tipuri de date**. Puteți controla accesul utilizatorilor la resursele web pe baza tipului specific de date al datelor publicate (de exemplu, *imagini grafice*).

   Pentru a configura filtrul de conținut:

   a. Faceți clic pe linkul **Configurare**.

   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 **Adrese**, selectați filtrul de adrese de resurse web relevante:

   - **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. Pentru a crea o listă de adrese de resurse web:

     a. Faceți clic pe butonul **Adăugare adresă** sau **Adăugare grup de adrese**.

     b. În fereastra deschisă, creați 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.

     c. Reveniți la fereastră pentru configurarea regulii de acces la resursele web.

   Dacă este dezactivată opțiunea Scanare conexiuni criptate, pentru protocolul HTTPS puteți filtra doar după numele de server.

10. În blocul **Utilizatori**, selectați filtrul relevant pentru utilizatori:

    - **Pentru toți utilizatorii**. Control Web nu va filtra resursele web pentru anumiți utilizatori.
    - **Aplicare pentru utilizatorii individuali și/sau grupuri individuale**. Control Web va filtra resursele web numai pentru anumiți utilizatori. Pentru a crea o listă de utilizatori cărora doriți să le aplicați regula:

      a. Faceți clic pe butonul **Adăugare**.

      b. În fereastra deschisă, selectați utilizatorii sau grupul de utilizatori cărora doriți să le aplicați regula de acces la resursele web.

      c. Reveniți la fereastră pentru configurarea regulii de acces la resursele web.

11. În lista verticală **Planificare regulă**, selectați numele planificării necesare sau generează o planificare nouă bazată pe planificarea de regulă selectată. Pentru aceasta:

    a. Faceți clic pe butonul **Gestionare program**.

    b. În fereastră, faceți clic pe butonul **Adăugare**.

    c. În fereastra deschisă, introduceți numele programului regulilor.

    d. Configurați programul de acces la resurse web pentru utilizatori.

    e. Reveniți la fereastră pentru configurarea regulii de acces la resursele web.

12. Salvați-vă modificările.

Atribuirea de priorități regulilor de acces la resurse Web

Poți atribui priorități fiecărei reguli din lista de reguli aranjând regulile într-o anumită ordine.

Pentru a atribui o prioritate unei reguli de acces la resurse Web:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Control Web**.
3. În blocul **Setări**, faceți clic pe butonul **Reguli de acces la resurse Web**.
4. În fereastra deschisă, selectați regula a cărei prioritate doriți să o modificați.
5. Utilizați butoanele **Sus** și **Jos** pentru a muta regula în poziția relevantă din lista de reguli de acces la resursele web.
6. Salvați-vă modificările.

Activarea și dezactivarea unei reguli de acces la resurse Web

Pentru a activa sau a dezactiva o regulă de acces la resurse Web:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Control Web**.
3. În blocul **Setări**, faceți clic pe butonul **Reguli de acces la resurse Web**.
4. În fereastra deschisă, selectați regula pe care doriți să o activați sau să o dezactivați.
5. În coloana **Stare**, efectuați următoarele:
   - Dacă doriți să activați utilizarea regulii, selectați valoarea **Activă**.
   - Dacă doriți să dezactivați utilizarea regulii, selectați valoarea **Inactivă**.
6. Salvați-vă modificările.

Exportul și importul listei de adrese URL de încredere

Puteți exporta lista de reguli Web Policy Management într-un fișier XML. 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 Web Policy Management sau pentru a migra lista pe un alt server.

Cum se exportă și se importă o listă de reguli Web Policy Management în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Security Controls** → **Web Policy Management**.
6. Pentru a exporta lista de reguli Web Policy Management:
   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 **Exportare**.
   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. Faceți clic pe butonul **Save**.
      Kaspersky Endpoint Security exportă lista de reguli în fișierul XML.
7. Pentru a importa lista de reguli Web Policy Management:
   a. Faceți clic pe linkul **Importare**.
      În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de reguli.
   b. Faceți clic pe butonul **Deschidere**.
      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 Web Policy Management în Consola Web și Cloud Console

1. În fereastra principală a Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security pentru computerele pe care doriți să exportați sau să importați lista de reguli.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Accesați **Security Controls** → **Web Policy Management**.
5. Pentru a exporta lista de reguli, în blocul **Listă de reguli**:
   a. Selectați regulile pe care doriți să le exportați.
   b. Faceți clic pe butonul **Export**.
   c. Confirmați că doriți să exportați numai regulile selectate sau să exportați întreaga listă.
   d. Faceți clic pe butonul **Export**.

      Kaspersky Endpoint Security exportă lista de reguli într-un fișier XML în directorul de descărcări implicit.
6. Pentru a importa lista de reguli, în blocul **Listă de reguli**:
   a. Faceți clic pe linkul **Importare**.

      În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de reguli.
   b. Faceți clic pe butonul **Deschidere**.

      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.
7. Salvați-vă modificările.

Testarea regulilor de acces la resurse Web

Pentru a verifica consistența regulilor componentei Control Web, ai posibilitatea să le testezi. În acest scop, componenta Control Web include o funcție Diagnosticare reguli.

Pentru a testa regulile de acces la resurse Web:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Control Web**.
3. În blocul **Setări**, faceți clic pe linkul **Diagnosticare reguli**.

   Se deschide fereastra **Diagnosticare reguli**.
4. Dacă dorești să testezi regulile pe care aplicația Kaspersky Endpoint Security le utilizează pentru a controla accesul la o anumită resursă Web, bifați caseta de selectare **Specifică adresa** și 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 **Filtrare conținut** 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. Faceți clic pe butonul **Test**.

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 butonul **Test**. Tabloul de mai jos prezintă regulile de declanșare rămase, specificând acțiunea luată de Kaspersky Endpoint Security. Regulile sunt listate în ordine descrescătoare a priorității.

Exportul și importul unei liste de adrese de resurse 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 .txt. 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.

Pentru a importa sau exporta o listă de adrese de resurse web într-un fișier:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Control Web**.

3. În blocul **Setări**, faceți 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. Faceți clic pe butonul **Export**.

   c. În fereastra deschisă, introduceți numele fișierului TXT în care doriți să exportați lista de adrese de resurse web și selectați folderul în care doriți să salvați acest fișier.

   d. Faceți clic pe butonul **Save**.

      Kaspersky Endpoint Security exportă lista de adrese de resurse web într-un fișier TXT.

6. Pentru a importa lista resurselor web, efectuați următoarele în blocul **Adrese**:

   a. Faceți clic pe butonul **Import**.

În fereastra care se deschide, selectați fișierul TXT din care doriți să importați lista de resurse web.

b. Faceți clic pe butonul **Deschidere**.

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.

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.

Kaspersky Endpoint Security creează următoarele evenimente de activitate pe Internet a utilizatorilor:

- Blocare site web (starea *Evenimente critice*).
- Vizitarea unui site web nerecomandat (stare *Avertismenter)*).
- Vizită pe un site web permis (stare *Mesaje de informare*).

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.

Pentru a injecta un script de interacțiune a paginii web în traficul web:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul .
2. În fereastra cu setările aplicației, selectați **Setări de rețea**.
3. În blocul **Procesare trafic**, bifați caseta de selectare **Injectare script de interacțiune în trafic**.
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.

Pentru a configura înregistrarea în jurnal a evenimentelor componentei Control Web pe computerul utilizatorului:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul .
2. În fereastra de setări a aplicației, selectați secțiunea **Interfață**.

3. În blocul **Notificări**, faceți clic pe butonul **Reguli de notificare**.

4. În fereastra deschisă, selectați secțiunea **Control Web**.

   Aceasta deschide tabelul evenimentelor componentei Control Web și a metodelor de notificare.

5. Configurați metoda de notificare pentru fiecare eveniment: **Salvare în raport local** sau **Salvare 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, lWeb 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 și http://www.example.com/gallery, Kaspersky Endpoint Security va trimite un singur eveniment cu obiectul http://www.example.com.

Pentru a activa înregistrarea în jurnal a evenimentelor pentru vizitarea site-urilor web permise:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Control Web**.

3. În blocul **Suplimentar**, faceți clic pe butonul **Setări avansate**.

4. În fereastra deschisă, bifați caseta de selectare **Jurnalizați deschiderea paginilor permise**.

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 **Avertizare** este selectată din lista verticală **Acțiune** din cadrul setărilor regulii care descrie resursa Web respectivă.

  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 dacă opțiunea **Blocare** este selectată din lista verticală **Acțiune** din cadrul setările regulii care descrie resursa Web respectivă.

  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 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. Poți modifica conținutul acestora.

Pentru a modifica șablonul pentru mesajele componentei Control Web:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Control Web**.
3. În blocul **Șabloane**, configurați șabloanele pentru mesajele Control Web:
   - **Avertizări**. 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.
   - **Blocare**. Câmpul de intrare conține șablonul mesajului care apare dacă se declanșează o regulă care blochează accesul la o resursă Web.
   - **Mesaj către administrator**. Câmpul de intrare conține șablonul de mesaj care va fi trimis administratorului rețelei LAN în cazul în care utilizatorul consideră că blocarea s-a făcut din greșeală.
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 `imagini.`

- `http://user.pictures.example.com`. Masca de domeniu `*.` reprezintă `imagini.` și `utilizator.`
- `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.

Migrarea regulilor de acces la resurse Web de la versiuni anterioare ale aplicației

Atunci când se face upgrade de la Kaspersky Endpoint Security 10 Service Pack 2 for Windows sau o versiune anterioară a aplicației la Kaspersky Endpoint Security for Windows, regulile de acces la resurse Web bazate pe categorii de conținut pentru resurse Web sunt migrate după cum urmează:

- Regulile de acces la resurse Web care sunt bazate pe una sau mai multe categorii de conținut pentru resurse Web din listele „Chaturi și forumuri”, „E-mail pe Web” și „Rețele de socializare” migrează în categoria de conținut pentru resurse Web „Comunicare pe internet”.
- Regulile de acces la resurse Web bazate pe una sau mai multe categorii de conținut pentru resurse Web din listele „Magazine electronice” și „Sisteme de plată” migrează în categoria de conținut pentru resurse Web „Magazine online, bănci, sisteme de plată”.
- Regulile de acces la resurse Web bazate pe categoria de conținut pentru resurse Web „Jocuri de noroc” migrează în categoria de conținut „Jocuri de noroc, loterii, pronosport”.
- Regulile de acces la resurse Web bazate pe categoria de conținut pentru resurse Web „Jocuri în browser” migrează în categoria de conținut „Jocuri pe computer”.
- Regulile de acces la resurse Web bazate pe categorii de conținut pentru resurse Web care nu sunt cuprinse în lista de mai sus sunt migrate fără a se efectua modificări.

Control dispozitive

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 dispozitive gestionează accesul utilizatorilor la dispozitivele instalate sau conectate la computer (de exemplu, hard diskuri, camere video sau module Wi-Fi). Acest lucru îți permite să protejezi computerul de infecții atunci când sunt conectate astfel de dispozitive și să împiedici pierderea sau scurgerea de date.

Nivelurile de acces ale dispozitivului

Componenta Control dispozitive controlează accesul la următoarele niveluri:

- **Tip dispozitiv**. De exemplu, imprimante, unități amovibile și unități CD/DVD.

  Poți configura accesul la dispozitive după cum urmează:

  - Permitere – .
  - Blocare – .
  - Depinde de magistrala de conectare (exceptând Wi-Fi) – .
  - Blocare cu excepții (numai Wi-Fi) – .

- **Magistrală de conectare**. O *magistrală de conectare* este o interfață utilizată pentru conectarea dispozitivelor la computer (de exemplu, USB sau FireWire). Prin urmare, poți restricționa conectarea tuturor dispozitivelor, de exemplu, prin USB.

  Poți configura accesul la dispozitive după cum urmează:

  - Permitere – .
  - Blocare – .

- **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 de model**. 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.

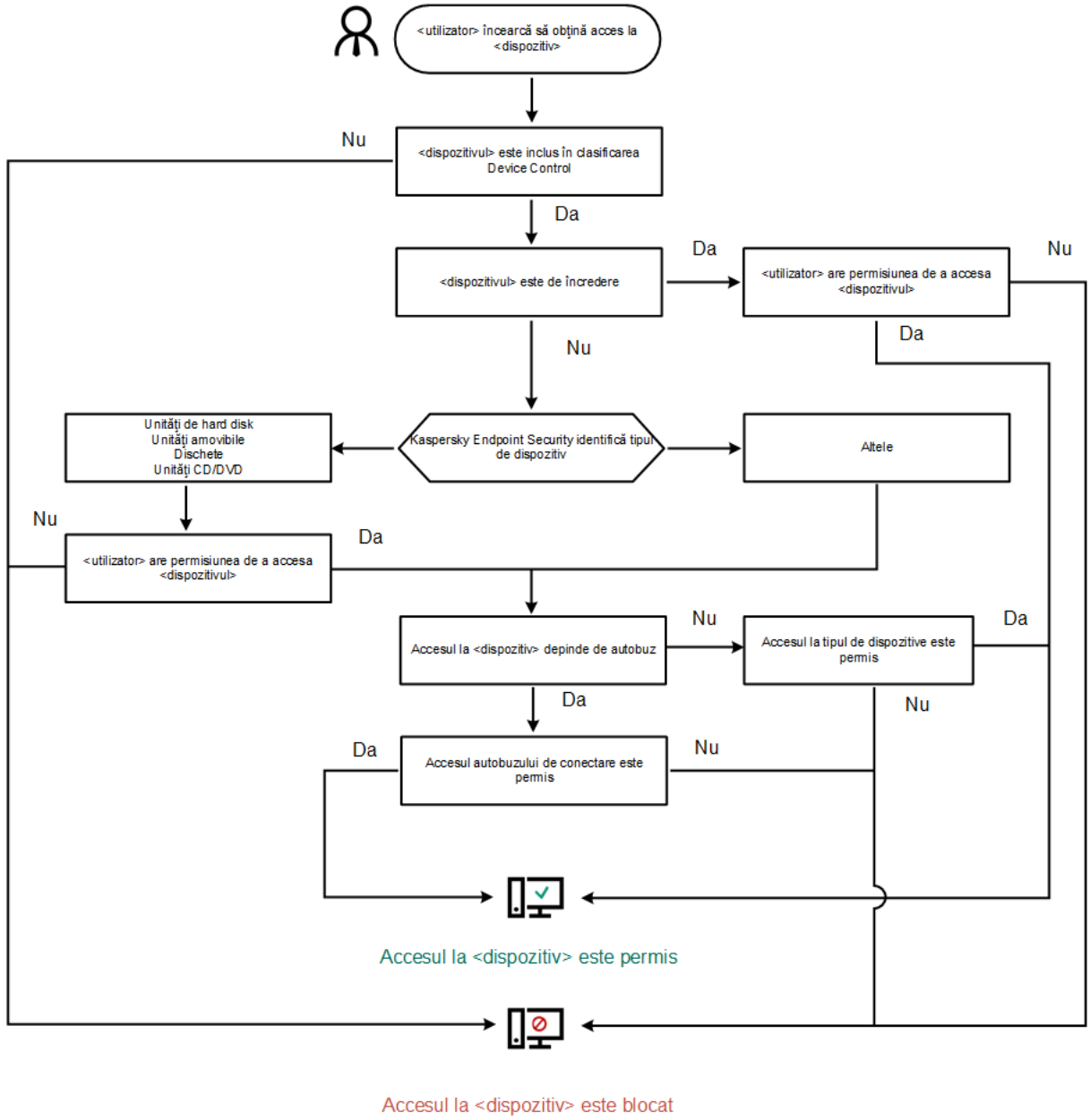
Dacă accesul la un dispozitiv depinde de magistrala de conectare (starea), Kaspersky Endpoint Security nu salvează evenimente de conectare/deconectare a dispozitivului. Pentru a permite Kaspersky Endpoint Security să salveze evenimente de conectare/deconectare a dispozitivului, permite accesul la tipul 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.

Activarea și dezactivarea componentei Control dispozitive

Componenta Control dispozitive este activată în mod implicit.

Activarea sau dezactivarea componentei Control dispozitive:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Control dispozitive**.

3. Utilizați comutatorul **Control dispozitive** pentru a activa sau dezactiva componenta.

4. Salvați-vă modificările.

Ca urmare, dacă Controlul dispozitivelor este activat, aplicația transmite informații despre dispozitivele conectate la Kaspersky Security Center. Puteți vizualiza lista dispozitivelor conectate în Kaspersky Security Center în directorul **Hardware**.

Despre regulile de acces

Regulile de acces cuprind un grup de setări care determină care utilizatori pot accesa dispozitive instalate sau conectate la computer. 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	✓	✓	✓	✓	✓
Imprimante	✓	–	–	–	–
Dischete	✓	✓	✓	✓	✓
Unități CD/DVD	✓	✓	✓	✓	✓
Modemuri	✓	–	–	–	–
Dispozitive cu bandă	✓	–	–	–	–
Dispozitive multifuncționale	✓	–	–	–	–
Cititoare de carduri inteligente	✓	–	–	–	–
Dispozitive Windows CE USB ActiveSync	✓	–	–	–	–
Plăci de rețea externe	✓	–	–	–	–
Dispozitive portabile (MTP)	✓	✓	✓	✓	✓
Bluetooth	✓	–	–	–	–

Camere și scanere	✓	–	–	–	–

Reguli de acces la dispozitive mobile

Dispozitivele mobile pe care se execută Android sau iOS sunt clasificate ca dispozitive 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.

Vă rugăm să rețineți următoarele considerații speciale cu privire la accesul la dispozitivele ADB- sau iTunes:

- Nu puteți configura o planificare de acces la dispozitiv. Dacă accesul la dispozitive este restricționat de reguli (acestea au starea), dispozitivele ADB- și iTunes sunt întotdeauna accesibile.
- Nu puteți configura accesul la dispozitiv pentru utilizatori individuali sau permisiunile de acces (citire/scriere). Dacă accesul la dispozitive este restricționat de reguli (acestea au starea), dispozitivele ADB- și iTunes sunt accesibile tuturor utilizatorilor cu toate permisiunile.
- Nu puteți configura accesul la dispozitivele ADB- sau iTunes de încredere pentru utilizatori individuali. Dacă dispozitivul este de încredere, dispozitivele ADB- și iTunes sunt accesibile tuturor utilizatorilor.
- 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.

În mod implicit, regulile de acces acordă tuturor utilizatorilor acces complet și în orice moment la dispozitive dacă accesul la magistralele de conectare pentru tipurile de dispozitive respective este permis (starea).

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

Regulile de acces la magistrale de conectare determină dacă conectarea dispozitivelor este permisă (starea ✓) sau interzisă (starea ⊘). În mod implicit, se creează reguli care permit accesul la magistrale pentru toate magistralele de conectare prezente în clasificarea componentei Control dispozitive.

Editarea unei reguli de acces la dispozitive

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.

Pentru a edita o regulă de acces la dispozitive:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Control dispozitive**.

3. În blocul **Configurare acces**, faceți 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 dispozitive de stocare**, selectați regula de acces pe care doriți să o editați. Blocul conține dispozitive care au un sistem de fișiere pentru care puteți configura setări suplimentare de acces. În mod implicit, o regulă de acces la dispozitive acordă tuturor utilizatorilor acces permanent la tipul de dispozitive specificat.

   a. În blocul **Acces**, selectați opțiunea de acces corespunzătoare a dispozitivului:

      - **Permitere**.
      - **Blocare**.
      - **Depinde de magistrala de conectare**.

        Pentru a bloca sau a permite accesul la un dispozitiv, configurați accesul la magistrala de conexiune.

      - **Restricționat de reguli**.

        Această opțiune vă permite să configurați drepturile utilizatorului, permisiunile și un program pentru accesul la dispozitiv.

   b. În secțiunea **Drepturile utilizatorilor**, faceți clic pe butonul **Adăugare**.

      Aceasta deschide o fereastră pentru adăugarea unei noi reguli de acces la dispozitiv.

   c. Atribuiți o prioritate noii *reguli*. 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 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.

   d. Selectați starea **Activată** pentru regula de acces la dispozitiv.

   e. Configurați permisiunile utilizatorilor de acces la dispozitiv: citire și/sau scriere.

   f. Selectați utilizatorii sau grupul de utilizatori cărora doriți să le aplicați regula de acces la dispozitiv.

   g. Configurați un program de acces la dispozitiv pentru utilizatori.

   h. Faceți clic pe butonul **Adăugare**.

5. În blocul **Acces la dispozitivele externe**, selectați regula și configurați accesul: **Permitere**, **Refuzare** sau **În funcție de magistrala de conectare**. Dacă este necesar, configurați accesul la magistrala de conectare.

6. În blocul **Acces la rețelele Wi-Fi**, faceți clic pe linkul **Wi-Fi** și configurați accesul: **Permitere**, **Bloare** sau **Blocare cu excepții**. Dacă este necesar, adăugați rețele Wi-Fi la lista de încredere.

7. Salvați-vă modificările.

Editarea unei reguli de acces la magistrale de conectare

Pentru a edita o regulă de acces la magistrale de conectare:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Control dispozitive**.

3. În blocul **Setări**, faceți 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: **Permitere** sau **Refuzare**.

6. Salvați-vă modificările.

Adăugarea unei rețele Wi-Fi la lista de încredere

Poți permite utilizatorilor să se conecteze la rețele Wi-Fi pe care le consideri a fi sigure, cum ar fi o rețea Wi-Fi de companie. Pentru aceasta, trebuie să adaugi rețea la lista de rețele Wi-Fi de încredere. Component Control dispozitive va bloca accesul la toate rețelele Wi-Fi, cu excepția celor specificate în lista de încredere.

Pentru a adăuga o rețea Wi-Fi la lista de încredere:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Control dispozitive**.

3. În blocul **Setări**, faceți clic pe butonul **Reguli de acces pentru 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.

5. În coloana **Acces**, selectați **Blocare cu excepții**.

6. Faceți clic pe butonul **Adăugare** din blocul **Rețea Wi-Fi de încredere**.

7. În fereastra deschisă, efectuați una dintre următoarele acțiuni:

   a. În câmpul **Nume rețea**, specifică numele rețelei Wi-Fi pe care dorești s-o adaugi în lista de încredere.

b. În lista verticală **Tip autentificare**, selectați tipul de autentificare folosită la conectarea la rețeaua Wi-Fi de încredere.

c. În lista verticală **Tip criptare**, selectați tipul de criptare folosită pentru securizarea traficului prin rețeaua Wi-Fi de încredere.

d. În câmpul **Comentariu** poți specifica orice informație despre rețeaua Wi-Fi adăugată.

O rețea Wi-Fi este considerată a fi de încredere dacă setările sale corespund tuturor setărilor specificate în regulă.

8. Salvați-vă modificările.

Monitorizarea utilizării unităților amovibile

Pentru a permite monitorizarea utilizării unității amovibile:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Control dispozitive**.
3. În blocul **Setări**, faceți clic pe butonul **Reguli de acces pentru 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 dispozitive de stocare**, selectați **Unități amovibile**.
5. Faceți clic pe linkul **Înregistrare în jurnal**.
6. În fereastra deschisă, selectați fila **Înregistrare în jurnal**.
7. Activați comutatorul **Înregistrare în jurnal**.
8. În blocul **Operații cu fișiere**, selectați operațiile pe care doriți să le monitorizați: **Scriere**, **Ștergere**.
9. În blocul **Filtrare după formate de fișiere**, selectați formatele fișierelor ale căror operațiuni asociate ar trebui înregistrate de Control dispozitive.
10. Selectați utilizatorii sau grupul de utilizatori a căror utilizare a unităților amovibile care doriți să o monitorizați.
11. 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 **Server de administrare** din fila **Evenimente**. Pentru ca evenimentele să fie afișate în jurnalul de evenimente Kaspersky Endpoint Security local, trebuie să bifezi caseta de selectare **S-a efectuat o operație 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
- Verdict de autorizare a cererii pentru această acțiune: permis sau refuzat
- 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.

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 are următoarele limitări atunci când lucrează cu dispozitive de încredere:

- Versiunile plug-inului de administrare Kaspersky Endpoint Security 11.0.0 – 11.2.0 nu pot funcționa cu o listă de dispozitive de încredere care a fost creată în Kaspersky Endpoint Security versiunea 11.3.0 și 11.4.0. Pentru a lucra cu o listă de dispozitive de încredere din aceste versiuni, plug-inul de administrare trebuie să fie actualizat la versiunea 11.3.0 și, respectiv, 11.4.0.

- Plug-inurile de administrare Kaspersky Endpoint Security versiunea 11.3.0 și 11.4.0 nu pot funcționa cu o listă de dispozitive de încredere care a fost creată în Kaspersky Endpoint Security versiunea 11.2.0 sau una anterioară. Pentru ca aceste versiuni să funcționeze cu o listă de dispozitive de încredere, aplicația trebuie să fie actualizată la versiunea 11.3.0 și, respectiv, 11.4.0. De asemenea, puteți trimite o cerere care conține o descriere a situației dvs. către Suportul tehnic prin intermediul Kaspersky CompanyAccount.

- Pentru a migra o listă de dispozitive de încredere de la Kaspersky Endpoint Security versiunea 11.2.0 la versiunea 11.3.0, trimiteți o cerere care conține o descriere a situației dvs. către Suportul tehnic prin intermediul Kaspersky CompanyAccount.

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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul .
2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Control dispozitive**.
3. În blocul **Setări**, faceți clic pe butonul **Dispozitive de încredere**.

   Aceasta deschide lista dispozitivelor de încredere.
4. Faceți clic pe butonul **Selectare**.

   Aceasta deschide lista dispozitivelor conectate. Lista de dispozitive depinde de valoarea selectată în lista verticală **Afișare dispozitive conectate**.
5. În lista de dispozitive, selectați dispozitivul pe care doriți să îl adăugați la lista de încredere.

6. În câmpul **Comentariu**, puteți furniza orice informații relevante despre dispozitivul de încredere.

7. Selectați utilizatorii sau grupul de utilizatori pentru care doriți să permiteți accesul la dispozitive de încredere.

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 de model**. 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_ *`.

Pentru a adăuga un dispozitiv la lista de dispozitive de încredere:

1. Deschide Consolă de administrare a Kaspersky Security Center.

2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.

3. În spațiul de lucru, selectați fila **Politici**.

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

5. În fereastra politicii, selectați **Security Controls → Control dispozitive** .

6. În partea dreaptă a ferestrei, selectați fila **Dispozitive de încredere**.

7. Bifați caseta de selectare **Îmbinare valori 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.

8. Faceți clic pe butonul **Adăugare** și selectați o metodă pentru adăugarea unui dispozitiv în lista de încredere.

9. Pentru a filtra dispozitivele, selectați un tip de dispozitiv din lista verticală **Tip dispozitiv** (de exemplu, **Unități amovibile**).

10. În câmpul **Nume/Model**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 **Reîmprospătare**. Pentru a afișa corect lista dispozitivelor, puteți adăuga dispozitive după masca de ID a dispozitivului.

11. 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.

12. Faceți clic pe butonul **Împrospătare**.

    Tabelul afișează o listă de dispozitive care îndeplinesc criteriile de filtrare definite.

13. Bifați caseta de selectare de lângă numele dispozitivelor pe care doriți să le adăugați în lista de încredere.

14. În câmpul **Comentariu**, introduceți o descriere a motivului pentru adăugarea dispozitivelor în lista de încredere.

15. Faceți clic pe butonul **Selectare** din dreapta câmpului **Permitere pentru utilizatorii și/sau grupurile de utilizatori**.

16. Selectați un utilizator sau un grup în Active Directory și confirmă selecția.

    În mod implicit, accesul la dispozitivele de încredere este permis pentru grupul Toți.

17. 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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Control dispozitive**.

3. În blocul **Setări**, faceți 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. Faceți clic pe butonul **Export**.

   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. Faceți clic pe butonul **Save**.

      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 **Importare**, 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. Faceți clic pe butonul **Deschidere**.

      În cazul în care computerul are deja o listă de dispozitive de încredere, Kaspersky Endpoint Security vă va solicita să ștergeți lista existentă sau să adăugați noi intrări la acesta din fișierul XML.

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.

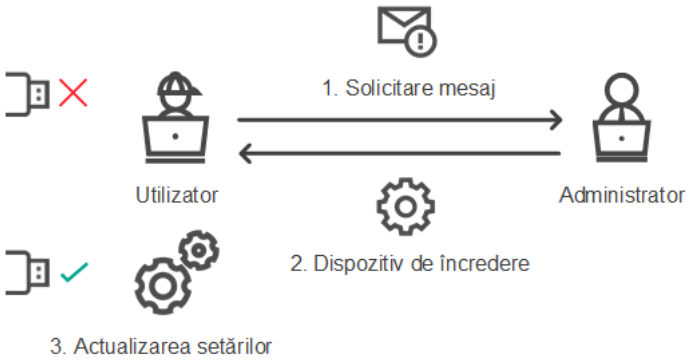
Modul online pentru acordarea accesului

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 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.
3. 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 **Permitere solicitări de acces 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 fereastra **Mesaj al administratorului**. Acest mesaj conține informații despre dispozitivul blocat.

3. Faceți clic pe butonul **Trimitere**.

Administratorul va primi un mesaj care conține o solicitare pentru a oferi acces, de exemplu, prin e-mail. Pentru mai multe detalii despre procesarea solicitărilor utilizatorilor, consultați *Ajutor pentru Kaspersky Security Center* . După adăugarea dispozitivului la lista de încredere și actualizarea setărilor Kaspersky Endpoint Security pe computer, utilizatorul va 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 **Permitere solicitări de acces 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**.

   Fereastra **Solicitare acces la dispozitive** se deschide cu o listă de dispozitive conectate.

3. Din lista de dispozitive conectate, selectați dispozitivul la care doriți să obțineți acces.

4. Faceți clic pe butonul **Generare 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

Administratorul creează o cheie de acces pentru un dispozitiv blocat, după cum urmează:

1. Deschide Consolă de administrare a Kaspersky Security Center.

2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparține computerul client relevant.

3. În spațiul de lucru, selectați fila **Dispozitive**.

4. În lista de computere client, selectați computer al cărui utilizator trebuie să primească acces temporar la un dispozitiv blocat.

5. În meniul contextual al computerului, selectați opțiunea **Acordă acces în modul offline**.

6. În fereastra deschisă, selectați fila **Control dispozitive**.

7. Faceți clic pe butonul **Răsfoire** 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.

    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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Control dispozitive**.

3. În blocul **Solicitare acces**, faceți clic pe butonul **Solicitare acces la dispozitive**.

4. În fereastra deschisă, faceți clic pe butonul **Activare cheie de acces**.

5. În fereastra deschisă, selectați fișierul cu cheia de acces pentru dispozitiv primit de la administratorul rețelei LAN corporative. Faceți clic pe butonul **Deschidere**.

   Aceasta deschide o fereastră care conține informații despre furnizarea accesului.

6. Faceți 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. 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.

Sunt disponibile șabloane pentru mesaje de reclamație și șabloane pentru mesajele despre accesul blocat la dispozitive sau despre operațiunile interzise cu conținutul dispozitivului și pentru mesajul trimis către administrator. Poți modifica șabloanele de mesaje.

Pentru a edita șabloanele pentru mesajele componentei Control dispozitive:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Control dispozitive**.
3. În blocul **Șabloane**, configurați șabloanele pentru mesajele Control dispozitive:
   - **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.
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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Control dispozitive**.
3. În blocul **Setări**, faceți clic pe butonul **Anti-Bridging**.
4. Utilizați comutatorul **Activare Anti-Bridging** pentru a activa sau 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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Control dispozitive**.
3. În blocul **Setări**, faceți 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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Control dispozitive**.
3. În blocul **Setări**, faceți 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 anomalie adaptivă

Această componentă este disponibilă numai pentru Kaspersky Endpoint Security for Business Advanced și Kaspersky Total Security for Business. Pentru mai multe detalii despre Kaspersky Endpoint Security for Business, vizitați *site-ul web Kaspersky*.

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 necaracteristic (de exemplu, regula *Pornire Microsoft PowerShell din aplicația de birou*). 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 Raport declanșare regulă și în depozitul **Declanșarea regulilor în modul Instruire inteligentă**.

2. Analizarea raportului declanșării regulii.

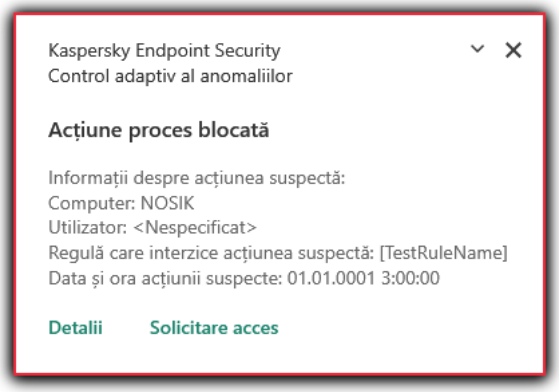
   Administratorul analizează raportul declanșării regulii sau conținutul depozitului **Declanșarea regulilor în modul Instruire inteligentă**. Apoi, administratorul poate selecta comportamentul componentei Control adaptiv al anomaliilor atunci când regula este declanșată: să o blocheze sau să o accepte. 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. Componenta Control adaptiv al anomaliilor este configurată prin următoarele metode:

- Componenta Control adaptiv al anomaliilor începe automat să blocheze acțiunile asociate regulilor 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 de declanșare a regulilor și conținutul depozitului **Declanșarea regulilor în modul Instruire inteligentă**.

Se recomandă analizarea raportului declanșării regulii sau conținutul depozitului **Declanșarea regulilor în modul Instruire inteligentă**.

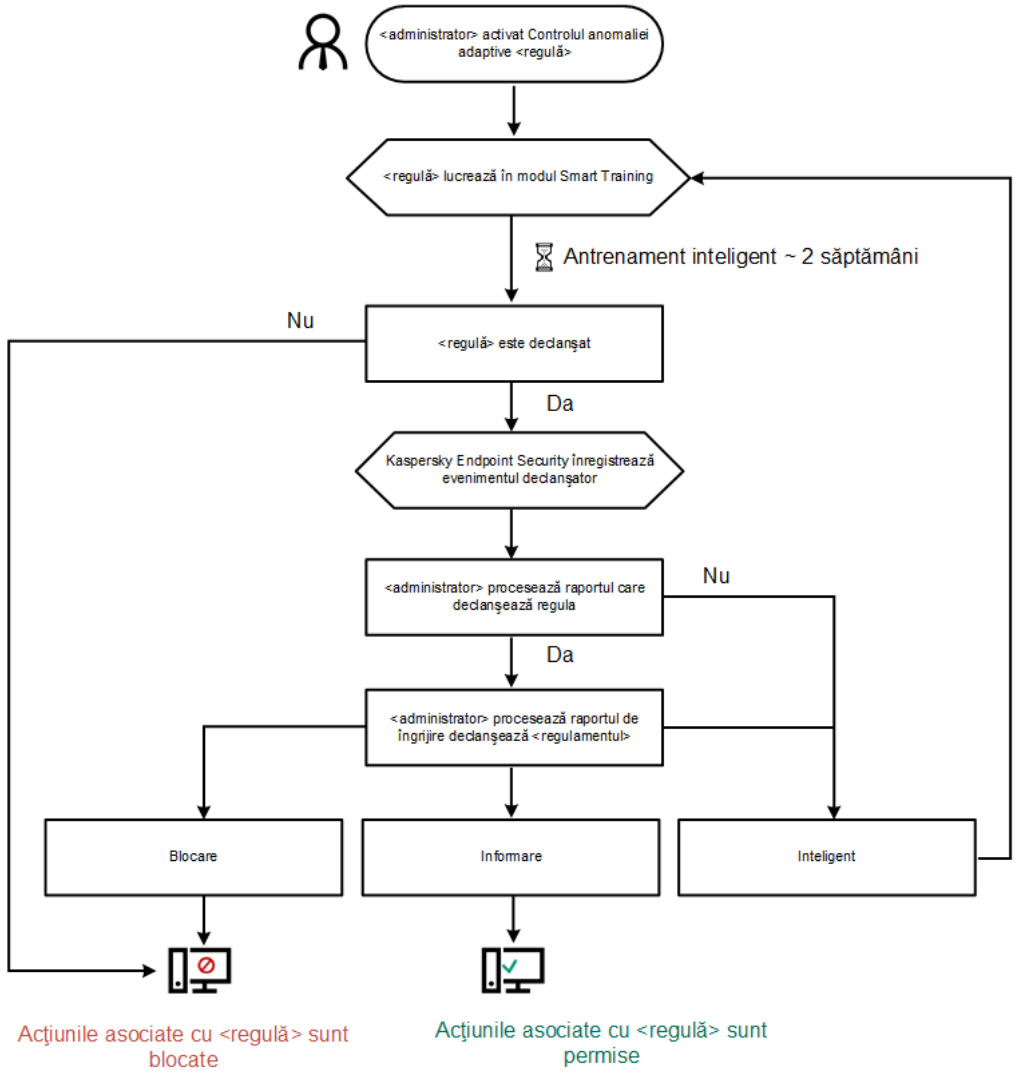
Când o aplicație periculoasă încearcă să efectueze o acțiune, Kaspersky Endpoint Security va bloca acțiunea și va afișa o notificare (consultați figura de mai jos).



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

Activarea și dezactivarea componentei Control adaptiv al anomaliilor

Componenta Control adaptiv al anomaliilor este activată în mod implicit.

Pentru a activa sau a dezactiva componenta Control adaptiv al anomaliilor:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Control adaptiv al anomaliilor**.
3. Utilizați comutatorul **Control adaptiv al anomaliilor** pentru a activa sau dezactiva componenta.
4. Salvați-vă modificările.

Activarea și dezactivarea unei reguli Control adaptiv al anomaliilor

Pentru a activa sau a dezactiva o regulă Control adaptiv al anomaliilor:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Control adaptiv al anomaliilor**.
3. În blocul **Reguli**, faceți clic pe butonul **Editare reguli**.
   Se deschide lista regulilor de control adaptiv al anomaliilor.
4. În tabel, selectați un set de reguli (de exemplu, *Activitatea aplicațiilor pentru birou*) și extindeți setul.
5. Selectați o regulă (de exemplu, Start *Windows PowerShell din aplicațiile Office*).
6. Utilizați comutatorul din coloana **Stare** pentru a activa sau a dezactiva regula de 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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Control adaptiv al anomaliilor**.
3. În blocul **Reguli**, faceți clic pe butonul **Editare reguli**.
   Se deschide lista regulilor de control adaptiv al anomaliilor.
4. Selectați o regulă din tabel.

5. Faceți clic pe butonul **Editare**.

   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 modul 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 introduce o înregistrare în depozitul **Declanșarea regulilor în modul instruire inteligentă** al serverului de administrare Kaspersky Security Center. Atunci când perioada de timp setată pentru activitatea în modul 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.

   - **Blocare**. 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.

   - **Informare**. 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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Control adaptiv al anomaliilor**.

3. În blocul **Reguli**, faceți clic pe butonul **Editare reguli**.

   Se deschide lista regulilor de control adaptiv al anomaliilor.

4. Selectați o regulă din tabel.

5. Faceți clic pe butonul **Editare**.

   Se deschide fereastra de proprietăți a regulii de control adaptiv al anomaliilor.

6. În blocul **Excluderi**, faceți clic pe butonul **Adăugare**.

Se deschide fereastra de proprietăți ale excluderii.

7. Selectați utilizatorul pentru care dorești să configurezi o excludere.

   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**. Cod hash fișier.
   - **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. Specifică obiectul în conformitate cu următorul șablon: `object://<obiect>,` unde `<obiect>` 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**. Cod hash fișier.

   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**. Cod hash fișier.
    - **Obiect țintă**. Comanda pentru pornirea procesului țintă. Specificați comanda utilizând următorul model `obiect://<comandă>`, de exemplu, `object://cmdline:powershell -Command "$result = 'C:\windows\temp\result_local_users_pwdage txt'"`. Puteți utiliza, de asemenea, măști, de exemplu, `obiect://*C:\windows\temp\*`.
    - **Cod hash obiect țintă**. Cod hash fișier.

    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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Control adaptiv al anomaliilor**.
3. În blocul **Reguli**, faceți clic pe butonul **Editare reguli**.
   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. Faceți clic pe butonul **Export**.
   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. Faceți clic pe butonul **Save**.
5. Pentru a importa lista de reguli:
   a. Faceți clic pe butonul **Import**.
   b. În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de excluderi.
   c. Faceți clic pe butonul **Deschidere**.
      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 *Dezactivat*. Nu este posibilă modificarea setărilor acestor reguli.

Pentru a aplica actualizări pentru reguli Control adaptiv al anomaliilor:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Control adaptiv al anomaliilor**.

3. În blocul **Reguli**, faceți clic pe butonul **Editare reguli**.

   Se deschide lista regulilor de control adaptiv al anomaliilor.

4. În fereastra deschisă, faceți clic pe butonul **Aprobare actualizări**.

   Butonul **Aprobare actualizări** 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 mesajul privind blocarea acțiunilor potențial dăunătoare și pentru ca mesajul să fie trimis administratorului. Poți modifica șabloanele de mesaje.

Pentru a edita un șablon de mesaj:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul .

2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Control adaptiv al anomaliilor**.

3. În blocul **Șabloane**, configurați șabloanele pentru mesajele Control adaptiv al anomaliilor:

   - **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.

4. Salvați-vă modificările.

Vizualizarea rapoartelor componentei Control adaptiv al anomaliilor

Pentru a vizualiza rapoarte Control adaptiv al anomaliilor:

1. Deschide Consolă de administrare a Kaspersky Security Center.

2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.

3. În spațiul de lucru, selectați fila **Politici**.

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

5. În secțiunea **Control endpoint**, selectați subsecțiunea **Control adaptiv al anomaliilor**.

Setările componentei Control adaptiv al anomaliilor sunt afișate în partea dreaptă a ferestrei.

6. Efectuează una dintre următoarele acțiuni:

   - Dacă vrei să vizualizezi un raport despre regulile Control adaptiv al anomaliilor, faceți clic pe butonul **Raport stare reguli**.
   - Dacă vrei să vizualizezi un raport despre declanșarea regulilor Control adaptiv al anomaliilor, faceți clic pe butonul **Raport declanșare reguli**.

7. Începe procesul de generare a raportului.

Raportul este afișat într-o fereastră nouă.

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*), hash-ul de fișiere, vânzătorul aplicației 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.

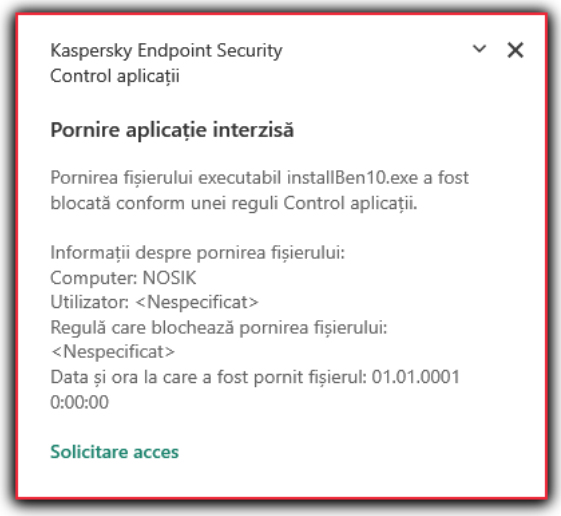
3. Selectarea modului Application Control.

   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.

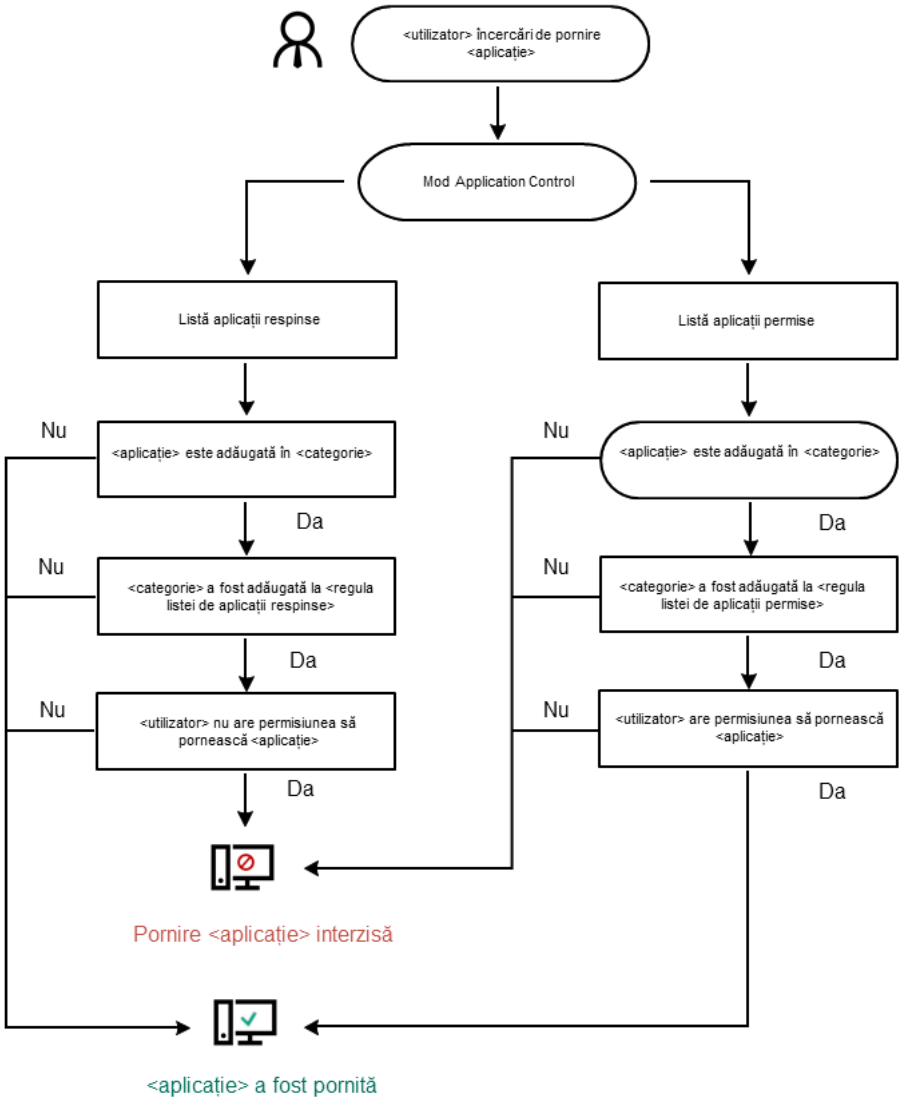
  Regulile Application Control create în Consola de administrare Kaspersky Security Center se bazează pe categorii tale particularizate de aplicații și nu pe condițiile de includere și de excludere, ca în cazul interfeței locale Kaspersky Endpoint Security.

- 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.
- Când se face upgrade pentru versiunea aplicației, importarea setărilor Application Control este acceptată numai dacă se face upgrade pentru Kaspersky Endpoint Security 10 Service Pack 2 for Windows sau versiuni ulterioare la Kaspersky Endpoint Security 11.6.0 for Windows.

  Când se face upgrade-ul altor versiuni de aplicații decât Kaspersky Endpoint Security 10 Service Pack 2 for Windows, setările Application Control trebuie configurate din nou pentru a readuce această componentă la starea de funcționare.

- 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 atribuite de Kaspersky Endpoint Security categoriei KL **Aplicații de încredere conform reputației din KSN** când este disponibilă o conexiune la serverele KSN poate să difere de lista aplicațiilor atribuite de Kaspersky Endpoint Security categoriei KL **Aplicații de încredere conform reputației din KSN** când nu există o conexiune la 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.

Activarea și dezactivarea componentei Application Control

Componenta Application Control este activată în mod implicit.

Pentru a activa sau a dezactiva componenta Application Control:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Application Control**.
3. Utilizați comutatorul de **Application Control** pentru a activa sau a dezactiva componenta.
4. Salvați-vă modificările.

Ca urmare, dacă Application Control este activat, aplicația transmite informații despre rularea fișierelor executabile către Kaspersky Security Center. Puteți vizualiza lista fișierelor executabile care rulează în Kaspersky Security Center în directorul **Fișiere executabile**. Pentru a primi informații despre toate fișierele executabile în locul fișierelor executabile care rulează, rulați activitatea *Inventar*.

Selectarea modului Application Control

Pentru a selecta modul Application Control:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Application Control**.
3. În blocul **Modul Control la pornirea aplicației**, selectați 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 din 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 din Application Control.

  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.

Toate regulile create în cursul modului selectat sunt salvate după modificarea modului, astfel încât regulile să poată fi refolosite. Pentru a reveni la utilizarea acestor reguli, tot ce trebuie să faceți este să selectați modul necesar.

4. În secțiunea **Acțiune la pornirea aplicațiilor blocate**, selectați acțiunea care va fi efectuată atunci când un utilizator încearcă să pornească o aplicație care este blocată de regulile Application Control.

5. Bifați caseta de selectare **Controlează încărcarea modulelor DLL** dacă doriți ca aplicația Kaspersky Endpoint Security să monitorizeze încărcarea modulelor DLL atunci când aplicațiile sunt pornite de către utilizatori.

   Informațiile despre modul și aplicația care a încărcat modulul vor fi salvate într-un raport.

   Kaspersky Endpoint Security monitorizează numai modulele și driverele DLL care au fost încărcate după bifarea casetei de selectare. Repornește computerul după ce ai bifat caseta de selectare dacă vrei ca aplicația Kaspersky Endpoint Security să monitorizeze modulele și driverele DLL, inclusiv cele încărcate înainte de pornirea aplicației Kaspersky Endpoint Security.

   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 „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.

   Recomandăm activarea protecție prin parolă pentru configurarea setărilor aplicației pentru a fi posibilă dezactivarea regulilor de blocare a modulelor DLL și driverelor critice de la început, fără a modifica setările politicii Kaspersky Security Center.

6. Salvați-vă modificările.

Lucrul cu regulile de control al aplicației în interfața aplicației

Kaspersky Endpoint Security controlează pornirea aplicațiilor de către utilizatori prin intermediul regulilor. O regulă Application Control specifică condițiile de declanșare și acțiunile efectuată de componenta 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 regulii 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.

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:

- **Pornit**. Această stare înseamnă că regula este utilizată atunci când componenta Application Control este activată.
- **Oprit**. Această stare înseamnă că regula este ignorată atunci când componenta Application Control este activată.
- **Test**. 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 reguli Application Control

Pentru a adăuga sau a edita o regulă Application Control:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Application Control**.
3. Faceți clic pe butonul **Aplicații blocate** sau **Aplicații permise**.

   Aceasta deschide lista regulilor Application Control.
4. Faceți clic pe butonul **Adăugare**.

   Se deschide fereastra **Regulă 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. Compilează sau editează o listă de utilizatori și/sau grupuri de utilizatori care au permisiunea de a lansa aplicații care îndeplinesc condițiile de declanșare a regulii. Pentru aceasta, faceți clic pe butonul **Adăugare** în tabelul **Subiecți și drepturile lor**.

   În mod implicit, la lista de utilizatori este adăugată valoarea **Oricine**. Regula se aplică tuturor utilizatorilor.

   > Dacă în tabel nu este specificat niciun utilizator, regula nu poate fi salvată.

   d. În tabelul **Subiecți și drepturile lor**, utilizați comutatorul pentru a defini dreptul utilizatorilor de a porni aplicații.

   e. Bifați caseta de selectare **Refuză pentru alți utilizatori** dacă dorești ca toți utilizatorii care nu apar în coloana **Subiect** și care nu fac parte din grupul de utilizatori specificat în coloana **Subiect** să nu poată porni aplicațiile care corespund condițiilor de declanșare a regulii.

   > 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 **Subiecți și drepturile lor** și care nu aparțin grupului de utilizatori specificat în tabelul **Subiecți și drepturile lor**.

   f. Dacă dorești ca aplicația Kaspersky Endpoint Security să considere aplicațiile care corespund condițiilor de declanșare a regulii 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, bifați caseta de selectare **Programe de actualizare de încredere**.

6. În fila **Condiții**, creați sau editați lista condițiilor de includere pentru declanșarea regulii.
7. În fila **Excluderi**, 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.

Adăugarea unei condiții de declanșare pentru o regulă Application Control

Pentru a adăuga o condiție nouă de declanșare pentru o regulă Application Control:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Application Control**.
3. Faceți 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** sau fila **Excluderi** și faceți clic pe butonul **Adăugare**.
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: **Cod hash fișier**, **Certificat**, **Categorie KL**, **Metadate** sau **Cale director**.
   - **Condiții „Categorie KL”**. O *categorie KL* este o listă de aplicații care partajează atribute de temă. Lista este întreținută de experții Kaspersky. De exemplu, categoria KL „Aplicații Office” include toate aplicațiile din suita Microsoft Office, Adobe® Acrobat® și altele.
   - **Condiție particularizată**. Puteți selecta fișierul aplicației și puteți selecta una dintre condițiile de declanșare a regulii: **Cod 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: **Cod hash fișier**, **Certificat**, **Categorie KL**, **Metadate** sau **Cale director**.
7. Salvați-vă modificările.

Când adăugați condiții, vă rugăm să țineți cont de următoarele considerații speciale pentru Application Control:

- 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 **Subiect** 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, faceți clic pe butonul **Rezolvare link simbolic**.

Modificarea stării unei reguli Application Control

Pentru a modifica starea unei reguli Application Control:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul .
2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Application Control**.
3. Faceți 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:
   - **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.
   - **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.

Gestionarea regulilor Application Control folosind Kaspersky Security Center

Kaspersky Endpoint Security controlează pornirea aplicațiilor de către utilizatori prin intermediul regulilor. O regulă Application Control specifică condițiile de declanșare și acțiunile efectuată de componenta 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 regulii 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.

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:

- **Pornit**. Această stare înseamnă că regula este utilizată atunci când componenta Application Control este activată.

- **Oprit**. Această stare înseamnă că regula este ignorată atunci când componenta Application Control este activată.

Test. Această stare înseamnă că Kaspersky Endpoint Security permite pornirea aplicațiilor cărora li se aplică regula, dar înregistrează în raport informații despre pornirea aplicațiilor respective.

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.

Informații despre aplicațiile folosite pe computerele din rețeaua LAN a companiei sunt disponibile în directorul **registru Aplicații** și în directorul **Fișiere executabile**. Directoarele **registru Aplicații** și **Fișiere executabile** sunt amplasate în directorul **Administrare aplicații** din nodul Consolă de administrare al Kaspersky Security Center.

Directorul **registru Aplicații** conține lista de aplicații care au fost detectate de Agentul de rețea instalat pe computerul client.

Directorul **Fișiere executabile** conține o listă cu toate fișierele executabile care au fost lansate vreodată pe computerele client sau care au fost detectate în cursul activității de inventar a Kaspersky Endpoint Security.

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 **registru Aplicații** sau în directorul **Fișiere executabile**.

*Pentru a deschide fereastra cu proprietățile aplicației în directorul **Registru aplicații**:*

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele Consolei de administrare, selectați **Suplimentar** → **Administrare aplicații** → **Registru aplicații**.
3. Selectați o aplicație.
4. În meniul contextual al aplicației, selectați **Proprietăți**.

*Pentru a deschide fereastra de proprietăți pentru un fișier executabil în directorul **Fișiere executabile**:*

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele Consolei de administrare, selectați directorul **Suplimentar** → **Administrare aplicații** → **Fișiere executabile**.
3. Selectați un fișier executabil.
4. În meniul contextual al fișierului executabil, selectați **Proprietăți**.

Crearea categoriilor de aplicații

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:

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele Consolei de administrare, selectați directorul **Suplimentar** → **Administrare aplicații** → **Categoriile de aplicații**.
3. Faceți clic pe butonul **Creare categorie** 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:

- **Categorie cu conținut adăugat manual**. Dacă ați selectat acest tip de categorie, la pasul „Configurarea condițiilor de includerea aplicațiilor într-o categorie" și la pasul „Configurarea condițiilor de excludere a aplicațiilor dintr-o categorie", veți putea să definiți criteriile cu ajutorul cărora fișierele executabile vor fi incluse într-o categorie.
- **Categorie care include fișiere executabile de pe dispozitivele selectate**. Dacă ați selectat acest tip de categorie, la pasul „Setări" veți putea să specificați un computer ale cărui fișiere executabile vor fi incluse automat în categorie.
- **Categorie care include fișiere executabile dintr-un anumit director**. Dacă ați selectat acest tip de categorie, la pasul „Director depozite" veți putea să specificați un director din care fișierele executabile vor fi incluse automat în categorie.

Când creezi o categorie cu conținut adăugat automat, Kaspersky Security Center efectuează inventarul fișierelor cu formatele următoare: 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

Acest pas este disponibil dacă ai selectat tipul de categorie **Categorie cu conținut adăugat manual**.

La acest pas, în lista verticală **Adăugare**, selectați condițiile pentru includerea aplicațiilor în categorie:

- **Din lista fișierelor executabile**. Adaugă în categoria particularizată aplicații din lista fișierelor executabile pe dispozitivul client.
- **Din proprietățile fișierului**. Specifică datele detaliate ale fișierelor executabile drept condiție pentru adăugarea aplicațiilor în categoria particularizată.
- **Metadate din fișiere în director**. 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.
- **Sume de verificare ale fișierelor din director**. 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.
- **Certificate pentru fișiere din director**. 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 îți recomandăm să folosești condiții ale căror proprietăți nu au specificat parametrul **Amprentă certificat**.

- **Metadate fișiere program de instalare MSI**. Selectați pachetul MSI. Kaspersky Security Center va indica metadatele fișierelor executabile cuprinse în acest pachet MSI drept condiție pentru adăugarea aplicațiilor în categoria particularizată.
- **Sume de verificare ale fișierelor din programul de instalare MSI al aplicației**. 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.
- **Categorie KL**. Specifică o categorie KL drept condiție pentru adăugarea aplicațiilor în categoria particularizată. O *categorie KL* 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.

  Poți selecta toate categoriile KL ca să generezi o listă extinsă cu aplicații de încredere.
- **Cale către aplicație**. Selectați un director pe dispozitivul client. Kaspersky Security Center va adăuga fișierele executabile din acest director în categoria particularizată.
- **Certificate din depozitul de certificate**. Selectați certificatele care au fost utilizate pentru a semna fișierele executabile drept condiție pentru adăugarea de aplicații la categoria particularizată.

  Nu îți recomandăm să folosești condiții ale căror proprietăți nu au specificat parametrul **Amprentă certificat**.

- **Tip unitate**. 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 **Categorie cu conținut adăugat manual**.

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 **Adăugare**, selectați condițiile pentru excluderea aplicațiilor din categorie:

- **Din lista fișierelor executabile**. Adaugă în categoria particularizată aplicații din lista fișierelor executabile pe dispozitivul client.
- **Din proprietățile fișierului**. Specifică datele detaliate ale fișierelor executabile drept condiție pentru adăugarea aplicațiilor în categoria particularizată.
- **Metadate din fișiere în director**. 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.
- **Sume de verificare ale fișierelor din director**. 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.
- **Certificate pentru fișiere din director**. 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.
- **Metadate fișiere program de instalare MSI**. Selectați pachetul MSI. Kaspersky Security Center va indica metadatele fișierelor executabile cuprinse în acest pachet MSI drept condiție pentru adăugarea aplicațiilor în categoria particularizată.
- **Sume de verificare ale fișierelor din programul de instalare MSI al aplicației**. 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.
- **Categorie KL**. Specifică o categorie KL drept condiție pentru adăugarea aplicațiilor în categoria particularizată. O *categorie KL* 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.

  Poți selecta toate categoriile KL ca să generezi o listă extinsă cu aplicații de încredere.
- **Cale către aplicație**. Selectați un director pe dispozitivul client. Kaspersky Security Center va adăuga fișierele executabile din acest director în categoria particularizată.
- **Certificate din depozitul de certificate**. Selectați certificatele care au fost utilizate pentru a semna fișierele executabile drept condiție pentru adăugarea de aplicații la categoria particularizată.
- **Tip unitate**. 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 **Categorie care include fișiere executabile de pe dispozitivele selectate**.

La acest pas, faceți clic pe butonul **Adăugare** 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 **Fișiere executabile**, vor fi adăugate la categoria de aplicații de către Kaspersky Security Center.

La acest pas, mai poți configura setările următoare:

- Algoritm pentru calcularea funcției hash de către Kaspersky Security Center. Pentru a selecta un algoritm, trebuie să bifezi cel puțin una dintre casetele de selectare următoare:
  - **Calculați SHA-256 pentru fișierele din această categorie (acceptate de Kaspersky Endpoint Security 10 Service Pack 2 for Windows și orice versiuni ulterioare)**.
  - **Calculați MD5 pentru fișierele din această categorie (acceptate de versiuni anterioare produsului Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.
- Caseta de selectare **Sincronizează datele cu depozitul serverului de administrare**. 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 **Fișiere executabile**.

  În cazul în care caseta de selectare **Sincronizează datele cu depozitul serverului de administrare** este debifată, Kaspersky Security Center nu va efectua nicio modificare pentru o categorie de aplicații după crearea sa.
- Câmpul **Perioadă de scanare (h)**. În acest câmp poți specifica durata (în ore) după care Kaspersky Security Center golește categoria de aplicații și adaugă în acesta toate fișierele executabile de pe computerele specificate, existente în directorul **Fișiere executabile**.

  Câmpul este disponibil dacă se bifați caseta de selectare **Sincronizează datele cu depozitul serverului de administrare**.

Pasul 6. Directorul depozitului

Acest pas este disponibil dacă ai selectat tipul de categorie **Categorie care include fișiere executabile din directorul selectat**.

La acest pas, faceți clic pe butonul **Răsfoire** și specifică directorul în care Kaspersky Security Center va căuta fișiere executabile pentru a adăuga automat aplicații în categoria de aplicații.

La acest pas, mai poți configura setările următoare:

- Caseta de selectare **Include în această categorie bibliotecile cu legături dinamice (DLL)**. 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 în această categorie datele scripturilor**. 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.

- Algoritm pentru calcularea funcției hash de către Kaspersky Security Center. Pentru a selecta un algoritm, trebuie să bifezi cel puțin una dintre casetele de selectare următoare:
  - **Calculați SHA-256 pentru fișierele din această categorie (acceptate de Kaspersky Endpoint Security 10 Service Pack 2 for Windows și orice versiuni ulterioare)**.
  - **Calculați MD5 pentru fișierele din această categorie (acceptate de versiuni anterioare produsului Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.
- Caseta de selectare **Forțează scanarea directorului pentru detectarea modificărilor**. 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 **Forțează scanarea directorului pentru detectarea modificărilor**, 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 **Perioadă de scanare (h)**. 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.

  Acest câmp este disponibil dacă se bifați caseta de selectare **Forțează scanarea directorului pentru detectarea modificărilor**.

Pasul 7. Crearea unei categorii particularizate

Pentru a închide Expertul de instalare a aplicației, fă clic pe butonul **Terminare**.

Adăugarea fișierelor executabile din directorul Fișiere executabile în categoria de aplicații

În directorul **Fișiere executabile** 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 **Fișiere executabile** în categoria de aplicații:*

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În arborele Consolei de administrare, selectați directorul **Suplimentar → Administrare aplicații → Fișiere executabile**.
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 **Adăugare în categorie**.

   Se deschide fereastra **Selectare categorie de aplicații**.
5. În fereastra **Selectare categorie de aplicații**:

- În partea de sus a ferestrei, alege una dintre următoarele opțiuni:
  - **Creează o categorie de aplicații**. Alege această opțiune dacă dorești să creezi o nouă categorie de aplicații și să adaugi fișiere executabile în aceasta.
  - **Adaugă reguli în categoria specificată**. Alege această opțiune dacă dorești să selectezi o categorie de aplicații existentă și să adaugi fișiere executabile în aceasta.
- În secțiunea **Tip regulă**, selectați una dintre următoarele opțiuni:
  - **Adaugă la reguli de includere**. Selectați această opțiune dacă dorești să creezi o condiție care adaugă fișiere executabile în categoria de aplicații.
  - **Adaugă la reguli de excludere**. Selectați această opțiune dacă dorești să creezi o condiție care exclude fișiere executabile în categoria de aplicații.
- În secțiunea **Tip informații fișier**, selectați una dintre următoarele opțiuni:
  - **Date certificat (sau SHA-256 pentru fișiere fără certificat)**.
  - **Date certificat (fișierele fără certificat vor fi omise)**.
  - **Doar SHA-256 (fișierele fără SHA-256 vor fi omise)**.
  - **MD5 (mod întrerupt, doar pentru Kaspersky Endpoint Security 10 Service Pack 1)**.

6. Faceți clic pe **OK**.

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 **Server de administrare** din arborele consolei de administrare, selectați fila **Evenimente**.
3. Alege o selecție de evenimente legate de funcționarea componentei Application Control (Vizualizarea evenimentelor rezultate din funcționarea componentei Application Control, Vizualizarea evenimentelor rezultate din testarea funcționării componentei Application Control) în lista verticală **Selecție evenimente**.
4. Faceți clic pe butonul **Executare selecție**.
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 **Adăugare în categorie**.

   Se deschide fereastra **Selectare categorie de aplicații**.
7. În fereastra **Selectare categorie de aplicații**:
   - În partea de sus a ferestrei, alege una dintre următoarele opțiuni:

- **Creează o categorie de aplicații**. Alege această opțiune dacă dorești să creezi o nouă categorie de aplicații și să adaugi fișiere executabile în aceasta.
- **Adaugă reguli în categoria specificată**. Alege această opțiune dacă dorești să selectezi o categorie de aplicații existentă și să adaugi fișiere executabile în aceasta.

- În secțiunea **Tip regulă**, selectați una dintre următoarele opțiuni:
  - **Adaugă la reguli de includere**. Selectați această opțiune dacă dorești să creezi o condiție care adaugă fișiere executabile în categoria de aplicații.
  - **Adaugă la reguli de excludere**. Selectați această opțiune dacă dorești să creezi o condiție care exclude fișiere executabile în categoria de aplicații.
- În secțiunea **Tip informații fișier**, selectați una dintre următoarele opțiuni:
  - **Date certificat (sau SHA-256 pentru fișiere fără certificat)**.
  - **Date certificat (fișierele fără certificat vor fi omise)**.
  - **Doar SHA-256 (fișierele fără SHA-256 vor fi omise)**.
  - **MD5 (mod întrerupt, doar pentru Kaspersky Endpoint Security 10 Service Pack 1)**.

8. Faceți clic pe **OK**.

Adăugarea și modificarea unei reguli Application Control folosind Kaspersky Security Center

Pentru a adăuga sau modifica o regulă Application Control folosind Kaspersky Security Center:

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Security Controls → Application Control**.
   În partea dreaptă a ferestrei se afișează setările componentei Application Control.
6. Efectuează una dintre următoarele acțiuni:
   - Pentru a adăuga o regulă, faceți clic pe butonul **Adăugare**.
   - Dacă dorești să editezi o regulă existentă, selectați regula în lista de reguli și apasă pe butonul **Editare**.

   Se deschide fereastra **Regulă Application Control**.
7. Efectuează una dintre următoarele acțiuni:

- Dacă dorești să creezi o categorie nouă:

  a. Faceți clic pe butonul **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 butonul **Proprietăți**.

  Se deschide fereastra **Proprietăți: <Nume categorie>**.

  c. Modifică setările categoriei de aplicații selectate.

  d. Faceți clic pe **OK**.

  e. În lista verticală **Categorie**, selectați categoria de aplicații creată pe baza căreia dorești să creezi o regulă.

8. În tabelul **Subiecți și drepturile lor**, faceți clic pe butonul **Adăugare**.

   Se deschide fereastra Microsoft Windows standard **Select Users or Groups** (Selectare utilizatori sau grupuri).

9. În fereastra **Select Users or Groups** (Selectare utilizatori sau grupuri), specifică lista de utilizatori și/sau grupuri de utilizatori pentru care dorești să configurezi permisiunea de pornire a aplicațiilor din categoria selectată.

10. În tabelul **Subiecți și drepturile lor**:

    - Dacă dorești să permiți utilizatorilor și/sau grupurilor de utilizatori să pornească aplicațiile care aparțin categoriei selectate, bifați caseta de selectare **Permitere** în rândurile relevante.

    - Dacă dorești să blochezi utilizatori și/sau grupuri de utilizatori să pornească aplicațiile care aparțin categoriei selectate, bifați casetele de selectare **Refuzare** în rândurile relevante.

11. Bifați caseta de selectare **Refuză pentru alți utilizatori** dacă dorești ca toți utilizatorii care nu apar în coloana **Subiect** și care nu fac parte din grupul de utilizatori specificat în coloana **Subiect** să nu poată porni aplicațiile care aparțin categoriei selectate.

12. 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.

13. Salvați-vă modificările.

Modificarea stării unei reguli Application Control folosind Kaspersky Security Center

Pentru a modifica starea unei reguli Application Control:

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Security Controls** → **Application Control**.
   În partea dreaptă a ferestrei se afișează setările componentei Application Control.
6. 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 componenta Application Control este activată.
   - **Oprit**. Această stare înseamnă că regula este ignorată atunci când componenta Application Control este activată.
   - **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.

     Poți utiliza starea **Test** ca să atribui acțiunea echivalentă cu opțiunea **Reguli test** pentru o serie de reguli dacă este selectată opțiunea **Aplicare reguli** în lista verticală **Acțiune**.
7. 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 Kaspersky Security Center Help*.

[Cum se exportă și se importă o listă de reguli Application Control în Consola de administrare (MMC)]

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Security Controls** → **Application Control**.
6. 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 **Exportare**.
   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. Faceți clic pe butonul **Save**.
      Kaspersky Endpoint Security exportă lista de reguli în fișierul XML.
7. Pentru a exporta o listă de reguli Application Control:
   a. Faceți clic pe linkul **Importare**.
      În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de reguli.
   b. Faceți clic pe butonul **Deschidere**.
      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 Application Control în Consola Web și Cloud Console]

1. În fereastra principală a Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security pentru computerele pe care doriți să exportați sau să importați lista de reguli.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Selectați **Security Controls** → **Application Control**.
5. Faceți clic pe linkul **Setări liste reguli**.
6. Selectați o listă de reguli: lista de aplicații permise sau respinse.
7. Pentru a exporta lista de reguli Application Control:
   a. Selectați regulile pe care doriți să le exportați.
   b. Faceți clic pe butonul **Export**.
   c. Confirmați că doriți să exportați numai regulile selectate sau să exportați întreaga listă.
   d. Faceți clic pe butonul **Export**.

      Kaspersky Endpoint Security exportă lista de reguli într-un fișier XML în directorul de descărcări implicit.
8. Pentru a exporta o listă de reguli Application Control:
   a. Faceți clic pe linkul **Importare**.

      În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de reguli.
   b. Faceți clic pe butonul **Deschidere**.

      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.
9. Salvați-vă modificările.

Testarea regulilor Application Control folosind Kaspersky Security Center

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.

Pentru a activa sau dezactiva testarea regulilor funcției Application Control în Kaspersky Security Center:

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Security Controls → Application Control**.

   În partea dreaptă a ferestrei se afișează setările componentei Application Control.
6. În lista verticală **Mod Application 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 din 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 din Application Control.
7. Efectuează una dintre următoarele acțiuni:

   - Dacă doreiți să activați testarea regulilor Application Control, selectați opțiunea **Reguli testare** în lista verticală **Acțiune**.
   - Dacă doriți să activați Aplicația Application Control pentru a gestiona pornirea aplicațiilor pe computerele utilizatorilor, selectați opțiunea **Aplicare reguli** din lista derulantă **Acțiune**.
8. Salvați-vă modificările.

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 **Server de administrare** din arborele consolei de administrare, selectați fila **Evenimente**.
3. Faceți clic pe butonul **Creează o selecție**.

   Se deschide fereastra **Proprietăți: <Nume selecție>**.
4. Deschide secțiunea **Evenimente**.
5. Faceți clic pe butonul **Deselectare totală**.

6. În tabelul **Evenimente**, bifați casetele de selectare **Pornire aplicație interzisă în modul testare** și **Pornire aplicație permisă în modul testare**.
7. Faceți clic pe **OK**.
8. În lista verticală **Selectare evenimente**, selectați selecția creată.
9. Faceți clic pe butonul **Executare selecție**.

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 **Server de administrare** din arborele consolei de administrare, selectați fila **Rapoarte**.
3. Faceți clic pe butonul **Șablon raport nou**.
   Se lansează Expertul pentru șablon de raport.
4. Urmează instrucțiunile din Expertul pentru șablon de raport. La pasul **Selectarea tipului șablonului de raport**, selectați **Altele** → **Raport despre aplicațiile blocate în modul de testare**.
   După ce ai finalizat Expertul pentru șablon de raport nou, un nou șablon de raport apare în tabelul din fila **Rapoarte**.
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 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 **Server de administrare** din arborele consolei de administrare, selectați fila **Evenimente**.
3. Faceți clic pe butonul **Creează o selecție**.
   Se deschide fereastra **Proprietăți: <Nume selecție>**.
4. Deschide secțiunea **Evenimente**.
5. Faceți clic pe butonul **Deselectare totală**.
6. În tabelul **Evenimente**, bifați caseta de selectare **Pornire aplicație interzisă**.
7. Faceți clic pe **OK**.

8. În lista verticală **Selectare evenimente**, selectați selecția creată.

9. Faceți clic pe butonul **Executare selecție**.

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 **Server de administrare** din arborele consolei de administrare, selectați fila **Rapoarte**.

3. Faceți clic pe butonul **Șablon raport nou**.

   Se lansează Expertul pentru șablon de raport.

4. Urmează instrucțiunile din Expertul pentru șablon de raport. La pasul **Selectarea tipului șablonului de raport**, selectați **Altele** → **Raport despre aplicațiile blocate**.

   După ce ai finalizat Expertul pentru șablon de raport nou, un nou șablon de raport apare în tabelul din fila **Rapoarte**.

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.

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.

Pentru a activa testarea regulilor Application Control sau pentru a selecta o acțiune de blocare pentru Application Control:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.

2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Application Control**.

   Aceasta deschide lista regulilor Application Control.

3. În coloana **Stare**, selectați **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.

4. 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.

Monitorizare activitate aplicație

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, faceți clic pe **Mai multe instrumente** → **Monitorizare activitate aplicație**.

Se deschide fereastra **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 **Se execută** 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 **Executare la pornire** afișează lista de aplicații care pornesc odată cu pornirea computerului.

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:).
- Caracterul `?` (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. 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.

Sunt disponibile șabloane speciale pentru mesajul afișat atunci când pornirea unei aplicații este blocată și pentru mesajul care este trimis administratorului. Poți modifica șabloanele de mesaje.

Pentru a edita un șablon de mesaj:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Protecție** → **Security Controls** → **Application Control**.
3. În blocul **Șabloane**, configurați șabloanele pentru mesajele Application Control:
   - **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.
4. Salvați-vă modificările.

Cele mai bune practici pentru implementarea unei liste de aplicații permise

Când planificați implementarea modului 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:

   - **Categorie cu conținut adăugat manual**. 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.
     - Cale către aplicație. Kaspersky Security Center adăugă în categoria de aplicații toate fișierele executabile din acest director.

       Folosirea condiției directorului Aplicații 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 directorului Aplicații doar acelor utilizatori pentru care trebuie permisă instalarea automată a actualizărilor.

   - **Categorie care include fișiere executabile dintr-un anumit director**. Poți specifica un director din care fișierele executabile vor fi atribuite automat categoriei de aplicații create.
   - **Categorie care include fișiere executabile de pe dispozitivele selectate**. 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 **Fișiere executabile**.

2. Selectați modul listei permise 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.

Imagine de aur

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 **Subiect** 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 „Director aplicații” și stabilește calea către respectivul director. Apoi creează o regulă de permitere și selectați această categorie.

     Folosirea condiției directorului Aplicații 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 directorului Aplicații 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 și Web Threat Protection monitorizează fluxurile de date transmise prin protocoale specifice 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.

Activarea monitorizării tuturor porturilor de rețea

Pentru a activa monitorizarea tuturor porturilor de rețea:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Setări de rețea**.
3. În secțiunea **Porturi monitorizate**, selectați opțiunea **Monitorizare toate porturile de rețea**.
4. Salvați-vă modificările.

Crearea unei liste de porturi de rețea monitorizate

Pentru a crea o listă de porturi de rețea monitorizate:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Setări de rețea**.
3. În secțiunea **Porturi monitorizate**, selectați **Monitorizare numai porturi de rețea selectate**.
4. Faceți clic pe butonul **Selectare**.

   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. Faceți clic pe butonul **Adăugare**.
   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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Setări de rețea**.
3. În secțiunea **Porturi monitorizate**, selectați **Monitorizare numai porturi de rețea selectate**.

4. Bifați caseta de selectare **Monitorizați 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 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 **Monitorizare toate porturile pentru aplicații specificate**.
6. Faceți clic pe butonul **Selectare**.

   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. Faceți clic pe butonul **Adăugare**.

   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 portului 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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Setări generale** → **Setări de rețea**.
6. În secțiunea **Porturi monitorizate**, selectați **Monitorizare numai porturi de rețea selectate**.
7. Fă clic pe butonul **Setări**.

   Se deschide fereastra **Porturi rețea**. Fereastra **Porturi 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.
8. 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. Faceți clic pe butonul **Export**.
   c. În fereastra care se deschide, specificați numele fișierului XML în care doriți să exporți lista de porturi de rețea și selectați directorul în care doriți să salvați acest fișier.
   d. Faceți clic pe butonul **Save**.

      Kaspersky Endpoint Security exportă întreaga listă de porturi de rețea în fișierul XML.
9. 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. Faceți clic pe butonul **Export**.
   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. Faceți clic pe butonul **Save**.

      Kaspersky Endpoint Security exportă întreaga listă de aplicații în fișierul XML.
10. Pentru a importa lista de porturi de rețea:
    a. În lista de porturi de rețea, faceți clic pe butonul din **Importare**.

       În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de porturi de rețea.

b. Faceți clic pe butonul **Deschidere**.

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.

11. 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 **Importare**.

În fereastra deschisă, selectați fișierul XML din care doriți să importați lista de aplicații.

b. Faceți clic pe butonul **Deschidere**.

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.

12. Salvați-vă modificările.

Cum se exportă și se importă liste de porturi monitorizate în Consola Web și Cloud Console

1. În fereastra principală a Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security pentru computerele pe care doriți să exportați sau să importați liste de porturi monitorizate.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Setări aplicație**.

4. Accesează secțiunea **Setări generale** → **Setări rețea**.

5. Pentru a exporta lista de porturi de rețea:

   a. În secțiunea **Porturi monitorizate**, selectați **Monitorizare numai porturi de rețea selectate**.

   b. Faceți clic pe linkul **N porturi selectate**.

      Se deschide fereastra **Porturi rețea**. Fereastra **Porturi 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.

   c. În lista de porturi de rețea, selectați porturile pe care doriți să le exportați.

   d. Faceți clic pe butonul **Export**.

   e. În fereastra care se deschide, specificați numele fișierului XML în care doriți să exporți lista de porturi de rețea și selectați directorul în care doriți să salvați acest fișier.

   f. Faceți clic pe butonul **Save**.

      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 **Porturi monitorizate**, bifați caseta de selectare **Monitorizare toate porturile pentru aplicații specificate**.

   b. Faceți clic pe linkul **N aplicații selectate**.

   c. În lista de aplicații, selectați aplicațiile pe care doriți să le exportați.

   d. Faceți clic pe butonul **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. Faceți clic pe butonul **Save**.

      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 **Importare**.

      În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de porturi de rețea.

   b. Faceți clic pe butonul **Deschidere**.

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 **Importare**.

      În fereastra deschisă, selectați fișierul XML din care doriți să importați lista de aplicații.

   b. Faceți clic pe butonul **Deschidere**.

      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.

Managed Detection and Response

Componenta Managed Detection and Response a fost adăugată la Kaspersky Endpoint Security versiunea 11.6.0. Această componentă facilitează interacțiunea cu soluția cunoscută drept Kaspersky Managed Detection and Response. *Kaspersky Managed Detection and Response (MDR)* caută, detectează și elimină în mod continuu amenințările îndreptate asupra organizației dvs. Pentru informații detaliate despre modul în care funcționează soluțiile, *consultați Ghidul de ajutor Kaspersky Managed Detection and Response*.

Când interacționați cu Kaspersky Managed Detection and Response, aplicația vă permite să efectuați următoarele funcții:

- să activați componenta Managed Detection and Response utilizând un fișier de configurare BLOB;
- să executați comenzi din Kaspersky Managed Detection and Response;
- să trimiteți date de telemetrie către Kaspersky Managed Detection and Response pentru detectarea amenințărilor.

Integrarea cu Kaspersky Managed Detection and Response

Integrarea cu Kaspersky Managed Detection and Response constă în următorii pași:

1. **Configurarea Private Kaspersky Security Network**

   Omiteți acest pas dacă utilizați Kaspersky Security Center Cloud Console. Kaspersky Security Center Cloud Console configurează automat componenta Kaspersky Security Network locală când instalează plug-in-ul MDR.

   Componenta Private KSN acceptă schimbul de date între computere și serverele dedicate Kaspersky Security Network, dar nu Global KSN.

   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 mai multe detalii despre configurarea Private KSN, consultați *Ghidul de 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 Private KSN din linia de comandă

1. Executați interpretorul de linii de comandă (cmd.exe) ca administrator.
2. Deschideți directorul în care se află pachetul de distribuție Kaspersky Endpoint Security.
3. Executați următoare comandă:

   ```
   avp.com KSN /private <nume fișier>
   ```

   unde `<nume fișier>` este numele fișierului de configurare care conține setările componentei Private KSN (format fișier PKCS7 sau PEM).

   Exemplu:

   ```
   avp.com KSN /private C:\kpsn_config.pkcs7
   ```

Ca rezultat, Kaspersky Endpoint Security va utiliza Private KSN pentru a determina reputația fișierelor, aplicațiilor și site-urilor web. Setările politicii din secțiunea **Kaspersky Security Network** vor afișa următoarea stare de funcționare: *Rețea KSN: Private KSN*.

Trebuie să activați modul KSN extins pentru ca Managed Detection and Response să funcționeze.

2 Activați 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 fișierul BLOB, *consultați Ghidul de ajutor Kaspersky Managed Detection and Response*.

Cum se activează componenta Managed Detection and Response în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Extindere Threat Protection → Detecție și răspuns**.
6. Bifați caseta de selectare **Managed Detection and Response**.
7. În blocul **Setări**, faceți clic pe **Import** și selectați fișierul BLOB primit în Kaspersky Managed Detection and Response Console. Fișierul are extensia P7.
8. Salvați-vă modificările.

Cum se activează Managed Detection and Response în Web Console și Cloud Console

1. În fereastra principală a Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Selectați **Extindere Threat Protection** → **Detecție și răspuns**.
5. Duceți comutatorul **Managed Detection and Response** la poziția activat.
6. Faceți clic pe **Import** și selectați fișierul BLOB care a fost obținut în Kaspersky Managed Detection and Response Console. Fișierul are extensia P7.
7. Salvați-vă modificările.

Cum se activează 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 pachetul de distribuție Kaspersky Endpoint Security.
3. Executați următoare comandă:

   - Dacă setările aplicației nu sunt protejate prin parolă:

     `avp.com MDRLICENSE /ADD <nume fișier>`

     `<nume fișier>` este numele fișierului de configurare pentru activarea componentei Managed Detection and Response (format fișier P7).

   - Dacă setările aplicației sunt protejate prin parolă:

     `avp.com MDRLICENSE /ADD <nume fișier> /login=<nume utilizator> /password=<parolă>`

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 încărca fișierul și îl va trimite către computer în timpul următoarei sincronizări cu Kaspersky Security Center. Verificați starea de funcționare a componentei, vizualizând *Application components status report*. 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 în lista de componente Kaspersky Endpoint Security.

Trebuie să activați următoarele componente pentru ca Managed Detection and Response să funcționeze:

- Kaspersky Security Network (modul extins);
- Behavior Detection.

Activarea acestor componente nu este opțională. În caz contrar, Kaspersky Managed Detection and Response nu poate funcționa deoarece nu poate primi datele de telemetrie necesare.

În plus, Kaspersky Managed Detection and Response utilizează datele primite de la alte componente ale aplicației. Activarea acelor componente este opțională. Printre componentele care furnizează date suplimentare se numără:

- Web Threat Protection.
- Mail Threat Protection.
- Firewall.

Migrarea de la Kaspersky Endpoint Agent la Kaspersky Endpoint Security for Windows

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 utilizați Kaspersky Endpoint Security 11.6.0 sau o versiune ulterioară, pentru a lucra cu soluția MDR, trebuie să selectați componenta Managed Detection and Response când instalați aplicația. În acest caz, nu trebuie să instalați Kaspersky Endpoint Agent.

Pentru a migra de la Kaspersky Endpoint Agent la Kaspersky Endpoint Security for Windows:

1. Configurați integrarea cu Kaspersky Managed Detection and Response în politica Kaspersky Endpoint Security.
2. Dezactivați componenta Managed Detection and Response în politica Kaspersky Endpoint Agent.

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.

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 informații complete despre componenta Kaspersky Endpoint Agent for Windows inclusă în soluția software pe care o utilizați și pentru informații complete despre soluțiile independente, consultați Ghidul de ajutor al produsului relevant:

- *Ghid de ajutor Kaspersky Anti Targeted Attack Platform*
- *Ghid de ajutor Kaspersky Sandbox*
- *Ghid de ajutor optim Kaspersky Endpoint Detection and Response*
- *Ghid de ajutor Kaspersky Managed Detection and Response*

Kaspersky Endpoint Agent este inclus în kitul de distribuție Kaspersky Endpoint Security. Puteți instala Kaspersky Endpoint Agent în timpul instalării Kaspersky Endpoint Security. Pentru a face acest lucru, selectați componenta Agent Endpoint în timpul instalării aplicației (de exemplu, în pachetul de instalare). După instalarea aplicației cu Agent Endpoint, Kaspersky Endpoint Security și Kaspersky Endpoint Agent vor fi adăugate la lista de aplicații instalate. După dezinstalarea Kaspersky Endpoint Security, Kaspersky Endpoint Agent va fi, de asemenea, dezinstalat automat.

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 *Ștergere date* 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 *Ștergere date*. 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 Consolei Web, selectează **Devices** → **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe butonul **Adăugare**.

   Expertul de activitate pornește.

3. Configurați setările pentru activitate:

   a. În lista verticală **Application**, selectați **Kaspersky Endpoint Security for Windows (11.6.0)**.

   b. În lista verticală **Tip activitate**, selectați **Ștergere date**.

   c. În câmpul **Nume activitate**, introduceți o descriere succintă, de exemplu `Ștergere date (Antifurt)`.

   d. În secțiunea **Select devices to which the task will be assigned**, selectați domeniul activității.

4. Selectați dispozitive în funcție de opțiunea selectată pentru domeniul activității. Faceți clic pe butonul **Next**.

   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. Termină expertul făcând clic pe butonul **Finish**.

   Se va afișa o activitate nouă în lista de activități.

6. Faceți clic pe activitatea **Ștergere date** a Kaspersky Endpoint Security.

   Se va deschide fereastra de proprietăți a activității.

7. Selectați fila **Setări aplicație**.

8. Selectați metoda de ștergere a datelor:

   - **Ștergere prin mijloacele sistemului de operare**. Kaspersky Endpoint Security folosește resursele sistemului de operare pentru a șterge fișierele, fără a le trimite la coșul de reciclare.
   - **Ștergere completă, nu este posibilă recuperarea**. 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 **Ștergere automată a datelor dacă nu există nicio conexiune la Kaspersky Security Center pentru mai mult de N zile**. 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 configurați ștergerea amânată a datelor, rețineți că angajații își pot închide computerul înainte de a pleca în vacanță. În acest caz, termenul de conectare absentă poate fi depășit și datele vor fi șterse. 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 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.
- **Directoare predefinite**. Kaspersky Endpoint Security va șterge fișierele din următoarele zone:
  - **Documente**. Fișiere din directorul standard *Documente* al sistemului de operare și subdirectoarele sale.
  - **Cookie-uri**. 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.
  - **Fișiere temporare de Internet Explorer**. Fișiere temporare legate de funcționarea Internet Explorer, precum copii ale paginilor web, imagini și fișiere media.
  - **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).
  - **Profil de utilizator**. 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. Faceți clic pe butonul **Save**.
12. Bifați caseta de selectare de lângă activitate.
13. Faceți clic pe butonul **Executare**.

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.

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:

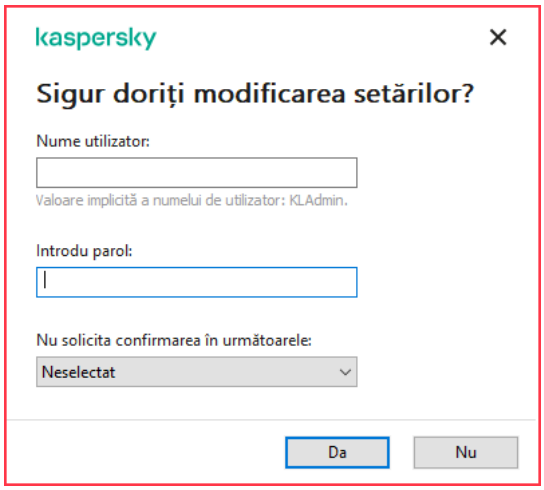
- Introdu un nume de utilizator și parola.

  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 este în domeniu, puteți utiliza contul KLAdmin.

- 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).



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 din domeniu. 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.

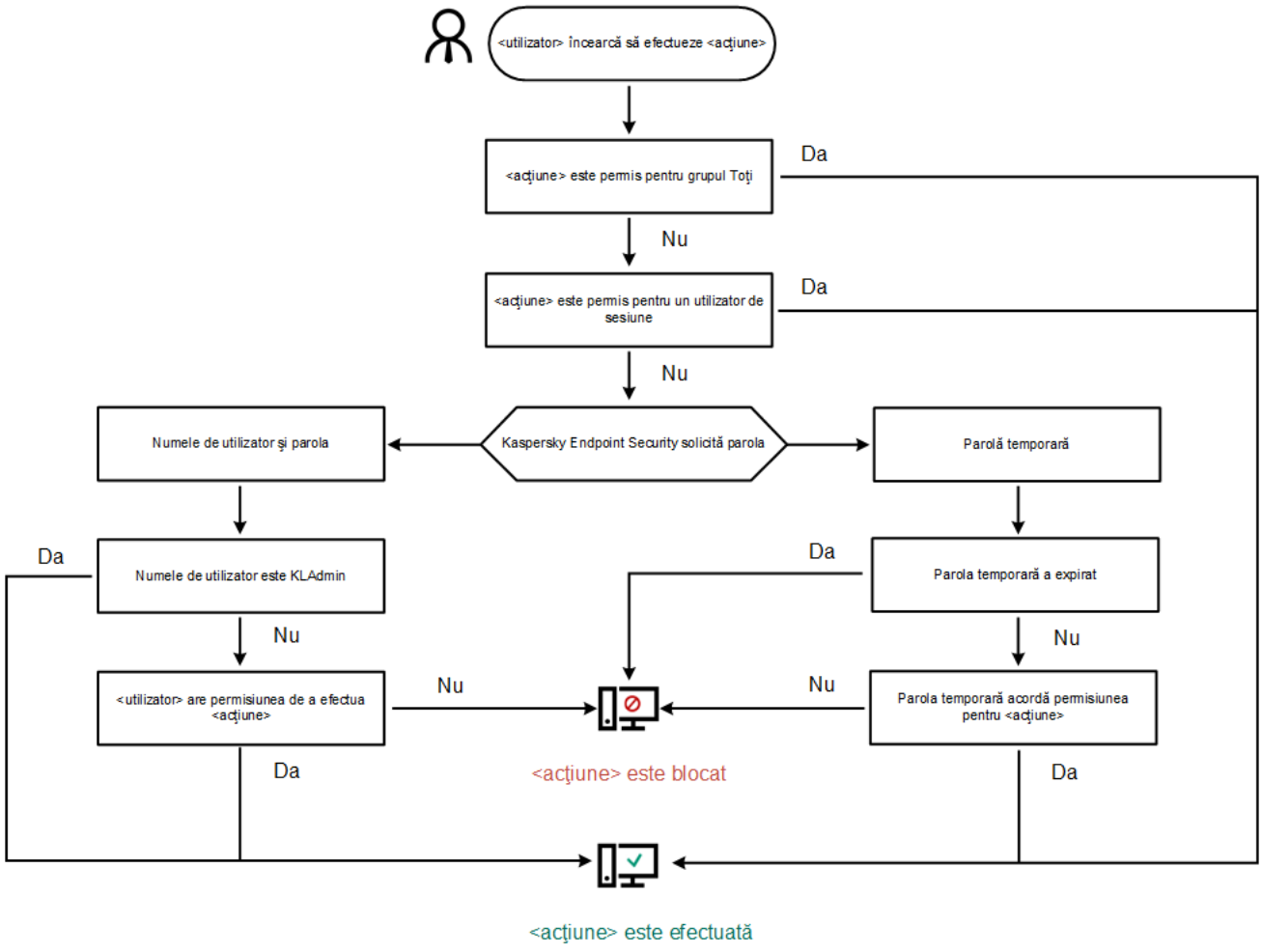
- **Grupul Toți**. Un grup încorporat în Windows care include toți utilizatorii din rețeaua corporației. Utilizatorii din grupul Toți pot să acceseze aplicația în conformitate cu permisiunile care le sunt acordate.
- **Utilizatori individuali sau grupuri**. Conturi de utilizatori pentru care poți să 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 **Salvare 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).

Pentru a activa protecția prin parolă:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.

   În fereastra de setări a aplicației, selectați secțiunea **Interfață**.

2. Utilizați comutatorul **Protecție prin parolă** pentru a activa sau a dezactiva componenta.

3. 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.

4. Setați permisiuni pentru toți utilizatorii din rețeaua corporației:

   a. În tabelul **Permisiuni**, faceți clic pe butonul **Editare** 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 **Ieșire din aplicație** 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.

   c. Faceți clic pe butonul **OK**.

5. 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 **Salvare 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

Poți acorda acces la Kaspersky Endpoint Security unor utilizatori individuali sau grupuri. De exemplu, dacă părăsirea aplicației este blocată pentru grupul Toți, poți acorda permisiunea **Ieșire din aplicație** 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.

Pentru a acorda permisiuni utilizatorilor individuali sau grupurilor:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.

   În fereastra de setări a aplicației, selectați secțiunea **Interfață**.

2. În secțiunea **Protecție prin parolă**, faceți clic pe butonul **Adăugare**.

3. În fereastra deschisă, faceți clic pe butonul **Selectare utilizator**.

   Se va deschide dialogul standard Selectare utilizatori sau grupuri.

4. Selectați un utilizator sau un grup în Active Directory și confirmă selecția.

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 **Ieșire din aplicație** 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.

Pentru a permite unui utilizator să efectueze o acțiune blocată utilizând o parolă temporară:

1. Deschide Consolă de administrare a Kaspersky Security Center.

2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.

3. În spațiul de lucru, selectați fila **Dispozitive**.

4. Fă dublu clic pentru a deschide fereastra cu proprietățile computerului.

5. În fereastra cu proprietățile computerului, selectează secțiunea **Aplicații**.

6. În lista de aplicații Kaspersky instalate pe computer, selectați **Kaspersky Endpoint Security for Windows** și faceți dublu clic pentru a deschide proprietățile aplicației.

7. În fereastra cu setările aplicației, selectați **Setări generale** → **Interfață**.

8. În secțiunea **Protecție prin parolă**, faceți clic pe butonul **Setări**.

   Se deschide fereastra **Protecție prin parolă**.

9. În secțiunea **Parolă temporară**, fă clic pe butonul **Setări**.

   Se deschide fereastra **Creare parolă temporară**.

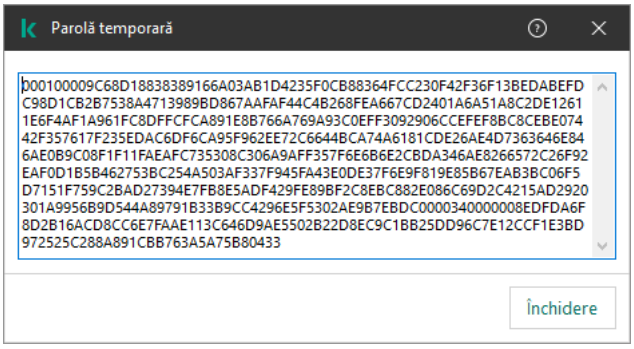
10. În câmpul **Data expirării**, specifică data când va expira parola temporară.

11. În tabelul **Domeniu parolă temporară**, bifează casetele de selectare de lângă acțiunile care vor fi disponibile pentru utilizator după introducerea parolei temporare.

12. Fă clic pe butonul **Creare**.

    Se va deschide o fereastră conținând parola temporară (vezi figura de mai jos).

13. Copiază parola și furnizeaz-o utilizatorului.



Parolă temporară

Aspecte speciale ale permisiunilor Protecție prin parolă

Permisiunile Protecție prin parolă au câteva aspecte importante și limitări care trebuie luate în considerare.

Configurare setări aplicație

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).

Ieșire din aplicație

Nu există considerații sau limitări speciale.

Dezactivează componentele protecției

- 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 protecție, adăugați un utilizator sau un grup care are permisiunea **Dezactivare componente 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 **Configurare setări aplicație**.
- Pentru a dezactiva componentele de protecție din meniul contextual (utilizând elementul de meniu **Pauză protecție**), un utilizator trebuie să aibă și permisiunea **Dezactivare componente de control** pe lângă cea de **Dezactivare componente de protecție**.

Dezactivare componente 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 **Dezactivare componente 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 **Configurare setări aplicație**.
- Pentru a dezactiva componentele de control din meniul contextual (utilizând elementul de meniu **Pauză protecție**), un utilizator trebuie să aibă și permisiunea **Dezactivare componente de protecție** pe lângă cea de **Dezactivare componente de control**.

Dezactivare politica aplicației 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 **Dezactivare politică Kaspersky Security Center** în setările opțiunii Protecție prin parolă.

Eliminare cheie

Nu există considerații sau limitări speciale.

Eliminare/modificare/restaurare aplicație

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.

Restabilire acces la date de pe unități 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.

Vizualizare rapoarte

Nu există considerații sau limitări speciale.

Restaurare din backup

Nu există considerații sau limitări speciale.

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.

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 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.

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.
- Activități de scanare.

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.

Cum se creează o excludere de la scanare în Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Setări generale** → **Excluderi**.
6. În secțiunea **Scan exclusions and trusted applications**, fă clic pe butonul **Settings**.
7. În fereastra **Zonă de încredere**, selectați fila **Excluderi de la scanare**.

   Acest lucru va deschide o fereastră care conține lista excluderilor.
8. Bifați caseta de selectare **Îmbinare valori 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.
9. 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. Dacă a fost generată o listă locală, după dezactivarea acestei funcționalități, Kaspersky Endpoint Security continuă să excludă din scanări fișierele listate.
10. Faceți clic pe butonul **Adăugare**.
11. Pentru a exclude un fișier sau un director de la scanare:

    a. În secțiunea **Proprietăți**, bifați caseta de selectare **Fișier sau director**.

    b. Faceți clic pe linkul **Selectare fișier sau director** din secțiunea **Descriere excludere de la scanare** pentru a deschide fereastra **Nume al fișierului sau al directorului**.

    c. 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 **Răsfoire**.

       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 din directorul denumit `Folder` și din subdirectoarele sale. Masca trebuie să includă cel puțin un nivel de imbricare. Masca `C:\**\*.txt` nu este o mască validă.

- Caracterul `?` (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.

d. În fereastra **Nume al fișierului sau al directorului**, faceți clic pe **OK**.

În secțiunea **Descriere excludere de la scanare** din fereastra **Excluderi de la scanare** apare un link către fișierul sau directorul adăugat.

12. Pentru a exclude de la scanare obiecte cu un anumit nume:

a. În secțiunea **Proprietăți**, bifați caseta de selectare **Nume obiect**.

b. Faceți clic pe linkul **Introducere nume obiect** în secțiunea **Descriere excludere de la scanare** pentru a deschide fereastra **Nume obiect**.

c. 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.

d. Faceți clic pe **OK** în fereastra **Nume obiect**.

În secțiunea **Descriere excludere de la scanare** din fereastra **Excluderi de la scanare** apare un link către numele obiectului.

13. Dacă doriți să excludeți un fișier individual din scanări:

a. În secțiunea **Proprietăți**, bifați caseta de selectare **Hash obiect**.

b. Faceți clic pe linkul de introducere a hash-ului obiectului pentru a deschide fereastra **Hash obiect**.

c. Introduceți hash-ul fișierului sau selectați fișierul făcând clic pe butonul **Răsfoire**.

Dacă fișierul este modificat, va fi modificat și hash-ul fișierului. Dacă se întâmplă acest lucru, fișierul modificat nu va fi adăugat la excluderi.

d. Faceți clic pe **OK** în fereastra **Hash obiect**.

În blocul **Descriere excludere de la scanare** din fereastra **Excluderi de la scanare** apare un link către obiect.

14. Dacă este necesar, în câmpul **Comentariu**, introdu o descriere succintă a excluderii de la scanare pe care o creezi.

15. Specifică apoi componentele aplicației Kaspersky Endpoint Security care trebuie să utilizeze excluderea de la scanare:

a. Dacă faci clic pe linkul **oricare** din secțiunea **Descriere excludere de la scanare** pentru a activa linkul **Selectare componente**.

b. Faceți clic pe linkul **Selectare componente** pentru a deschide fereastra **Componente protecție**.

c. Bifați casetele de selectare de lângă componentele pentru care trebuie aplicată excluderea de la scanare.

d. În fereastra **Componente protecție**, faceți clic pe **OK**.

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.

16. Puteți utiliza caseta de selectare pentru a opri o excludere în orice moment.

17. Salvați-vă modificările.

Cum se creează o excludere de la scanare în Web Console și Cloud Console

1. În fereastra principală a Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.

2. Faceți clic pe numele politicii Kaspersky Endpoint Security pentru computerele pe care doriți să adăugați o excludere.

   Se deschide fereastra de proprietăți a politicii.

3. Selectați fila **Setări aplicație**.

4. Selectați **General settings** → **Exclusions**.

5. În blocul **Excluderi de la scanare și aplicații de încredere**, faceți clic pe linkul **Excluderi de la scanare**.

6. Bifați caseta de selectare **Îmbinare valori 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.

7. 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. Dacă a fost generată o listă locală, după dezactivarea acestei funcționalități, Kaspersky Endpoint Security continuă să excludă din scanări fișierele listate.

8. Faceți clic pe butonul **Adăugare**.

9. Selectați modul în care doriți să adăugați excluderea: **Fișier sau director** , **Nume obiect** sau **Hash obiect**.

10. Dacă doriți să excludeți un fișier sau director din scanări, selectați fișierul sau directorul făcând clic pe butonul **Răsfoire**.

    De asemenea, puteți introduce manual calea. 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 din directorul denumit `Folder` și din subdirectoarele sale. Masca trebuie să includă cel puțin un nivel de imbricare. Masca `C:\**\*.txt` nu este o mască validă.

    - Caracterul `?` (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.

11. Dacă doriți să excludeți un anumit tip de obiect din scanări, în câmpul **Obiect** 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 **Hash fișier**.

    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 **Componente de protecție**, selectați componentele la care doriți să se aplice excluderea scanării.

14. Dacă este necesar, în câmpul **Comentariu**, introdu o descriere succintă a excluderii de la scanare pe care o creezi.

15. Puteți utiliza comutatorul pentru a opri o excludere în orice moment.

16. Salvați-vă modificările.

[Cum se creează o excludere de scanare în interfața aplicației](#)

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul .
2. În fereastra cu setările aplicației, selectați **Amenințări și excluderi**.
3. În blocul **Excluderi**, faceți clic pe linkul **Gestionare excluderi**.
4. Faceți clic pe butonul **Adăugare**.
5. Dacă doriți să excludeți un fișier sau director din scanări, selectați fișierul sau directorul făcând clic pe butonul **Răsfoire**.

   De asemenea, puteți introduce manual calea. 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 din directorul denumit `Folder` și din subdirectoarele sale. Masca trebuie să includă cel puțin un nivel de imbricare. Masca `C:\**\*.txt` nu este o mască validă.
   - Caracterul `?` (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.
6. Dacă doriți să excludeți un anumit tip de obiect din scanări, în câmpul **Obiect** 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 fișier**.

   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.

    Puteți utiliza comutatorul pentru a opri o excludere în orice moment.
11. Salvați-vă modificările.

Exemple de mască de cale:
Căi către fișiere aflate în oricare dosar:

- Masca `*.exe` va include toate căile către fișierele care au extensia exe.
- Masca `exemplu*` va include toate căile către fișierele denumite EXEMPLU.

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\, însă nu în subdirectoarele din C:\dir\.
- Masca `C:\dir\` va include toate căile către fișierele aflate în directorul C:\dir\, însă nu în subdirectoarele din C:\dir\.
- 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\.

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.

Activarea și dezactivarea unei excluderi de la scanare

Pentru a activa și a dezactiva o excludere de la scanare:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Amenințări și excluderi**.
3. În blocul **Excluderi**, faceți clic pe linkul **Gestionare excluderi**.
4. Selectați excluderea de care ai nevoie în lista de excluderi de la scanare.

5. Utilizați comutatorul de lângă un obiect pentru a include acest obiect în domeniul de scanare sau pentru a-l exclude.

6. Salvați-vă modificările.

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 scanează 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. Cu toate acestea, o aplicație care a fost adăugată la lista de aplicații de încredere este exclusă de la scanări de către Kaspersky Endpoint Security.

De exemplu, dacă presupui obiectele utilizate de aplicația Microsoft Windows Notepad standard ca fiind sigure fără scanare, ceea ce înseamnă că ai încredere în această aplicație, poți adăuga Microsoft Windows Notepad în lista de aplicații de încredere. Scanarea va omite atunci obiectele utilizate de această aplicație.

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.

Excluderea aplicațiilor de încredere din scanare permite evitarea conflictelor de compatibilitate dintre Kaspersky Endpoint Security și alte programe (de exemplu, problema scanării duble a traficului de rețea al unui computer terț de către Kaspersky Endpoint Security și de altă aplicație antivirus), crescând astfel performanțele computerului, aspect critic în cazul utilizării aplicațiilor server.

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 din scanarea Kaspersky Endpoint Security cu ajutorul excluderilor de la scanare.

Cum se adaugă o aplicație în lista de încredere din Consola de administrare (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** 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 **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Setări generale** → **Excluderi**.
6. În secțiunea **Scan exclusions and trusted applications**, fă clic pe butonul **Settings**.
7. În fereastra **Trusted zone**, selectați fila **Trusted applications**.

   Acest lucru va deschide o fereastră care conține lista aplicațiilor de încredere.
8. Bifați caseta de selectare **Îmbinare valori 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.
9. 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. Dacă a fost generată o listă locală, după dezactivarea acestei funcționalități, Kaspersky Endpoint Security continuă să excludă din scanări aplicațiile de încredere listate.
10. Faceți clic pe butonul **Adăugare**.
11. În fereastra deschisă, introduceți 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 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.
12. Configurați setările avansate pentru aplicația de încredere (consultați tabelul de mai jos).
13. Puteți utiliza caseta de selectare pentru a exclude o aplicație din zona de încredere în orice moment.
14. Salvați-vă modificările.

[Cum se adaugă o aplicație în lista de încredere din Web Console și Cloud Console]

1. În fereastra principală a Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security pentru computerele pe care doriți să adăugați aplicația la lista de încredere.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Selectați **General settings** → **Exclusions**.
5. În blocul **Excluderi de la scanare și aplicații de încredere**, faceți clic pe linkul **Aplicații de încredere**.

   Acest lucru va deschide o fereastră care conține lista aplicațiilor de încredere.
6. Bifați caseta de selectare **Îmbinare valori 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.
7. 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. Dacă a fost generată o listă locală, după dezactivarea acestei funcționalități, Kaspersky Endpoint Security continuă să excludă din scanări aplicațiile de încredere listate.
8. Faceți clic pe butonul **Adăugare**.
9. În fereastra deschisă, introduceți 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 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. Puteți utiliza caseta de selectare pentru a exclude o aplicație din zona de încredere în orice moment.
12. Salvați-vă modificările.

[Cum se adaugă o aplicație în lista de încredere din interfața aplicației]

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Amenințări și excluderi**.
3. În blocul **Excluderi**, faceți clic pe linkul **Specificare aplicații de încredere**.
4. În fereastră, faceți clic pe butonul **Adăugare**.
5. Selectați fișierul executabil al aplicației de încredere.

   De asemenea, puteți introduce manual calea. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști.

   > 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 ignorăprogramul 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 (consultați tabelul de mai jos).
7. Puteți utiliza comutatorul pentru a exclude o aplicație din zona de încredere în orice moment.
8. Salvați-vă modificările.

Setările aplicației de încredere

Parametru	Descriere
Nu scana fișiere deschise	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. Activitatea aplicației este monitorizată prin următoarele componente: Behavior Detection, Exploit Prevention, Host Intrusion Prevention, Remediation Engine și Firewall.
Nu moșteni restricții de la procesul părinte (aplicație)	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 aplicațiilor secundare	Kaspersky Endpoint Security nu va monitoriza activitatea fișierelor sau activitatea de rețea a aplicațiilor care sunt pornite de această aplicație.
Permitere interacțiune cu	Autoprotecția Kaspersky Endpoint Security blochează toate încercările de a gestiona serviciile aplicațiilor de pe un computer la distanță. Dacă această casetă de selectare

interfața Kaspersky Endpoint Security	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 *(disponibil numai în consola Kaspersky Security Center)*	Kaspersky Endpoint Security nu va monitoriza cererile aplicației de încredere pentru ca obiectele să fie scanate de componenta de protecție AMSI.
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.
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.

Activarea și dezactivarea regulilor pentru zona de încredere pentru o aplicație din lista de aplicații de încredere

Pentru a activa sau a dezactiva acțiunea aplicată de regulile pentru zona de încredere asupra unei aplicații din lista de aplicații de încredere:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Amenințări și excluderi**.
3. În blocul **Excluderi**, faceți clic pe linkul **Specificare aplicații de încredere**.
4. În lista de aplicații de încredere, selectați aplicația de încredere respectivă.
5. Utilizați comutatorul din coloana **Stare** pentru a include o aplicație de încredere în domeniul de scanare sau pentru a o exclude.
6. Salvați-vă modificările.

Folosirea depozitului de certificate de sistem 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*.

Pentru a începe să folosești depozitul de certificate de sistem de încredere:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Amenințări și excluderi**.
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.

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\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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra de setări a aplicației, selectați secțiunea **Rapoarte și zone de stocare**.
3. Dacă doriți să limitați perioada de stocare pentru copiile de rezervă ale fișierelor, bifați caseta de selectare **Stocare obiecte nu mai mult de N zile** din blocul **Copie de rezervă**. În câmpul din dreapta casetei de selectare **Stocare obiecte nu mai mult de N zile**, specifică perioada maximă de stocare pentru copiile fișierelor din 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 se atinge limita maximă, aplicația Kaspersky Endpoint Security șterge automat cele mai vechi fișiere din Copie de rezervă, astfel încât dimensiunea maximă să nu fie depășită.

Pentru a configura dimensiunea maximă pentru Copie de rezervă:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra de setări a aplicației, selectați secțiunea **Rapoarte și zone de stocare**.
3. Dacă doriți să limitați dimensiunea copiei de rezervă, bifați caseta de selectare **Limitați dimensiunea Copiei de rezervă la N MB** din blocul **Copie de rezervă**. Specificați dimensiunea maximă pentru copia de rezervă.
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 *Infectat*, plasează o copie 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 fi dezinfectat 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 din sistemul de operare Microsoft Windows 8 (consultați *fișierele de ajutor Microsoft Windows 8* 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, faceți clic pe **Mai multe instrumente** → **Stocare**.

   Se deschide fereastra **Copie de rezervă**.
2. În tabelul din fereastra **Copie de rezervă**, selectați unul sau mai multe fișiere copiate de rezervă.
3. Faceți clic pe butonul **Restaurare**.

   Kaspersky Endpoint Security restaurează toate fișierele din copiile de rezervă selectate în directoarele lor inițiale.

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, faceți clic pe **Mai multe instrumente** → **Stocare**.

   Se deschide fereastra **Copie de rezervă**.

2. Selectați copiile de rezervă ale fișierelor pe care doriți să le ștergeți din Copie de rezervă și faceți clic pe butonul **Ștergere**. De asemenea, puteți șterge toate fișierele din Copie de rezervă făcând clic pe butonul **Ștergere toate fișierele**.

Kaspersky Endpoint Security șterge copiile de rezervă selectate ale fișierelor din 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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul .
2. În fereastra de setări a aplicației, selectați secțiunea **Interfață**.
3. În secțiunea **Notificări**, faceți clic pe butonul **Configurare notificări**.

   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 **Salvare în raport local** și **Salvare în Jurnal evenimente Windows**.

   Evenimentele ale căror casete de selectare sunt bifate în coloana **Salvare în raport local** sunt afișate în **Jurnale aplicații și servicii** din secțiunea **Jurnal evenimente Kaspersky**. Evenimentele ale căror casete de selectare sunt bifate în coloana **Salvare în Jurnal evenimente Windows** sunt afișate în **Jurnale Windows** în secțiunea **Aplicație**. Pentru a deschide jurnalele de evenimente, selectați **Start** → **Control Panel** → **Administration** → **Event Viewer**.

6. Salvați-vă modificările.

Configurarea afișării și livrării notificărilor

Pentru a configura afișarea și livrarea notificărilor:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.

2. În fereastra de setări a aplicației, selectați secțiunea **Interfață**.

3. În secțiunea **Notificări**, faceți clic pe butonul **Configurare notificări**.

   Componentele și activitățile aplicației Kaspersky Endpoint Security se afișează în partea stângă a ferestrei. În partea dreaptă a ferestrei se listează evenimentele generate pentru componenta selectată sau pentru 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 **Notificare pe ecran**, bifați casetele de selectare de lângă evenimentele necesare.

   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 **Notificare prin e-mail**, bifați casetele de selectare de lângă evenimentele necesare.

   Informațiile despre evenimentele selectate sunt livrate prin e-mail, dacă setările de livrare a notificărilor prin e-mail sunt configurate.

7. Faceți clic pe **OK**.

8. Dacă ați activat notificările prin e-mail, configurați setările pentru livrarea prin e-mail:

   a. Faceți clic pe butonul **Setări notificare e-mail**.

b. Bifați caseta de selectare **Notificare despre evenimente** pentru a activa furnizarea de informații despre evenimentele Kaspersky Endpoint Security selectate în coloana **Notificare prin e-mail**.

c. Specifică setările de livrare a notificărilor prin e-mail.

d. Faceți 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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul .

2. În fereastra de setări a aplicației, selectați secțiunea **Interfață**.

3. În secțiunea **Afișare stare aplicație în zona de notificare**, bifați casetele de selectare de lângă categoriile 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.

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\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.

Avertizări. 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.

Dacă Kaspersky Endpoint Security fse execută sub gestionarea Kaspersky Security Center, informațiile despre evenimente pot fi transmise către Serverul de administrare Kaspersky Security Center (pentru mai multe detalii, consultați *Ghidul de ajutor al Kaspersky Endpoint Security*).

Vizualizare rapoarte

Dacă un utilizator poate vizualiza rapoartele, mai poate vizualiza toate evenimentele reflectate în rapoarte.

Pentru a vizualiza rapoarte:

1. În fereastra principală a aplicației, faceți clic pe **Mai multe instrumente** → **Rapoarte**.
2. În stânga ferestrei **Rapoarte**, în lista de componente și activități, selectați 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. În mod implicit, evenimentele din raport sunt sortate în ordinea crescătoare a valorilor din celulele coloanei **Dată eveniment**.
3. Pentru a vizualiza informații detaliate despre un eveniment, selectați evenimentul în raport.

   În partea de jos a ferestrei este afișată o secțiune din 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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra de setări a aplicației, selectați secțiunea **Rapoarte și zone de stocare**.
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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra de setări a aplicației, selectați secțiunea **Rapoarte și zone de stocare**.
3. În blocul **Rapoarte**, bifați caseta de selectare **Limitare dimensiune fișier raport la N MB** 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, faceți clic pe **Mai multe instrumente** → **Rapoarte**.
2. În fereastra deschisă, 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 **Salvare raport** în partea din dreapta sus a ferestrei.

5. În fereastra care se deschide, specificați folderul de destinație pentru fișierul de raport.
6. În câmpul **Nume fișier**, tastează numele de fișier al raportului.
7. În câmpul **Tip fișier**, selectați formatul fișierului raport necesar: TXT sau CSV.
8. Salvați-vă modificările.

Golirea rapoartelor

Pentru a elimina informații din rapoarte:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra de setări a aplicației, selectați secțiunea **Rapoarte și zone de stocare**.
3. În blocul **Rapoarte**, faceți clic pe butonul **Golire**.
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 permisiunile necesare.

Kaspersky Endpoint Security va șterge toate rapoartele pentru toate componentele și activitățile aplicației.

Autoprotecția aplicației Kaspersky Endpoint Security

Kaspersky Endpoint Security protejează computerul de aplicații rău intenționate care încearcă să blocheze funcționarea Kaspersky Endpoint Security sau chiar să șteargă aplicația 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).

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 • cheile de registry 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.	✓	–
Mecanismul de apărare a gestionării externe	Tehnologia restricționează gestionarea Kaspersky Endpoint Security utilizând aplicații speciale de administrare de la distanță (cum ar fi TeamViewer sau RemotelyAnywhere).	✓	– (cu excepția Windows 7)

Activarea și dezactivarea Autoprotecției

Mecanismul de autoprotecție a aplicației Kaspersky Endpoint Security este activat în mod implicit.

Pentru a activa sau a dezactiva Autoprotecția:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra de setări a aplicației, selectați secțiunea **General**.
3. Utilizați caseta de selectare **Activare 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.

Serviciul AM-PPL este disponibil 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.

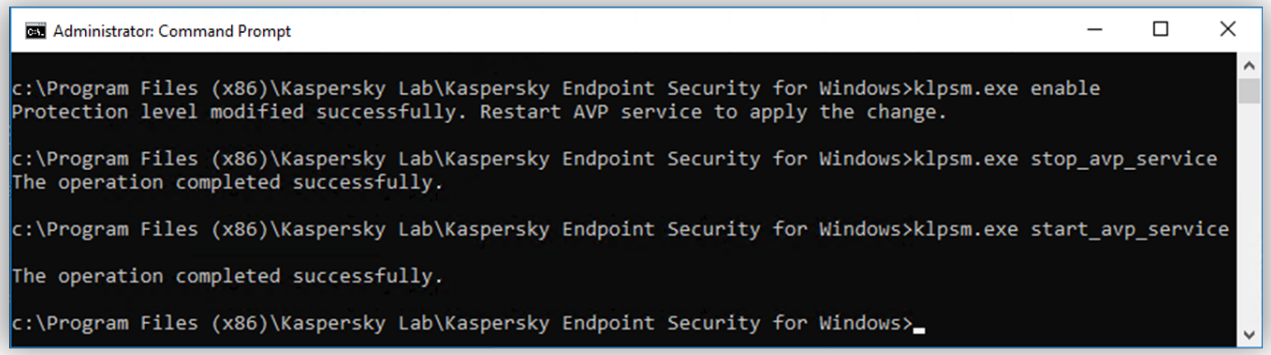
3. Deschideți directorul în care se află fișierul executabil Kaspersky Endpoint Security.

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

Activarea și dezactivarea protecției prin management extern

Protecția împotriva gestionării externe vă permite să interziceți funcționarea componentei Kaspersky Endpoint Security utilizând aplicații de gestionare de la distanță (cum ar fi TeamViewer sau RemotelyAnywhere). Tehnologia are următoarele funcții:

- protecție împotriva modificării setărilor componentei Kaspersky Endpoint Security,
- protecție împotriva gestionării serviciilor Kaspersky Endpoint Security (cum ar fi serviciul `AVP`),
- protecție împotriva opririi proceselor aplicației.

Protecția împotriva gestionării externe este disponibilă numai pe computerele pe care se execută sisteme de operare pe 32-biți. Tehnologia nu este disponibilă pentru computerele pe care se execută sisteme de operare pe 64-biți.

Pentru a activa sau dezactiva protecia împotriva gestionării externe:

1. În fereastra principală a aplicației, faceți clic pe butonul .
2. În fereastra cu setările aplicației, selectați **Setări avansate** → **General**.
3. Utilizați caseta de selectare **Permite gestionarea setărilor Kaspersky Endpoint Security prin aplicații de control de la distanță** pentru a activa sau dezactiva protecția împotriva modificărilor setărilor Kaspersky Endpoint Security. Dacă utilizați aplicații de administrare la distanță, ar trebui să permiteți gestionarea setărilor Kaspersky Endpoint Security și să adăugați aplicațiile la lista de încredere. Aplicațiilor de administrare la distanță care nu sunt de încredere nu li se permite să modifice setările Kaspersky Endpoint Security chiar și atunci când este bifată caseta de selectare **Permite gestionarea setărilor Kaspersky Endpoint Security prin aplicații de control de la distanță**. Această casetă de selectare nu este disponibilă atunci când este bifată caseta de selectare **Activare Autoprotecție**.
4. Utilizați caseta de selectare **Activare control serviciu extern** pentru a activa sau dezactiva protecția serviciilor Kaspersky Endpoint Security împotriva gestionării externe.

   Pentru a părăsi aplicația din linia de comandă, dezactivați protecția serviciilor Kaspersky Endpoint Security împotriva gestionării externe.

5. Salvați-vă modificările.

Ca urmare, atunci când mecanismele de apărare împotriva managementului extern sunt activate, Kaspersky Endpoint Security împiedică indicatorul mouse-ului să se îndrepte spre pictograma aplicației. Când un utilizator la distanță încearcă să închidă un serviciu al aplicației, apare o fereastră de sistem cu un mesaj de eroare.

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 partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Amenințări și excluderi**.
3. În blocul **Excluderi**, faceți clic pe linkul **Specificare aplicații de încredere**.
4. În fereastră, faceți clic pe butonul **Adăugare**.
5. Selectați fișierul executabil al aplicației de administrare la distanță.

   De asemenea, puteți introduce manual calea. Kaspersky Endpoint Security acceptă variabilele de mediu și caracterele `*` și `?` la introducerea unei măști.
6. Bifați caseta de selectare **Nu monitoriza activitatea aplicației**.
7. Salvați-vă modificările.

Performanța și compatibilitatea produsului Kaspersky Endpoint Security cu alte aplicații

Performanțele Kaspersky Endpoint Security

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:

- Activitate de actualizare
- Activitate de scanare completă
- Activitate de scanare a zonelor critice
- Activitate de scanare particularizată
- Activitate de 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

Utilizarea resurselor computerului de către Kaspersky Endpoint Security poate afecta performanțele altor aplicații. 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 pune în pauză activitățile planificate și poate ceda resurse altor aplicații.

Cu toate acestea, o serie de aplicații pornesc imediat ce devin disponibile resurse de procesor, lucrând în fundal. Pentru ca scanarea să nu depindă de performanțele altor aplicații, este mai bine să nu li se cedeze resurse ale sistemului de operare.

Poți porni aceste activități manual, dacă este necesar.

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. *Tehnologia de dezinfectare avansată* 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 infecții active de pe un server, activați tehnologia Dezinfectare activă pentru servere și porniți o activitate de grup *Scanare de viruși* într-un moment convenabil pentru utilizatorii serverului.

Selectarea tipurilor de obiecte detectabile

Pentru a selecta tipurile de obiecte detectabile:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra cu setările aplicației, selectați **Amenințări și excluderi**.
3. În secțiunea **Tipuri de obiecte detectate**, selectați casetele din dreptul tipurilor de obiecte pe care doriți să le detecteze Kaspersky Endpoint Security:
   - **Viruși și viermi**

Subcategorie: viruși și viermi (Viruses_and_Worms)

Nivel amenințare: 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 cu *suprascriere* își scriu codul peste o parte din codul fișierului infectat, ștergând astfel o parte din conținutul fișierului. Fișierul infectat nu mai funcționează și nu poate fi restaurat. Virușii *paraziți* modifică fișiere, lăsându-le complet sau parțial funcționale. *Virușii de companie* 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.

Viermi

La fel ca un virus clasic, codul unui vierme se activează și efectuează acțiuni periculoase 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	Nume	Descriere
Viermi e-mail	Viermi 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.
Viermi de MI	Clienți de IM	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 Internet	Se răspândesc prin camerele de 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.
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 de mai sus pentru a se răspândi (de exemplu, viermi care se răspândesc prin telefoane celulare).

- Troieni

Subcategoria: Troieni

Nivel amenințare: 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	Nume	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 descriși 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 clic	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, intruşii execută atacuri de reţea şi sporesc numărul de vizite pe un site Web, sporind numărul de reclame banner afişate.
Troian-program de descărcare	Troieni programe de descărcare	Ei accesează pagina Web a intrusului, descarcă de pe ea alte aplicaţii rău intenţionate şi le instalează pe computerul utilizatorului. Ei pot conţine numele fişierului aplicaţiei rău intenţionate de descărcat sau îl pot primi de pe pagina Web accesată.
Trojan-Dropper	Troieni de tip Dropper	Ei conţin alţi troieni, pe care îi pot depune şi apoi instala pe unitatea de hard disc. Intruşii pot folosi programe de tipul Trojan Dropper în următoarele scopuri: • Instalarea unei aplicaţii rău intenţionate fără a fi observat de utilizator: Programele de tipul Trojan Dropper nu afişează mesaje sau afişează mesaje false care informează, de exemplu, că există o eroare într-o arhivă sau o versiune incompatibilă a sistemului de operare. • Protejarea altei aplicaţii rău intenţionate cunoscute de la detecţie: nu toate software-urile antivirus pot detecta o aplicaţie rău intenţionată din interiorul altei aplicaţii de tip Trojan Dropper.
Trojan-Notifier	Troieni de notificare	Ei informează un intrus că este accesibil computerul infectat, trimiţând intrusului informaţii 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 conţin mai mulţi troieni. Ei îl notifică pe intrus că alţi 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 folosiţi 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. Aceşti troieni găsesc date confidenţiale în fişierele de sistem şi în registru şi le trimit „stăpânului" prin e-mail, FTP, accesând pagina Web a intrusului sau într-un alt mod. Unii dintre aceşti troieni sunt încadraţi în tipuri separate descrise în acest tabel. Aceştia sunt Troieni care fură conturi bancare (Trojan-Banker), date de la utilizatori de clienţi de mesagerie instantanee (Trojan-IM) şi informaţii de la utilizatori de jocuri online (Trojan-GameThief).
Trojan-Spy	Spioni troieni	Ei îl spionează pe utilizator, colectând informaţii despre acţiunile 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 aplicaţii active. După ce primesc informaţiile, le transferă intrusului prin e-mail, FTP, accesând pagina Web a intrusului sau într-un alt mod.
Trojan-DDoS	Troieni atacatori 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) 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. Intrușii pot trimite spam către adresele pe care le-au colectat.

- instrumente periculoase

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	Nume	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 cod de program care folosește vulnerabilități din aplicația 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 computere.
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

  Subcategorie: software de advertising (Adware);

  Nivel amenințare: 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

Subcategorie: software legal care ar putea fi utilizat de infractori 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 Internet pentru FTP, HTTP și Telnet.

Cu toate acestea, dacă intruşii 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	Nume	Descriere
Client-IRC	Clienți de chat Internet	Utilizatorii instalează aceste programe pentru a vorbi cu alte persoane în camere Internet Relay Chats. Intruşii îi folosesc pentru a răspândi malware.
Dialer	Programe de apelare automată	Ei pot stabili conexiuni telefonice către un modem în mod ascuns.
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. Intruşii 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. Intruşii 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. Intruşii le instalează pe computerul utilizatorului pentru a deschide accesul la distanță prin FTP.
Server-Proxy	Proxy server	Ele funcționează ca servere proxy. Intruşii le instalează pe computerul utilizatorului pentru a trimite spam în numele utilizatorului.
Server-Telnet	Servere Telnet	Ele funcționează ca servere Telnet. Intruşii 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.

- Alt software legitim care poate fi utilizat de infractori pentru a aduce daune computerului sau datelor personale

Subcategorie: software legal care ar putea fi utilizat de infractori 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 Internet pentru FTP, HTTP și Telnet.

Cu toate acestea, dacă intruşii 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	Nume	Descriere
Client-IRC	Clienți de chat Internet	Utilizatorii instalează aceste programe pentru a vorbi cu alte persoane în camere Internet Relay Chats. Intruşii îi folosesc pentru a răspândi malware.
Dialer	Programe de apelare automată	Ei pot stabili conexiuni telefonice către un modem în mod ascuns.
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. Intruşii 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. Intruşii 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. Intruşii le instalează pe computerul utilizatorului pentru a deschide accesul la distanță prin FTP.
Server-Proxy	Proxy server	Ele funcționează ca servere proxy. Intruşii le instalează pe computerul utilizatorului pentru a trimite spam în numele utilizatorului.
Server-Telnet	Servere Telnet	Ele funcționează ca servere Telnet. Intruşii 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.

- **Obiecte arhivate a căror arhivare poate fi utilizată pentru a proteja cod rău intenționat**

  Kaspersky Endpoint Security scanează obiecte comprimate și modulul de dezarhivare din arhive SFX (cu autoextragere).

  Pentru a ascunde programe periculoase de aplicații antivirus, intruși le arhivează folosind arhivatoare speciale sau creează fișiere împachetate multiplu.

  Analiștii de viruși de la Kaspersky au identificat arhivatoarele care sunt cele mai populare în rândul hackerilor.

  În cazul în care Kaspersky Endpoint Security detectează un astfel de arhivator într-un fișier, fișierul conține cel mai probabil o aplicație rău intenționată sau o aplicație care poate fi folosită de infractori pentru a dăuna computerului sau datelor personale.

  Kaspersky Endpoint Security identifică următoarele tipuri de programe:

  - *Fișiere împachetate care pot fi dăunătoare* – folosite pentru a ambala programe malware, cum ar fi viruși, viermi și troieni.
  - *Fișiere împachetate multiplu* (nivel de amenințare mediu) – obiectul a fost arhivat de trei ori cu unul sau cu mai multe arhivatoare.

- **Fișiere împachetate multiplu**

Kaspersky Endpoint Security scanează obiecte comprimate și modulul de dezarhivare din arhive SFX (cu autoextragere).

Pentru a ascunde programe periculoase de aplicații antivirus, intruși le arhivează folosind arhivatoare speciale sau creează fișiere împachetate multiplu.

Analiștii de viruși de la Kaspersky au identificat arhivatoarele care sunt cele mai populare în rândul hackerilor.

În cazul în care Kaspersky Endpoint Security detectează un astfel de arhivator într-un fișier, fișierul conține cel mai probabil o aplicație rău intenționată sau o aplicație care poate fi folosită de infractori pentru a dăuna computerului sau datelor personale.

Kaspersky Endpoint Security identifică următoarele tipuri de programe:

- *Fișiere împachetate care pot fi dăunătoare* – folosite pentru a ambala programe malware, cum ar fi viruși, viermi și troieni.
- *Fișiere împachetate multiplu* (nivel de amenințare mediu) – obiectul a fost arhivat de trei ori cu unul sau cu mai multe arhivatoare.

4. Salvați-vă modificările.

Activarea sau dezactivarea tehnologiei Dezinfectare avansată

Dacă Kaspersky Endpoint Security nu poate opri din rulare o aplicație rău intenționată, puteți utiliza tehnologia Dezinfectare avansată. În mod implicit, tehnologia Dezinfectare avansată este dezactivată, deoarece aceasta necesită o cantitate semnificativă de resurse de procesare. Prin urmare, puteți activa Dezinfectarea avansată doar atunci când lucrați cu amenințări active.

Tehnologia Dezinfectare avansată funcționează diferit în cazul serverelor și stațiilor de lucru. Pentru a utiliza tehnologia pe servere, este necesar să activați Dezinfectarea avansată imediată în proprietățile activității *Scanare antivirus*. Această cerință nu este necesară pentru a putea utiliza tehnologia pe stațiile de lucru.

Pentru a activa sau dezactiva tehnologia Dezinfectare avansată:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.
2. În fereastra de setări a aplicației, selectați secțiunea **General**.
3. În secțiunea **Mod protecție**, bifați sau debifați caseta de selectare **Activare tehnologie Dezinfectare avansată** 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 activă. Când activitatea de dezinfectare este finalizată, computerul este repornit.

Activarea sau dezactivarea modului de economisire a energiei

Pentru a activa sau a dezactiva modul de conservare a energiei:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul .
2. În fereastra cu setările aplicației, selectați **Amenințări și excluderi**.
3. În secțiunea **Performanță**, utilizați caseta de selectare **Amână activități planificate la funcționarea cu alimentare de la baterie** pentru a activa sau dezactiva modul de economisire a energiei.

   Atunci când modul de conservare a energiei este activat și computerul funcționează cu alimentare de la baterie, următoarele activități nu sunt executate, chiar dacă sunt planificate:

   - Activitate de actualizare
   - Activitate de scanare completă
   - Activitate de scanare a zonelor critice
   - Activitate de scanare particularizată
   - Activitate de verificare integritate
4. Salvați-vă modificările.

Activarea sau dezactivarea cedării de resurse pentru alte aplicații

Pentru a activa sau a dezactiva cedarea de resurse pentru alte aplicații:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul .
2. În fereastra de setări a aplicației, selectați secțiunea **General**.
3. În secțiunea **Performanță**, utilizați caseta de selectare **Cedare resurse pentru alte aplicații** pentru a activa sau dezactiva cedarea resurselor către alte aplicații.

   Atunci când este configurat să cedeze resurse altor aplicații, Kaspersky Endpoint Security amână activitățile planificate care încetinesc alte aplicații:

   - Activitate de actualizare
   - Activitate de scanare completă
   - Activitate de scanare a zonelor critice
   - Activitate de scanare particularizată
   - Activitate de verificare integritate

   În mod implicit, aplicația este configurată să cedeze resurse pentru alte aplicații.
4. Salvați-vă modificările.

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.

  Pentru aceasta, trebuie să salvezi fișierul de configurare în același director în care se găsește kitul de distribuție.

- Efectuarea instalării la distanță a Kaspersky Endpoint Security, prin intermediul Kaspersky Security Center, cu setări predefinite.

- Migrarea setărilor Kaspersky Endpoint Security de pe un computer pe altul.

Pentru a crea un fișier de configurare:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul .
2. În fereastra cu setările aplicației, selectați **Gestionare setări**.
3. Faceți clic pe butonul **Export**.
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. Faceți clic pe butonul **Save**.

Pentru a importa setările Kaspersky Endpoint Security dintr-un fișier de configurare:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul .
2. În fereastra cu setările aplicației, selectați **Gestionare setări**.
3. Faceți clic pe butonul **Import**.
4. În fereastra care se deschide, introduceți calea către fișierul de configurare.
5. Faceți clic pe butonul **Deschidere**.

Toate valorile setărilor Kaspersky Endpoint Security vor fi setate conform fișierului de configurare selectat.

Restaurarea setărilor implicite ale aplicației

Puteți restaura oricând setările recomandate de Kaspersky for Endpoint Security. Când setările sunt restabilite, nivelul de securitate **Recomandat** este setat pentru toate componentele de protecție.

Pentru a restaura setările implicite ale aplicației:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul .
2. În fereastra cu setările aplicației, selectați **Gestionare setări**.
3. Faceți clic pe butonul **Restaurare**.
4. Faceți clic pe butonul **Save**.

Mesajele între utilizatori și administrator

Componentele Application Control, Control dispozitive și Control Web și Control adaptiv al anomaliilor 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 Control dispozitive.

- 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 Control Web.

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 **Server de administrare** din arborele consolei de administrare, selectați fila **Evenimente**.

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 **Selectare evenimente**, selectați **Solicitare utilizator**.

4. Selectați mesajul trimis către administrator.

5. Faceți clic butonul **Deschide fereastra de proprietăți a evenimentului** în partea dreaptă a spațiului de lucru Consolă de administrare.

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 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.
- **Criptarea unităților amovibile**. 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**. Poți selecta o tehnologie de criptare: Kaspersky Disk Encryption sau BitLocker Drive Encryption (denumită și „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. Puteți utiliza, de asemenea, tehnologia Single Sign-On (SSO), care vă permite să vă conectați automat la sistemul de operare folosind numele de utilizator și parola din contul 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**, toate sectoarele se criptează după un interval de 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 12 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.

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 Express Cache.
- 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 Think Center 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 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 amovibile 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

Criptarea Full disk encryption folosind tehnologia 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.

Pentru a efectua o criptare Full disk encryption folosind tehnologia Kaspersky Disk Encryption:

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Data Encryption → Full Disk Encryption**.
6. În lista verticală **Tehnologie de criptare**, selectați opțiunea **Kaspersky Disk Encryption**.

   Tehnologia Kaspersky Disk Encryption nu poate fi folosită dacă computerul are unități de hard disk criptate de BitLocker.

7. În lista verticală **Mod criptare**, selectați **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.

8. Configurează reguli pentru adăugarea conturilor Agent autentificare în timpul criptării discului. Agentul îi permite unui utilizator să finalizeze autentificarea pentru accesarea unităților de disk criptate și să încarce sistemul de operare. Pentru a adăuga automat conturi Agent de autentificare, configurați următoarele setări:

- **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.

- **Creează 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.

Dacă ați dezactivat crearea automată a conturilor Agent de autentificare, puteți adăuga manual conturi Agent de autentificare utilizând activitatea *Gestionare conturi*. De asemenea, puteți utiliza această activitate pentru a modifica setările conturilor Agent de autentificare care au fost create automat.

9. Pentru confortul utilizatorului, puteți salva numele de utilizator în memoria Agentului de autentificare pentru ca utilizatorul să introducă doar parola data viitoare când se conectează la sistem. Pentru aceasta, bifați caseta de selectare **Salvare nume de utilizator introdus în Agentul de autentificare**.

10. Selectați una dintre următoarele metode de criptare:

    - Dacă dorești să aplici criptarea numai acelor sectoare de pe unitatea de hard disk care sunt ocupate de fișiere, bifați caseta de selectare **Criptează doar spațiul de disc utilizat**.

      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 dorești să aplici criptarea întregii unități de hard disk, debifați caseta de selectare **Criptează doar spațiul de disc utilizat**.

      Dacă un dispozitiv a fost criptat anterior folosind funcția **Criptează doar spațiul de disc utilizat**, după aplicarea unei politici în modul **Se criptează toate unitățile de hard disk**, sectoarele care nu sunt ocupate de fișiere în continuare nu vor fi criptate.

11. Dacă apare o problemă de incompatibilitate hardware în timpul criptării computerului, puteți selecta caseta de selectare **Utilizare 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.

    Când funcția Legacy USB Support este activată, Agentul de Autentificare în modul BIOS nu acceptă lucrul cu simboluri 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.

12. 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.

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.

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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Data Encryption → Full Disk Encryption**.
6. În lista verticală **Tehnologie de criptare**, selectați opțiunea **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.
7. Pentru a adăuga unități de hard disk noi la lista de unități de hard disk excluse de la criptare:

   a. Faceți clic pe butonul **Adăugare**.

      Se deschide fereastra **Adăugare dispozitive din lista Kaspersky Security Center**.

   b. În fereastra **Toate dispozitivele din lista Kaspersky Security Center**, specifică valorile pentru următorii parametri: **Nume**, **Computer**, **Tip de disc** și **Kaspersky Disk Encryption**.

   c. Faceți clic pe butonul **Împrospătare**.

   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. Faceți clic pe **OK**.

   Unitățile de hard disk selectate apar în tabelul **Nu se criptează următoarele unități hard disk**.
8. Dacă doriți să eliminați unități de hard disk din tabelul de excluderi, selectați una sau mai multe linii în tabelul **Nu se criptează următoarele unități hard disk** și faceți clic pe butonul **Ștergere**.

   Pentru a selecta linii multiple în tabel, selectați-le în timp ce țineți apăsată tasta **CTRL**.
9. 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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Data Encryption** → **Full Disk Encryption**.
6. În lista verticală **Tehnologie de criptare**, selectați opțiunea **Kaspersky Disk Encryption**.

   Înregistrările care corespund unităților de hard disk excluse de la criptare apar în tabelul **Nu se criptează următoarele unități hard disk**.
7. 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. Faceți clic pe linkul **Exportare**.
   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. Faceți clic pe butonul **Save**.

      Kaspersky Endpoint Security exportă întreaga listă de excluderi în fișierul XML.
8. Pentru a importa lista de reguli:
   a. Faceți clic pe butonul **Import**.
   b. În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de excluderi.
   c. Faceți clic pe butonul **Deschidere**.

      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.
9. 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 Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security pentru computerele pe care doriți să exportați sau să importați o listă de excluderi.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Selectați **Data Encryption** → **Full Disk Encryption**.
5. Selectați tehnologia **Kaspersky Disk Encryption** și urmați linkul pentru a configura setările.

   Setările de criptare se deschid.
6. Faceți clic pe linkul **Excluderi**.
7. Pentru a exporta lista de reguli:
   a. Selectați excluderile pe care doriți să le exportați.
   b. Faceți clic pe butonul **Export**.
   c. Confirmați că doriți să exportați numai excluderile selectate sau exportați întreaga listă de excluderi.
   d. 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.
   e. Faceți clic pe butonul **Save**.

      Kaspersky Endpoint Security exportă întreaga listă de excluderi în fișierul XML.
8. Pentru a importa lista de reguli:
   a. Faceți clic pe butonul **Import**.
   b. În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de excluderi.
   c. Faceți clic pe butonul **Deschidere**.

      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.
9. Salvați-vă modificările.

Activarea tehnologiei Single Sign-On (SSO)

Tehnologia Single Sign-On (SSO) vă permite să vă conectați automat la sistemul de operare folosind acreditările Agentului 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.

Tehnologia Single Sign-On nu este compatibilă cu furnizori terți de acreditări pentru cont.

Cum se activează tehnologia Single Sign-On în Consola de administrare. (MMC)

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Data Encryption** → **Setări de criptare comune**.
6. În blocul **Setări parolă**, faceți clic pe butonul **Setări**.
7. În fereastra care se deschide, în fila **Agent de Autentificare**, bifați caseta de selectare **Utilizare tehnologie Single Sign-On (SSO)** .
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.

Cum se activează utilizarea tehnologiei Single Sign-On în Web Console

1. În fereastra principală a Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security pentru computerele pe care doriți să activați utilizarea tehnologiei Single Sign-On.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Accesați **Data Encryption** →**Full Disk Encryption**.
5. Selectați tehnologia **Kaspersky Disk Encryption** și urmați linkul pentru a configura setările.

   Setările de criptare se deschid.
6. În secțiunea **Setări parolă**, bifați caseta de selectare **Utilizare tehnologie Single Sign-On (SSO)**.
7. Faceți clic pe **OK**.

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. După aceea, Kaspersky Endpoint Security înlocuiește parola contului Agentului de autentificare cu parola contului de 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 Agentului 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 Consola de administrare, accesați directorul **Server de administrare** → **Activități**.

   Lista activităților se deschide.

2. Faceți clic pe butonul **Activitate nouă**.

Expertul de activitate pornește. Urmează instrucțiunile din expert.

Pasul 1. Selectarea tipului activității

Selectați **Kaspersky Endpoint Security for Windows (11.6.0)** → **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 **Executare activitate după terminarea Expertului**. 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 Consolei Web, selectează **Devices** → **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe butonul **Adăugare**.

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**, selectați **Kaspersky Endpoint Security for Windows (11.6.0)**.
2. În lista verticală **Tip activitate**, selectați **Gestionare conturi Agent de Autentificare**.
3. În câmpul **Nume activitate**, introduceți o descriere succintă, cum ar fi `Conturi de administrator`.
4. În secțiunea **Select 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

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 **Pornire**.

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 Setări politică Full Disk Encryption. 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 **Opțiuni**.

3. Faceți clic pe **Adăugare → Comandă 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 **Permitere** pentru a defini identificatorul de securitate al contului (SID).

   Dacă ai ales să nu determini identificatorul de securitate (SID) făcând clic pe butonul **Permitere**, 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 nu este disponibil dacă adaugi o comandă pentru crearea contului de Agent de Autentificare în proprietățile activității locale **Full Disk Encryption, gestionare cont**.

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. Efectuează una dintre următoarele acțiuni:

    - Selectați opțiunea **Permitere autentificare** dacă dorești ca aplicația să permită utilizatorului care lucrează sub contul specificat în comandă accesul la dialogul de autentificare în Agentul de Autentificare.

    - Selectați opțiunea **Blocare autentificare** dacă dorești ca aplicația să blocheze utilizatorului care lucrează sub contul specificat în comandă accesul la dialogul de autentificare în Agentul de Autentificare.

12. Salvați-vă modificările.

[Cum se adaugă un cont Agent de Autentificare prin Web Console]

1. În fereastra principală a Consolei Web, selectează **Devices → Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe activitatea **Gestionare conturi Agent de autentificare** a aplicației Kaspersky Endpoint Security.

   Se va deschide fereastra de proprietăți a activității.

3. Selectați fila **Setări aplicație**.

4. În lista de conturi Agent de Autentificare, faceți clic pe butonul **Adăugare**.

   Aceasta pornește Expertul de gestionare a contului Agent de Autentificare.

5. Selectați tipul de comandă **Adăugare cont**.

6. Selectați un cont de utilizator. Puteți selecta un cont din lista conturilor de domeniu sau puteți introduce manual numele contului. Faceți clic pe butonul **Next**.

   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.

   - **Creați un nou cont Agent de Autentificare pentru a înlocui contul existent**. 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.

   - **Nume utilizator**. Numele de utilizator implicit al contului Agent de autentificare corespunde numelui de domeniu al utilizatorului.

   - **Permitere autentificare pe bază de parolă**. 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.

   - **Permitere autentificare pe bază de certificat**. 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.

   - **Acces cont la datele criptate**. Configurați accesul utilizatorului la unitatea criptată. Puteți, de exemplu, dezactiva temporar autentificarea utilizatorului în loc să ștergeți contul Agent de Autentificare.

   - **Comentariu**. 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 **Pornire**.

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 **Opțiuni**.
3. Faceți clic pe **Adăugare** → **Comandă 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 **Permitere** pentru a defini identificatorul de securitate al contului (SID).

   Dacă ai ales să nu determini identificatorul de securitate (SID) făcând clic pe butonul **Permitere**, 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 pe baza contului 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 pentru toate conturile de Agent de autentificare create pe baza contului 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 Consolei Web, selectează **Devices** → **Tasks**.

   Lista activităților se deschide.

2. Faceți clic pe activitatea **Gestionare conturi Agent de autentificare** a aplicației Kaspersky Endpoint Security.

   Se va deschide fereastra de proprietăți a activității.

3. Selectați fila **Setări aplicație**.

4. În lista de conturi Agent de Autentificare, faceți clic pe butonul **Adăugare**.

   Aceasta pornește Expertul de gestionare a contului Agent de Autentificare.

5. Selectați tipul de comandă **Editare cont**.

6. Selectați un cont de utilizator. Puteți selecta un cont din lista conturilor de domeniu sau puteți introduce manual numele contului. Faceți clic pe butonul **Next**.

   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.

   - **Creați un nou cont Agent de Autentificare pentru a înlocui contul existent**. 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.

   - **Nume utilizator**. Numele de utilizator implicit al contului Agent de autentificare corespunde numelui de domeniu al utilizatorului.

   - **Permitere autentificare pe bază de parolă**. 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.

   - **Permitere autentificare pe bază de certificat**. 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.

   - **Acces cont la datele criptate**. Configurați accesul utilizatorului la unitatea criptată. Puteți, de exemplu, dezactiva temporar autentificarea utilizatorului în loc să ștergeți contul Agent de Autentificare.

   - **Comentariu**. 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 **Pornire**.

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 **Opțiuni**.
3. Faceți clic pe **Adăugare** → **Comandă 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 **Permitere** pentru a defini identificatorul de securitate al contului (SID).

   Dacă ai ales să nu determini identificatorul de securitate (SID) făcând clic pe butonul **Permitere**, 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 Consolei Web, selectează **Devices** → **Tasks**.

   Lista activităților se deschide.
2. Faceți clic pe activitatea **Gestionare conturi Agent de autentificare** a aplicației Kaspersky Endpoint Security.

   Se va deschide fereastra de proprietăți a activității.
3. Selectați fila **Setări aplicație**.
4. În lista de conturi Agent de Autentificare, faceți clic pe butonul **Adăugare**.

   Aceasta pornește Expertul de gestionare a contului Agent de Autentificare.
5. Selectați tipul de comandă **Eliminare cont**.
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 **Pornire**.

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 directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Dispozitive**.
4. Fă dublu clic pentru a deschide fereastra cu proprietățile computerului.
5. În fereastra cu proprietățile computerului, selectați secțiunea **Activități**.

   Lista activităților locale se deschide.
6. Selectați activitatea **Gestionare conturi Agent de autentificare**.
7. În proprietățile activității, selectați secțiunea **Opțiuni**.

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 Consolei Web. selectați **Dispozitive** → **Dispozitive gestionate**.
2. Faceți clic pe numele computerului pe care doriți să vizualizați lista conturilor Agent de Autentificare.

   Se vor deschide proprietățile computerului.
3. În fereastra cu proprietățile computerului, selectați secțiunea **Activități**.

   Lista activităților locale se deschide.
4. Selectați activitatea **Gestionare conturi Agent de autentificare**.
5. În proprietățile activității, selectați fila **Setări aplicație**.

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
- Aladdin-RD JaCarta PKI
- 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 activă care permite criptarea datelor.

Pentru a decripta unități de hard disk:

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Data Encryption** → **Full Disk Encryption**.
6. În lista verticală **Tehnologie de criptare**, selectați tehnologia cu care vor fi criptate unitățile de hard disk.
7. Efectuează una dintre următoarele acțiuni:
   - În lista verticală **Mod criptare**, selectați opțiunea **Se decriptează toate unitățile 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.
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.

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.

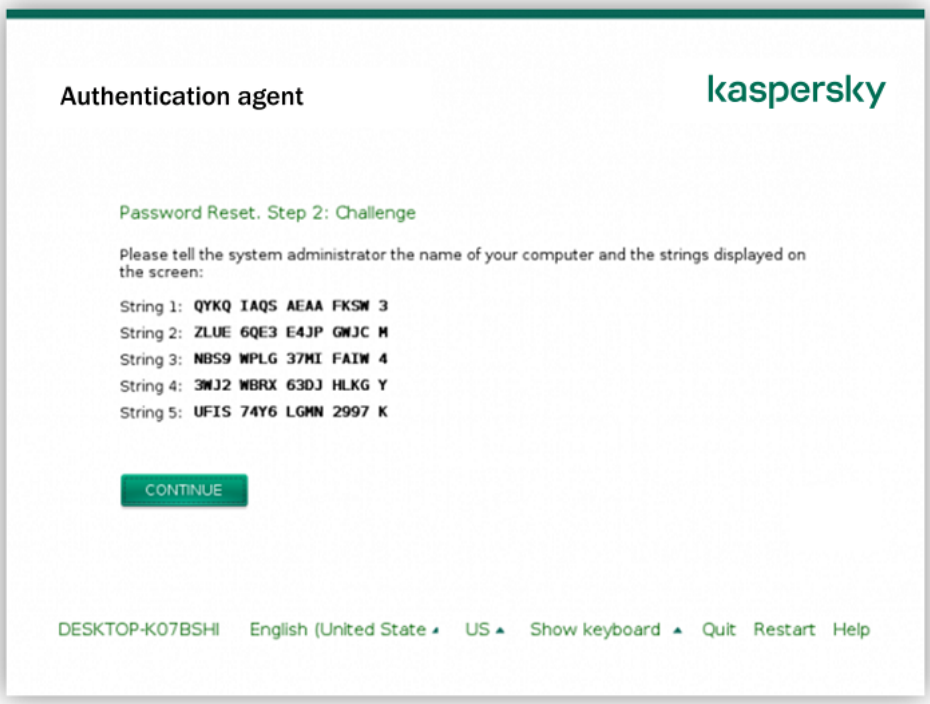
Restabilirea accesului la o unitate protejată de tehnologia Kaspersky Disk Encryption

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).

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 **V-ați uitat parola** 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 directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Dispozitive**.
4. În fila **Dispozitive**, selectați computerul utilizatorului care solicită accesul la datele criptate și faceți clic dreapta pe el pentru a deschide meniul contextual.
5. În meniul contextual, selectați opțiunea **Acordă acces în modul offline**.
6. În fereastra care se deschide, selectați fila **Agent de Autentificare**.
7. În secțiunea **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.
8. În lista verticală **Cont**, selectați numele contului de Agent de Autentificare al utilizatorului care a solicitat recuperarea accesului la unitate.
9. În lista verticală **Unitate de hard disk**, selectați unitatea de hard disk criptată pentru care trebuie să recuperezi accesul.
10. În secțiunea **Solicitare utilizator**, introdu blocurile din solicitare dictate de către 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.

[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 Consolei Web. selectați **Dispozitive** → **Dispozitive gestionate**.
2. Bifați caseta de selectare de lângă numele computerului la a cărui unitate doriți să restaurați accesul.
3. Faceți clic pe butonul **Partajați acest dispozitiv offline**.
4. În fereastra care se deschide, selectați fila **Agent de Autentificare**.
5. În lista verticală **Cont**, 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 directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Dispozitive**.
4. În fila **Dispozitive**, selectați computerul utilizatorului care solicită accesul la datele criptate și faceți clic dreapta pe el pentru a deschide meniul contextual.
5. În meniul contextual, selectați opțiunea **Acordă acces în modul offline**.
6. În fereastra care se deschide, selectați fila **Data Encryption**.
7. În fila **Data Encryption**, faceți clic pe butonul **Răsfoire**.
8. 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.

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 Consolei Web. selectați **Dispozitive** → **Dispozitive gestionate**.
2. Bifați caseta de selectare de lângă numele computerului la ale cărui date doriți să restaurați accesul.
3. Faceți clic pe butonul **Partajați acest dispozitiv offline**.
4. Selectați secțiunea **Data Encryption**.
5. Faceți clic pe butonul **Selectare fișier** 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 **Salvare cheie** 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.

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.

Pentru detalii despre actualizarea în siguranță a sistemului de operare, consultați Baza de cunoștințe pentru asistență tehnică.

Actualizarea automată a sistemului de operare este disponibilă în următoarele condiții:

1. Sistemul de operare este actualizat prin WSUS (Windows Server Update Services).
2. Windows 10 versiunea 1607 (RS1) sau o versiune ulterioară este instalat pe computer.
3. Kaspersky Endpoint Security versiunea 11.2.0 sau o versiune ulterioară este instalată pe computer.

Dacă sunt îndeplinite toate condițiile, puteți actualiza sistemul de operare în mod obișnuit.

Dacă utilizați tehnologia Kaspersky Disk Encryption (FDE) și Kaspersky Endpoint Security for Windows versiunea 11.1.0 sau 11.1.1 este instalat pe computer, nu este necesar să decriptați hard diskurile pentru a actualiza Windows 10.

Pentru a actualiza sistemul de operare, trebuie să faceți următoarele:

1. Înainte de actualizarea sistemului, copiați driverele numite cm_km.inf, cm_km.sys, klfde.cat, klfde.inf, klfde.sys, klfdefsf.cat, klfdefsf.inf și klfdefsf.sys într-un director local. De exemplu, C:\fde_drivers.

2. Rulați instalarea actualizării sistemului cu comutatorul `/ReflectDrivers` și specificați folderul care conține driverele salvate:

   ```
   setup.exe /ReflectDrivers C:\fde_drivers
   ```

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 11.6.0.

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.

Selectarea nivelului de urmărire pentru Agentul 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 selecta nivelul de urmărire pentru Agentul de Autentificare:

1. 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.
2. Selectați nivelul de urmărire în fereastra de setări a Agentului de Autentificare:

- **Dezactivare înregistrare în jurnal depanare (implicit)**. Dacă este selectată această opțiune, aplicația nu înregistrează în jurnal informațiile despre evenimentele Agentului de Autentificare în fișierul de urmărire.

- **Activare înregistrare în jurnal depanare**. 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.

- **Activare înregistrare detaliată în jurnal**. 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 **Activare înregistrare în jurnal depanare**. Un nivel mai mare de detalii pentru înregistrări poate încetini pornirea Agentului de Autentificare și a sistemului de operare.

- **Activare înregistrare în jurnal depanare și selectare port serial**. 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.

- **Activare înregistrare detaliată în jurnal depanare și selectare port serial**. 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 **Activare înregistrare în jurnal depanare și selectare port serial**. Un nivel mai mare de detalii pentru înregistrări poate încetini pornirea Agentului de Autentificare și a sistemului de operare.

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.

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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.

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

5. În fereastra politicii, selectați **Data Encryption** → **Setări de criptare comune**.

6. În secțiunea **Șabloane**, faceți clic pe butonul **Ajutor**.

   Această acțiune deschide fereastra **Mesaje de ajutor pentru Agentul de Autentificare**.

7. Efectuează următoarele acțiuni:

   - Selectați fila **Autentificare** pentru a edita textul de ajutor afișat în fereastra Agentului de Autentificare atunci când sunt introduse acreditările contului.
   - Selectați fila **Modificare parolă** 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.

8. 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.

9. 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 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 vă permite să controlați și să gestionați Bitlocker folosind Kaspersky Security Center. BitLocker criptează volumele logice. BitLocker nu poate fi utilizat pentru criptarea unităților amovibile. Pentru detalii suplimentare despre BitLocker, consultați documentația Microsoft.

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 unei unități, BitLocker creează o cheie principală. Kaspersky Endpoint Security trimite cheia principală către Kaspersky Security Center pentru a putea restabili accesul la disc, de exemplu, dacă un utilizator a uitat parola.

Dacă un utilizator criptează un disc folosind BitLocker, Kaspersky Endpoint Security va trimite informații despre criptarea discului către Kaspersky Security Center. Cu toate acestea, Kaspersky Endpoint Security nu va trimite cheia principală către Kaspersky Security Center, astfel încât va fi imposibil să restaurați accesul la disc utilizând Kaspersky Security Center. Pentru ca BitLocker să funcționeze corect cu Kaspersky Security Center, decriptați unitatea și re-criptați-o folosind o politică. Puteți decripta o unitate local sau utilizând o politică.

După criptarea hard disk-ului sistemului, utilizatorul trebuie să parcurgă procesul de autentificarea BitLocker pentru a porni sistemul de operare. După procedura de autentificare, BitLocker va permite utilizatorilor să se conecteze. BitLocker nu acceptă tehnologia de conectare unică (SSO).

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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Data Encryption** → **Full Disk Encryption**.
6. În lista verticală **Tehnologie de criptare**, selectați **BitLocker Drive Encryption**.
7. În lista verticală **Mod criptare**, selectați **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.

8. Configurați opțiunile avansate pentru componenta BitLocker Drive Encryption (consultați tabelul de mai jos).
9. Salvați-vă modificările.

Cum se rulează componenta BitLocker Drive Encryption din Web Console și Cloud Console

1. În fereastra principală a Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security pentru computerele pentru care dorești să pornești componenta BitLocker Drive Encryption.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Accesați **Data Encryption** →**Full Disk Encryption**.
5. În secțiunea **Gestionare criptare**, selectați **BitLocker Drive Encryption**.
6. Faceți clic pe linkul **BitLocker Drive Encryption**.

   Această acțiune deschide fereastra cu setările BitLocker Drive Encryption.
7. În lista verticală **Mod criptare**, selectați **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.
8. Configurați opțiunile avansate pentru componenta BitLocker Drive Encryption (consultați tabelul de mai jos).
9. Faceți clic pe **OK**.

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.

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).

Parametru	Descriere
Permite utilizarea autentificării BitLocker ce solicită intrarea de la tastatură înaintea preîncărcării sistemului pe tablete	Această casetă de selectare activează/dezactivează utilizarea autentificării 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. Se recomandă să folosești această setare 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 sporești 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 **Criptare 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. Această casetă de selectare nu este bifată în mod implicit.
Setări autentificare	**Utilizează 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).

Utilizare 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.
  Puteți permite utilizatorului să utilizeze codul PIN îmbunătățit. *Codul PIN îmbunătățit* permite utilizarea altor caractere în plus față de caracterele numerice: majuscule și litere mici din alfabetul latin, caractere speciale și spații.

- **Utilizare Trusted Platform Module (TPM); dacă este indisponibil, se utilizează parola**. Dacă această casetă de selectare este bifată, 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.

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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Data Encryption** → **Full Disk Encryption**.
6. În lista verticală **Tehnologie de criptare**, selectați **BitLocker Drive Encryption**.
7. În lista verticală **Mod criptare**, selectați **Decriptează toate unitățile de hard disk**.
8. 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 Consolei Web, selectați fila **Dispozitive** → **Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security pentru computerele pe care doriți să decriptați unitățile de hard disk.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Accesați **Data Encryption** →**Full Disk Encryption**.
5. Selectați tehnologia **BitLocker Drive Encryption** și urmați linkul pentru a configura setările.

   Setările de criptare se deschid.
6. În lista verticală **Mod criptare**, selectați **Decriptează toate unitățile de hard disk**.
7. Faceți clic pe **OK**.

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.

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.

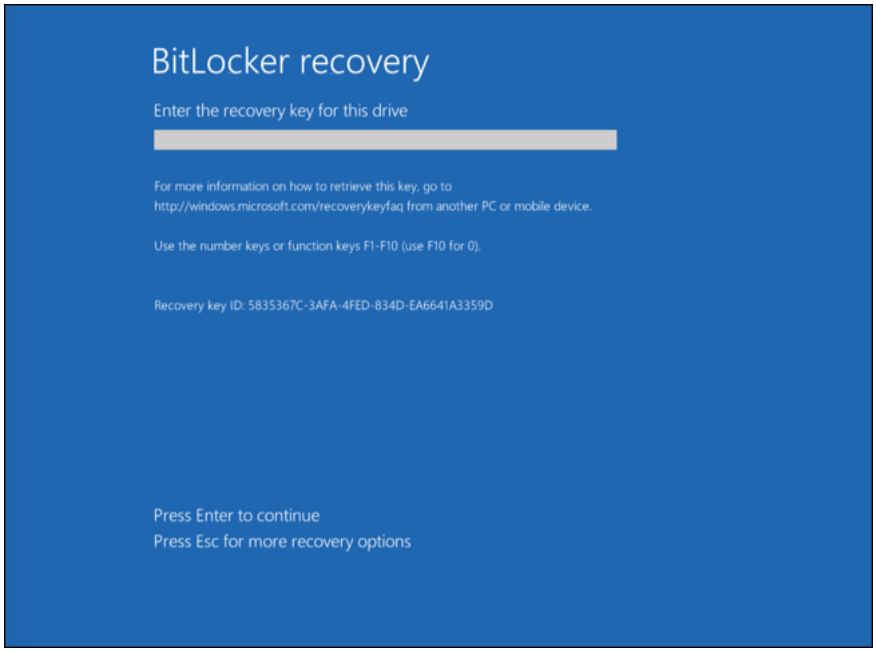
Restaurarea accesului la o unitate de hard disk criptată cu BitLocker constă în următorii pași:

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.
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 directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Dispozitive**.
4. În fila **Dispozitive**, selectați computerul utilizatorului care solicită accesul la datele criptate și faceți clic dreapta pe el pentru a deschide meniul contextual.
5. În meniul contextual, selectați opțiunea **Acordă acces în modul offline**.
6. În fereastra care se deschide, selectați fila **Acces la o unitate de sistem protejată de BitLocker** .
7. 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.

[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 Consolei Web. selectați **Dispozitive** → **Dispozitive gestionate**.
2. Bifați caseta de selectare de lângă numele computerului la a cărui unitate doriți să restaurați accesul.
3. Faceți clic pe butonul **Partajați acest dispozitiv offline**.
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. Faceți clic pe butonul **Primire cheie**.

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 ați setat o parolă sau un cod PIN nou, BitLocker va crea o nouă cheie principală 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 **V-ați 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 Consolei de administrare, selectați directorul **Suplimentar** → **Criptare date și protecție** → **Dispozitive criptate**.
3. În spațiul de lucru, selectați dispozitivul criptat pentru care doriți să creați un fișier cheie de acces și, în meniul contextual al dispozitivului, selectați **Obținere acces la dispozitiv în Kaspersky Endpoint Security for Windows (11.6.0)**.
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**.

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 **Operații → Criptare date și protecție → Dispozitive criptate**.
2. Bifați caseta de selectare de lângă numele computerului la a cărui unitate doriți să restaurați accesul.
3. Faceți clic pe butonul **Partajați acest dispozitiv offline**.

   Astfel, Expertul este pornit pentru permiterea accesului la un dispozitiv.
4. Urmați instrucțiunile din Expert pentru permiterea accesului la un dispozitiv:
   a. Selectați plug-inul **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. Faceți clic pe butonul **Primire cheie**.

Drept urmare, veți avea acces la cheia de recuperare sau la fișierul cheii de recuperare, care va trebui transferat de utilizator.

File Level Encryption pe unitățile locale ale computerului

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 fișiere ale căror conținuturi sunt localizate în spațiul de stocare în cloud OneDrive și blochează copierea fișierelor în spațiul de stocare în cloud OneDrive dacă aceste fișiere nu sunt adăugate la regula de decriptare.

Pentru a cripta fișiere de pe unitățile locale:

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Data Encryption** → **File level encryption**.
6. În partea dreaptă a ferestrei, selectați fila **Criptare**.
7. În lista verticală **Mod de criptare**, selectați elementul **Conform regulilor**.
8. În fila **Criptare**, faceți clic stânga pe butonul **Adăugare** 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.
   - **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 particularizat** 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. Puteți utiliza setul `\..\` (de exemplu, `C:\Users\..\UserFolder\`). Setul `\..\` denumește trecerea la directorul părinte.
- 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.

9. 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

Pentru a crea reguli de acces la fișiere criptate pentru aplicații:

1. Deschide Consolă de administrare a Kaspersky Security Center.

2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.

3. În spațiul de lucru, selectați fila **Politici**.

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

5. În fereastra politicii, selectați **Data Encryption → File level encryption**.

6. În lista verticală **Mod de criptare**, selectați elementul **Conform regulilor**.

   Regulile de acces sunt aplicate doar în modul **Conform regulilor**. După aplicarea regulilor de acces în modul **Conform regulilor**, dacă treceți la modul **Lasă nemodificat**, Kaspersky Endpoint Security va ignora toate regulile de acces. Toate aplicațiilor vor avea acces la toate fișierele criptate.

7. În partea dreaptă a ferestrei, selectați fila **Reguli pentru aplicații**.

8. Dacă dorești să selectezi aplicații exclusiv din lista Kaspersky Security Center, apasă pe butonul **Adăugare** 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. Faceți clic pe butonul **Împrospătare**.

   c. Tabelul listează aplicații care corespund filtrelor aplicate.

   d. În coloana **Aplicații**, 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 aplicații selectate anterior**, selectați acțiunea care trebuie efectuată de Kaspersky Endpoint Security pentru regulile de acces la fișiere criptate create anterior pentru aceste aplicații.

   g. Faceți clic pe **OK**.

   Detaliile unei reguli de acces la fișiere criptate pentru aplicații apar în tabelul din fila **Reguli pentru aplicații**.

9. Dacă dorești să selectezi manual aplicații, faceți clic pe butonul **Adăugare** și, în lista verticală, selectați elementul **Aplicații particularizate**.

   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 **Adăugare 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.

   d. Faceți clic pe **OK**.

Detaliile unei reguli de acces la fișiere criptate pentru aplicații apar în tabelul din fila **Reguli pentru aplicații**.

10. 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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Data Encryption → File level encryption**.
6. În lista verticală **Mod de criptare**, selectați elementul **Conform regulilor**.

   Regulile de criptare sunt aplicate doar în modul **Conform regulilor**. După aplicarea regulilor de criptare în modul **Conform regulilor**, dacă treceți la modul **Lasă nemodificat**, Kaspersky Endpoint Security va ignora toate regulile de criptare. Fișierele criptate anterior vor rămâne criptate.

7. În partea dreaptă a ferestrei, selectați fila **Reguli pentru aplicații**.
8. Dacă dorești să selectezi aplicații exclusiv din lista Kaspersky Security Center, apasă pe butonul **Adăugare** și, în lista verticală, selectați elementul **Aplicații din lista Kaspersky Security Center**.

   Se deschide fereastra **Adăugare aplicații din lista Kaspersky Security Center**.

   Efectuează următoarele acțiuni:

   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. Faceți clic pe butonul **Împrospătare**.

      Tabelul listează aplicații care corespund filtrelor aplicate.

   c. În coloana **Aplicații**, bifați casetele de selectare de lângă aplicațiile ale căror fișiere create doriți să le criptați.

   d. În lista verticală **Regulă pentru aplicații**, selectați **Criptare globală fișiere create**.

   e. În lista verticală **Acțiuni pentru aplicații 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.

f. Faceți clic pe **OK**.

Informațiile despre regulile de criptare pentru fișierele create sau modificate de către aplicațiile selectate apar în tabelul din fila **Reguli pentru aplicații**.

9. Dacă dorești să selectezi manual aplicații, faceți clic pe butonul **Adăugare** și, în lista verticală, selectați elementul **Aplicații particularizate**.

   Se deschide fereastra **Adăugare/editare nume de fișiere executabile ale aplicațiilor**.

   Efectuează următoarele acțiuni:

   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 **Adăugare 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 **Criptare globală fișiere create**.

   d. Faceți clic pe **OK**.

   Informațiile despre regulile de criptare pentru fișierele create sau modificate de către aplicațiile selectate apar în tabelul din fila **Reguli pentru aplicații**.

10. Salvați-vă modificările.

Generarea unei reguli de decriptare

Pentru a genera o regulă de decriptare:

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Data Encryption → File level encryption**.
6. În partea dreaptă a ferestrei, selectați fila **Decriptare**.
7. În lista verticală **Mod de criptare**, selectați elementul **Conform regulilor**.
8. În fila **Decriptare**, faceți clic pe butonul **Adăugare** 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 particularizat** 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.

9. 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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Data Encryption → File level encryption**.
6. În partea dreaptă a ferestrei, selectați fila **Criptare**.
7. 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 **Eliminare**.

   Poți șterge mai multe elemente simultan din lista de criptare. Pentru aceasta, în timp ce ții apăsată tasta **CTRL**, selectați fișierele de care ai nevoie făcând clic stânga pe ele și selectând elementul **Ștergere regulă și decriptare fișiere** în meniul contextual al butonului **Eliminare**.

   Fișierele și directoarele eliminate din lista de criptare sunt adăugate în mod automat în lista de decriptare.
8. Formează o listă de decriptare.
9. 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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Data Encryption** → **Setări de criptare comune**.
6. În blocul **Setări parolă**, faceți clic pe butonul **Setări**.
7. În fereastra care se deschide, selectați fila **Pachete criptate**.
8. 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 Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security pentru computerele pe care doriți să activați verificarea complexității parolei.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Accesați **Data Encryption** → **File Level Encryption**.
5. În blocul **Setări parolă pachet criptat**, 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.

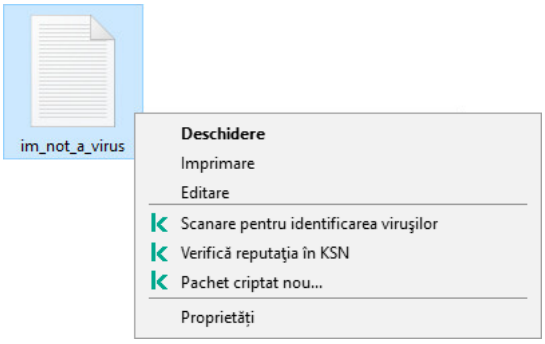
La adăugarea unui fișier la pachetul criptat al cărui conținut se află în spațiul de stocare în cloud OneDrive, Kaspersky Endpoint Security descarcă conținutul fișierului și execută criptarea.

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).
3. În fereastra care se deschide, selectați o locație pe o unitate amovibilă pentru a salva pachetul criptat → specificați numele pachetului și faceți clic pe butonul **Salvare**.
4. În fereastra care se deschide, specificați parola și confirmați-o.

   Parola trebuie să îndeplinească criteriile de complexitate specificate în politică.
5. Fă clic pe butonul **Creare**.

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.



Crearea unui pachet criptat

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.

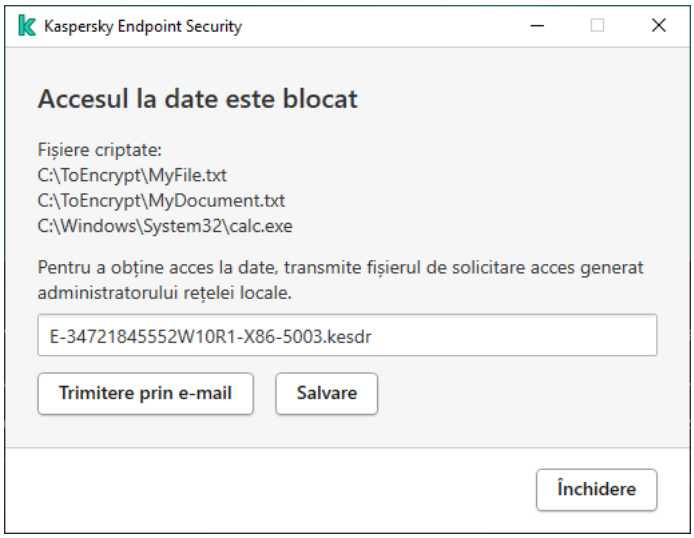
  Utilizatorul poate lucra cu fișiere criptate în următoarele situații:

  - 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 directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Dispozitive**.
4. În fila **Dispozitive**, selectați computerul utilizatorului care solicită accesul la datele criptate și faceți clic dreapta pe el pentru a deschide meniul contextual.
5. În meniul contextual, selectați opțiunea **Acordă acces în modul offline**.
6. În fereastra care se deschide, selectați fila **Data Encryption**.
7. În fila **Data Encryption**, faceți clic pe butonul **Răsfoire**.
8. 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.

Cum se obține un fișier cheie de acces la datele criptate în Web Console

1. În fereastra principală a Consolei Web. selectați **Dispozitive** → **Dispozitive gestionate**.
2. Bifați caseta de selectare de lângă numele computerului la ale cărui date doriți să restaurați accesul.
3. Faceți clic pe butonul **Partajați acest dispozitiv offline**.
4. Selectați secțiunea **Data Encryption**.
5. Faceți clic pe butonul **Selectare fișier** 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 **Salvare cheie** 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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Data Encryption → Setări de criptare comune**.
6. În secțiunea **Șabloane**, faceți clic pe butonul **Șabloane**.

   Se deschide fereastra **Șabloane**.
7. Efectuează următoarele acțiuni:

   - Dacă dorești să editezi șablonul pentru mesajul utilizatorului, selectați fila **Mesajul utilizatorului**. Fereastra **Accesul la date este blocat** se deschide atunci când utilizatorul încearcă să acceseze un fișier criptat când nu există pe computer nicio cheie disponibilă pentru accesul la fișierele criptate. Faceți clic pe butonul **Trimitere prin e-mail** în fereastra **Accesul la date este blocat** pentru a crea un mesaj. 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**. Acest mesaj este creat automat atunci când faci clic pe butonul **Trimitere prin e-mail** în fereastra **Solicitare acces la fișiere criptate** și este trimis utilizatorului după ce acestuia i se acordă acces la fișiere criptate.
8. Editează șabloanele de mesaje.

   Poți folosi butonul **În mod implicit** și lista verticală **Variabilă**.
9. Salvați-vă modificările.

Criptare unități amovibile

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 în sisteme de fișiere FAT32 și NTFS. Dacă o unitate amovibilă cu un sistem de fișiere neacceptat este conectată la computer, criptarea unității amovibile se termină cu o eroare și Kaspersky Endpoint Security atribuie unității amovibile acces numai în citire.

Pentru a cripta unități amovibile:

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.

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

5. În fereastra politicii, selectați **Data Encryption → Criptare unități amovibile**.

6. În lista verticală **Mod de criptare**, selectați acțiunea implicită pe care doriți ca Kaspersky Endpoint Security să o efectueze pe unitățile amovibile:

   - **Criptare 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.

   - **Criptare 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.

   - **Criptare 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.

7. Dacă doriți să utilizați modul portabil pentru criptarea unităților amovibile, selectați caseta de selectare **Mod portabil**.

   Modul portabil 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.

8. 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.

9. Dacă doriți să configurați criptarea pentru unități amovibile individuale, definiți regulile de criptare.

10. Dacă doriți să utilizați criptarea Full Disk Encryption a unităților amovibile în modul offline, bifați caseta de selectare **Permite criptarea unităților amovibile în modul offline**.

    Mod criptare offline 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 **Permite criptarea unităților amovibile în modul offline** este debifată și nu există nicio conexiune la Kaspersky Security Center, nu este posibilă criptarea unității amovibile.

11. Salvați-vă modificările.

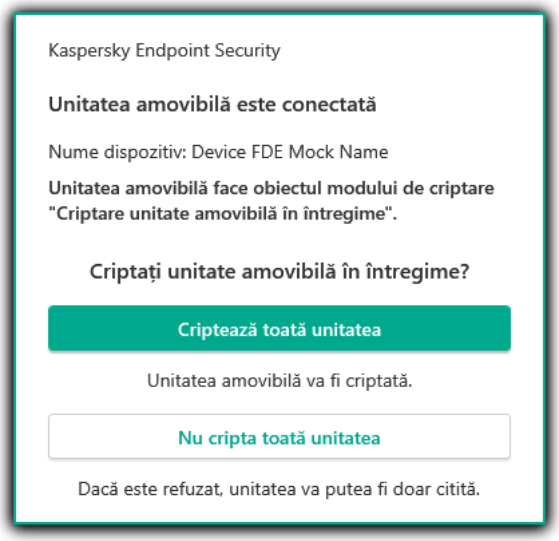
După aplicarea politicii, atunci când utilizatorul conectează o unitate amovibilă sau dacă o unitate amovibilă este deja conectată, Kaspersky Endpoint Security solicită utilizatorului confirmarea efectuării operației de criptare (consultați figura de mai jos).

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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Data Encryption** → **Criptare unități amovibile**.
6. Faceți clic pe butonul **Adăugare** 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 unități amovibile care sunt în lista Kaspersky Security Center, selectați **Din lista de dispozitive a Kaspersky Security Center**.

7. 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.

8. 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.

9. 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 **Criptare unitate amovibilă în întregime**, sectoarele care nu sunt ocupate de fișiere în continuare nu vor fi criptate.

10. 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 **Omitere**.

    - Dacă doriți ca regula de criptare creată anterior să fie înlocuită de noua regulă, selectați **Actualizare**.

11. 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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Data Encryption → Criptare unități amovibile**.
6. 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 **Exportare**.
   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. Faceți clic pe butonul **Save**.
      Kaspersky Endpoint Security exportă lista de reguli în fișierul XML.
7. Pentru a importa o listă de reguli de criptare a unităților amovibile:
   a. Faceți clic pe linkul **Importare**.
      În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de reguli.
   b. Faceți clic pe butonul **Deschidere**.
      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 criptare a unităților amovibile în Consola Web

1. În fereastra principală a Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security pentru computerele pe care doriți să exportați sau să importați o listă de reguli de criptare a unităților amovibile.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Accesați **Data Encryption** → **Criptare unități amovibile**.
5. În blocul **Reguli de criptare pentru dispozitivele selectate**, faceți clic pe linkul **Reguli criptare**.

   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. Faceți clic pe butonul **Export**.
   c. Confirmați că doriți să exportați numai regulile selectate sau să exportați întreaga listă.
   d. Faceți clic pe butonul **Export**.

      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 **Importare**.

      În fereastra care se deschide, selectați fișierul XML din care doriți să importați lista de reguli.
   b. Faceți clic pe butonul **Deschidere**.

      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.

Modul portabil pentru accesarea fișierelor criptate de pe unități amovibile

Modul portabil 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:

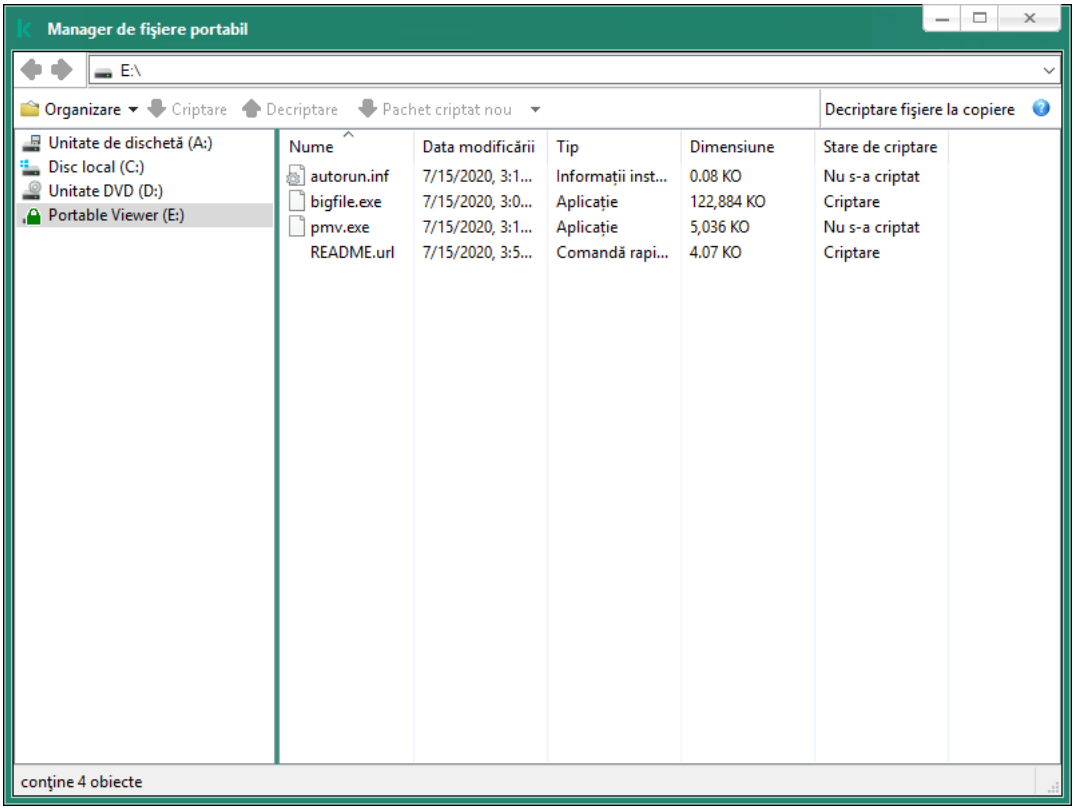
- Nu există nicio conexiune între computer și Serverul de administrare Kaspersky Security Center.
- Infrastructura s-a schimbat odată cu schimbarea Serverului de administrare Kaspersky Security Center.
- Kaspersky Endpoint Security nu este instalat pe computer.

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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Data Encryption** → **Criptare unități amovibile**.
6. În lista verticală **Mod de criptare pentru dispozitivele selectate**, selectați **Criptare toate fișierele** sau**Criptare 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).

7. Bifați caseta de selectare **Mod portabil**.
8. Dacă este necesar, adăugați reguli de criptare pentru unitățile amovibile individuale .
9. Salvați-vă modificările.
10. După aplicarea politicii, conectați unitatea amovibilă la computer.
11. Confirmă funcționarea criptării unității amovibile.

    Se deschide o fereastră în care puteți crea o parolă pentru Manager de fișiere portabil.
12. Specifică o parolă care îndeplinește cerințele de complexitate și confirm-o.
13. Faceți clic pe **OK**.

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.

Cum să activați asistența pentru modul portabil pentru lucrul cu fișierele criptate pe unitățile amovibile în Web Console

1. În fereastra principală a Consolei Web, selectați **Dispozitive** → **Politici și profiluri**.
2. Faceți clic pe numele politicii Kaspersky Endpoint Security pentru computerele pe care doriți să activați asistența pentru modul portabil.

   Se deschide fereastra de proprietăți a politicii.
3. Selectați fila **Setări aplicație**.
4. Accesați **Data Encryption** → **Criptare unități amovibile**.
5. În secțiunea **Gestionare criptare**, selectați **Criptare toate fișierele** sau **Criptare 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).
6. Bifați caseta de selectare **Mod portabil**.
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.
11. Specifică o parolă care îndeplinește cerințele de complexitate și confirm-o.
12. Faceți clic pe **OK**.

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.

- 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.

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 modulului 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.
  - Este selectat modul **Criptare toate fișierele** sau **Criptare numai fișiere noi**.

  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.

- **Solicitați 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 directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Dispozitive**.
4. În fila **Dispozitive**, selectați computerul utilizatorului care solicită accesul la datele criptate și faceți clic dreapta pe el pentru a deschide meniul contextual.
5. În meniul contextual, selectați opțiunea **Acordă acces în modul offline**.
6. În fereastra care se deschide, selectați fila **Data Encryption**.
7. În fila **Data Encryption**, faceți clic pe butonul **Răsfoire**.
8. 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.

Cum se obține un fișier criptat de acces la date în Web Console

1. În fereastra principală a Consolei Web. selectați **Dispozitive** → **Dispozitive gestionate**.
2. Bifați caseta de selectare de lângă numele computerului la ale cărui date doriți să restaurați accesul.
3. Faceți clic pe butonul **Partajați acest dispozitiv offline**.
4. Selectați secțiunea **Data Encryption**.
5. Faceți clic pe butonul **Selectare fișier** 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 **Salvare cheie** 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. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Politici**.
4. Selectați politica necesară și faceți dublu clic pentru a deschide proprietățile politicii.
5. În fereastra politicii, selectați **Data Encryption → Criptare unități amovibile**.
6. Dacă dorești să decriptezi toate fișierele criptate stocate pe unități amovibile, în lista verticală **Mod criptare** selectați **Decriptare unitate amovibilă în întregime**.
7. 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. Faceți clic pe butonul **Setare regulă** pentru a edita regula de criptare pentru unitatea amovibilă selectată.
   Se deschide meniul contextual al butonului **Setare regulă**.
   c. Selectați elementul **Decriptare toate fișierele** în meniul contextual al butonului **Setare regulă**.
8. 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. Criptarea 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.

Sunt posibile două valori pentru starea de criptare:

- *Politică de criptare nedefinită*. Nu a fost definită o politică de criptare a aplicației Kaspersky Security Center pentru acest computer.
- *Se aplică politica*. Criptarea și/sau decriptarea datelor este în curs pe acest computer.

- *Eroare*. A intervenit o eroare în cursul criptării și/sau decriptării datelor pe acest computer.
- *Repornire necesară*. Sistemul de operare trebuie repornit pentru a începe sau a finaliza criptarea sau decriptarea datelor pe acest computer.
- *Conform politicii*. Criptarea datelor pe acest computer a fost finalizată folosind setările de criptare specificate în politica pentru Kaspersky Security Center aplicată computerului.
- *Anulat de utilizator*. Utilizatorul a refuzat să confirme operațiunea de criptare a fișierelor pe unitatea amovibilă.

Vizualizarea stării de criptare

Pentru a vedea starea de criptare a datelor computerului:

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare căruia îi aparțin computerele client relevante.
3. În spațiul de lucru, selectați fila **Dispozitive**.

   Fila **Dispozitive** din spațiul de lucru prezintă proprietățile computerelor din grupul de administrare selectat.
4. În fila **Dispozitive** din spațiul de lucru, defilează până la maximum dreapta baza de defilare.
5. Dacă nu se afișează coloana **Stare de criptare**:

   a. Faceți clic dreapta pentru a deschide meniul contextual al antetului tabelului.

   b. În meniul contextual, în lista verticală **Vizualizare**, selectați **Adăugare/Eliminare coloane**.

   Apare fereastra **Adăugare/Eliminare coloane**.

   c. În fereastra **Adăugare/Eliminare coloane**, bifați caseta de selectare **Stare de criptare**.

   d. Faceți clic pe **OK**.

Coloana **Stare de criptare** 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.

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 **Server de administrare – <Nume computer>**.
3. În spațiul de lucru din dreapta arborelui consolei de administrare, selectați fila **Statistici**.
4. Creează o pagină nouă cu panouri de detalii care conțin statistici de criptare a datelor. Pentru aceasta:

a. În fila **Statistici**, faceți clic pe butonul **Particularizare vizualizare**.

Se deschide fereastra **Proprietăți: Statistici**.

b. În fereastra **Proprietăți: Statistici**, faceți clic pe **Adăugare**.

Se deschide fereastra **Proprietăți: Pagină nouă**.

c. În secțiunea **General** din fereastra **Proprietăți: Pagină nouă**, tastează numele paginii.

d. În secțiunea **Panouri de detalii**, faceți clic pe butonul **Adăugare**.

Se deschide fereastra **Panou de detalii nou**.

e. În fereastra **Panou de detalii nou** din grupul **Stare protecție**, selectați elementul **Criptare dispozitive**.

f. Faceți clic pe **OK**.

Se deschide fereastra **Proprietăți: Control criptare**.

g. Dacă este necesar, editează setările panoului de detalii. Pentru aceasta, folosește secțiunile **Vizualizare** și **Dispozitive** din fereastra **Proprietăți: Criptare dispozitive.**

h. Faceți clic pe **OK**.

i. Repetă pașii d – h din instrucțiuni, selectând elementul **Criptare unități amovibile** din secțiunea **Stare protecție** din fereastra **Panou de detalii nou**.

Panourile de detalii adăugate apar în lista **Panouri de detalii** din fereastra **Proprietăți: Pagină nouă**.

j. În fereastra **Proprietăți: Pagină nouă**, faceți clic pe **OK**.

Numele paginii cu panourile de detalii create în pașii anteriori apare în lista **Pagini** din fereastra **Proprietăți: Statistici**.

k. În fereastra **Proprietăți: Statistici**, faceți clic pe **Închidere**.

5. În fila **Statistici**, 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 directorul **Dispozitive gestionate** al arborelui consolei de administrare, deschide directorul cu numele grupului de administrare care include computerul client pentru care dorești să vezi lista de erori de criptare fișiere.

3. În spațiul de lucru, selectați fila **Dispozitive**.

4. În fila **Dispozitive**, selectați numele computerului în listă și faceți clic dreapta pe el pentru a deschide meniul contextual.

5. în meniul contextual al computerului, selectați elementul **Proprietăți**. În fereastra **Proprietăți: <nume computer>**, selectați secțiunea **Protecție**.

6. În secțiunea **Protecție** a ferestrei **Proprietăți: <nume computer>**, faceți clic pe linkul **Vizualizare listă erori criptare date** pentru a deschide fereastra **Erori criptare date**.

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 **Erori criptare date**.

Vizualizarea raportului de criptare a datelor

Pentru a vizualiza raportul de criptare a datelor:

1. Deschide Consolă de administrare a Kaspersky Security Center.
2. În nodul **Server de administrare** din arborele consolei de administrare, selectați fila **Rapoarte**.
3. Faceți clic pe butonul **Șablon raport nou**.

   Se lansează Expertul pentru șablon de raport.
4. Urmează instrucțiunile din Expertul pentru șablon de raport. În fereastra **Selectați tipul șablonului de raport**, în secțiunea **Altele**, selectați unul dintre elementele următoare:
   - **Raportul privind starea criptării dispozitivelor gestionate**.
   - **Raportul privind starea criptării dispozitivelor de stocare în masă**.
   - **Raportul privind erorile de criptare a fișierelor**.
   - **Raportul Acces blocat la fișiere criptate**.

   După ce ai finalizat Expertul pentru șablon de raport nou, un nou șablon de raport apare în tabelul din fila **Rapoarte**.
5. Selectați șablonul de raport creat în pasul anterior al instrucțiunilor.
6. În meniul contextual al șablonului, selectați **Afișare raport**.

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.

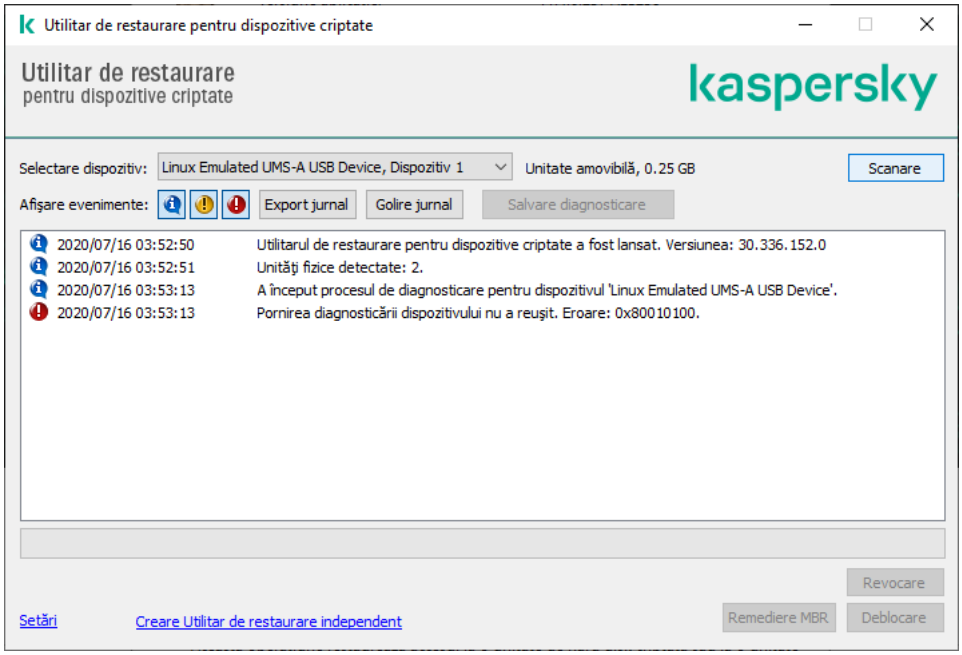
Înainte de a restaura datele pe dispozitive criptate, se recomandă să revoci politica aplicației Kaspersky Security Center sau să dezactivezi criptarea în setările politicii aplicației Kaspersky Security Center pe computerul pe care va fi efectuată operațiunea. Aceasta împiedică dispozitivul să fie criptat 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, fă clic pe butonul **Asistență**.
2. În fereastra care se deschide, faceți clic pe butonul **Restaurarea dispozitiv criptat**.

   Se lansează Utilitarul de restaurare pentru dispozitive criptate.
3. Faceți clic pe butonul **Creare Stand-alone Restore Utility** 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 Utilitar Restaurare, în lista verticală **Selectare dispozitiv**, selectați un dispozitiv criptat la care dorești să restaurezi accesul.

3. Faceți clic pe butonul **Scanare** 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 **Salvare diagnosticare**.

   Utilitarul va salva o arhivă cu fișierele care conțin informațiile diagnosticării.

5. Faceți clic pe butonul **Remediere 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 **Deblocare** sau **Decriptare** în funcție de rezultatele diagnosticării.

7. Dacă doriți să restaurați datele utilizând un cont Agent de Autentificare, selectați opțiunea **Utilizare 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 **Specificare manuală cheie de acces pentru dispozitiv**.

   b. Faceți clic pe butonul **Primire 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 **Primire 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 **Primire 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 **Răsfoire** pentru a furniza calea către locația de salvare a fișierul VHD.

10. Faceți 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 Consolei de administrare, selectați directorul **Suplimentar** → **Criptare date și protecție** → **Dispozitive criptate**.
3. În spațiul de lucru, selectați dispozitivul criptat pentru care doriți să creați un fișier cheie de acces și, în meniul contextual al dispozitivului, selectați **Obținere acces la dispozitiv în Kaspersky Endpoint Security for Windows (11.6.0)**.

   Dacă nu sunteți sigur pentru ce computer a fost generat fișierul de solicitare a accesului, în arborele Consolei de administrare selectați directorul **Suplimentar** → **Criptare date și protecție** și, în spațiul de lucru, faceți clic pe linkul **Obținere cheie de criptare în Kaspersky Endpoint Security for Windows (11.6.0)**.

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. Faceți clic pe butonul **Răsfoire**. În fereastra care se deschide, specificați calea către fișierul de solicitare a accesului (care are extensia FDErTC), primit de la utilizator.
6. Faceți clic pe butonul **Deschidere**.

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 **Operații** → **Criptare date și protecție** → **Dispozitive criptate**.

2. Bifați caseta de selectare de lângă numele computerului pe care doriți să recuperați datele.

3. Faceți clic pe butonul **Partajați acest dispozitiv offline**.

   Astfel, Expertul este pornit pentru permiterea accesului la un dispozitiv.

4. Urmați instrucțiunile din Expert pentru permiterea accesului la un dispozitiv:

   a. Selectați plug-inul **Kaspersky Endpoint Security for Windows**.

   b. Selectați algoritmul de criptare pe care doriți să îl utilizați: **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. Faceți clic pe butonul **Selectare fișier** și selectați fișierul de solicitare a accesului pe care l-ați primit de la utilizator (un fișier cu extensia FDERTC).

   d. Faceți clic pe butonul **Salvare cheie** și selectați un director pentru a salva fișierul cheie pentru accesarea datelor 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).

Gestionarea aplicației din linia de comandă

Puteți gestiona Kaspersky Endpoint Security din linia de comandă. Puteți vizualiza lista de comenzi pentru gestionarea aplicației executând comanda `HELP`. Pentru a citi despre sintaxa unei anumite comenzi, introduceți `<comanda> HELP`.

Caracterele speciale din cadrul comenzii trebuie omise. Pentru a omite caracterele &, |, (,), <, >, ^, utilizați caracterul ^ (de exemplu, pentru a folosi caracterul `&`, introduceți `^&`). Pentru a omite caracterul `%`, introduceți `%%`.

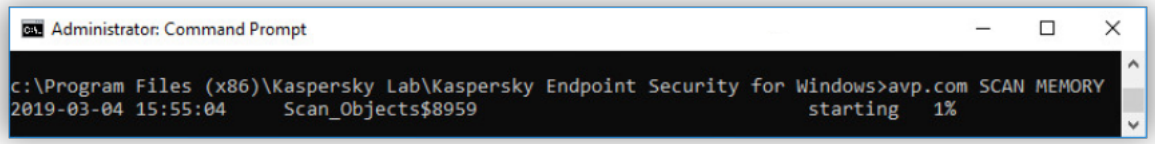
Comenzi AVP

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.
3. Pentru a executa o comandă, introduceți:

```
avp.com <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 de viruși

Executați activitatea de scanare de viruși.

Sintaxa de comandă

```
SCAN [<domeniu de scanare>] [<acțiune la detectarea amenințării>] [<tipuri de fișiere>] [<excluderi de la scanare>] [/R[A]:<fișier de raportare>] [<tehnologii de scanare>] [/C:<fișier cu setările scanării de viruși>]
```

Domeniu de scanare	

`<fișiere de scanat>`	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 completă*. Kaspersky Endpoint Security scanează următoarele obiecte: • Memorie 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
`/MEMORY`	Scanați memoria kernel
`/STARTUP`	Scanați obiectele încărcate la pornirea sistemului de operare
`/MAIL`	Scanați cutia poștală Outlook
`/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.
`/@:<fișier 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`	Informare. Dacă este selectată această opțiune, Kaspersky Endpoint Security adaugă informațiile despre fișierele infectate în lista de amenințări active la detectarea acestor fișiere.
`/i1`	Dezinfectare; blochează dacă dezinfectarea nu reușește. Dacă selectați această opțiune, Kaspersky Endpoint Security încearcă automat să dezinfecteze toate fișierele infectate care sunt detectate. Dacă nu este posibilă dezinfectarea, Kaspersky Endpoint Security adaugă informațiile despre fișierele infectate detectate în lista de amenințări active.
`/i2`	Dezinfectare; șterge dacă dezinfectarea nu reușește. Dacă selectați această opțiune, Kaspersky Endpoint Security încearcă automat să dezinfecteze toate fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, Kaspersky Endpoint Security șterge fișierele. Această acțiune este selectată în mod implicit.

`/i3`	Dezinfectați fișierele infectate detectate. Dacă dezinfectarea eșuează, ștergeți fișierele infectate. Ștergeți și fișierele compuse (de exemplu, arhivele) dacă fișierul infectat nu poate fi dezinfectat sau șters.
`/i4`	Ștergeți fișierele infectate. Ștergeți și fișierele compuse (de exemplu, arhivele) dacă fișierul infectat nu poate fi șters.
`/i8`	Solicită utilizatorului să acționeze imediat ce este detectată o amenințare.
`/i9`	Solicită utilizatorului să acționeze după finalizarea scanării.

Tipuri de fișiere	
`/fe`	Fișiere scanate după extensie. Dacă se activează această setare, Kaspersky Endpoint Security scanează numai fișierele infectabile. Formatul fișierului se determină în funcție de extensia sa.
`/fi`	Fișiere scanate după format. Dacă se activează această setare, Kaspersky Endpoint Security 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, Kaspersky Endpoint Security 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:b`	Bazele de date de e-mail, mesajele de e-mail primite și trimise sunt excluse din domeniul de scanare.
`-E:<mască de fișier>`	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 `exemplu*` va include toate căile către fișierele denumite EXEMPLU.
`-e:<secunde>`	Fișierele a căror scanare durează mai mult decât limita de timp specificată (în secunde) sunt excluse din domeniul de scanare.
`-es:<megabiți>`	Fișierele care sunt mai mari decât dimensiunea maximă specificată (în megabyți) sunt excluse din domeniul de scanare.

Salvarea evenimentelor într-un mod fișier raport	
`/R:<fișier de raportare>`	Salvați numai evenimente critice în fișierul raport.
`/RA:<fișier de raportare>`	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 scanare 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:<fișier cu setările scanării de viruși>`	Fișier cu setările activității Scanare de viruși. Fișierul trebuie creat manual și salvat în format TXT. Fișierul poate avea următorul conținut: `[<domeniu de scanare>] [<acțiune la detectarea amenințării>] [<tipuri de fișiere>] [<excluderi de la scanare>] [/R [A]:<fișier raport>] [<tehnologii de scanare>]`.

Exemplu:

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

UPDATE. Actualizarea bazelor de date și modulelor aplicației

Executați activitatea *Actualizare*

Sintaxa de comandă

```
UPDATE [local]["<sursă actualizare>"] [/R[A]:<fișier raport>] [/C:<fișier cu setările de actualizare >]
```

Setări activitate de actualizare	
`local`	Începerea activității de *actualizare* care a fost creată automat după ce aplicația a fost instalată. Puteți modifica setările activității de *actualizare* în interfața aplicației locale sau în consola Kaspersky Security Center. Dacă această setare nu este configurată, Kaspersky Endpoint Security pornește activitatea de *actualizare* cu setările implicite sau cu setările specificate în comandă. Puteți configura setările activității de actualizare după cum urmează: • `UPDATE` pornește activitatea *Actualizare* cu setările implicite: sursa de actualizare o reprezintă serverele de actualizare, contul este Sistem și alte setări implicite. • `UPDATE local` pornește activitatea *Actualizare* care a fost creată automat după instalare (activitate predefinită).

	• `UPDATE <setări actualizare>` pornește activitatea *Actualizare* setările stabilite manual (a se vedea mai jos).

Sursă actualizare	
`"<sursă actualizare>”`	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 fișier raport	
`/R:<fișier de raportare>`	Salvați numai evenimente critice în fișierul raport.
`/RA:<fișier de raportare>`	Salvați toate evenimentele într-un fișier raport.

Setări avansate	
`/C:<fișier cu setări de actualizare>`	Fișier cu setările activității *Actualizare*. Fișierul trebuie creat manual și salvat în format TXT. Fișierul poate avea următorul conținut: `["<sursă actualizare>"] [/R[A]: <fișier raport>]`.

Exemplu:
```
avp.com UPDATE local

avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

ROLLBACK. Derularea înapoi a celei mai recente actualizări

Derulați înapoi ultima actualizare 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.

Sintaxa de comandă

```
ROLLBACK [/R[A]:<fișier raport>]
```

Salvarea evenimentelor într-un mod fișier raport	
`/R:<fișier de raportare>`	Salvați numai evenimente critice în fișierul raport.
`/RA:<fișier de raportare>`	Salvați toate evenimentele într-un fișier raport.

Exemplu:
```
avp.com ROLLBACK /RA:rollback.txt
```

TRACES. Urme

Activați/dezactivați 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\Traces. În mod implicit, urmărirea este dezactivată.

Sintaxa de comandă

```
TRACES on|off [<nivel de urmărire>] [<setări avansate>]
```

Nivelul de urmărire	
`<nivel de urmărire>`	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`	Executați o comandă cu parametrii `dbg`, `fișier` și `mem`.
`dbg`	Utilizați funcția OutputDebugString și salvați fișierul de urmărire. Funcția OutputDebugString trimite un șir de caractere la depanatorul de aplicații pentru a fi afișat pe ecran. Pentru detalii, vizitați *Site-ul web MSDN*.
`fișier`	Salvați un fișier de urmărire (fără limită de dimensiune).
`rot`	Salvați urmărirea la un număr limitat de fișiere cu dimensiune limitată și suprascrieți fișierele mai vechi atunci când este atinsă dimensiunea maximă.
`mem`	Salvați urmărirea în fișierele dump.

Exemple:

- `avp.com TRACES on 500`
- `avp.com TRACES on 500 dbg`
- `avp.com TRACES off`
- `avp.com TRACES on 500 dbg mem`

- `avp.com TRACES off file`

START. Porniți profilul

Porniți profilul (de exemplu, pentru a actualiza bazele de date sau pentru a activa o componentă de protecție).

Sintaxa de comandă

```
START <profil> [/R[A]:<fișier de raportare>]
```

Profil	
`<profil>`	Numele profilului. Un *Profil* este o componentă, o activitate sau o caracteristică a aplicației Kaspersky Endpoint Security. Puteți vizualiza lista de profiluri disponibile executând comanda `HELP START`.

Salvarea evenimentelor într-un mod fișier raport	
`/R:<fișier de raportare>`	Salvați numai evenimente critice în fișierul raport.
`/RA:<fișier de raportare>`	Salvați toate evenimentele într-un fișier raport.

Exemplu:
`avp.com START Scan_Objects`

STOP. Oprirea unui profil

Opriți profilul în execuție (de exemplu, opriți scanarea, opriți scanarea unităților amovibile sau dezactivați o componentă de protecție).

Pentru a executa această comandă, funcția Protecție prin parolă trebuie activată. Utilizatorul trebuie să dispună de permisiunile de **Dezactivare componente de protecție** și **Dezactivare componente de control**.

Sintaxa de comandă

```
STOP <profil> /login=<nume utilizator> /password=<parolă>
```

Profil	
`<profil>`	Numele profilului. Un *Profil* este o componentă, o activitate sau o caracteristică a aplicației Kaspersky Endpoint Security. Puteți vizualiza lista de profiluri disponibile executând comanda `HELP STOP`.

Autentificare	
`/login=<nume utilizator>`	Acreditări de cont de utilizator cu permisiunile necesare de

`/password=<parolă>`	protecție prin parolă.

STATUS. Starea profilului

Afișează informații despre stare pentru profilurile de aplicații (de exemplu, `în executare` sau `finalizat`). Puteți vizualiza lista de profiluri disponibile executând 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.

Sintaxa de comandă

```
STATUS [<profil>]
```

STATISTICS. Statistici de funcționare a profilului

Vizualizați informații statistice despre un profil al aplicației (de exemplu, durata scanării sau numărul de amenințări detectate.) Puteți vizualiza lista de profiluri disponibile rulând comanda `HELP STATISTICS`.

Sintaxa de comandă

```
STATISTICS <profil>
```

RESTORE. Restaurarea fișierelor

Puteți restaura un fișier din Copie de rezervă în directorul său original. Dacă la calea specificată există deja un fișier cu același nume, sufixul „-copy" este anexat la numele fișierului. 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 **Restaurare din 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\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.

Sintaxa de comandă

```
RESTORE [/REPLACE] <nume fișier> /login=<nume utilizator> /password=<parolă>
```

Setări avansate	
/REPLACE	Suprascrieți un fișier existent.
<nume fișier>	Numele fișierului care va fi restaurat.

Autentificare	
/login=<nume utilizator> /password=<parolă>	Acreditări de cont de utilizator cu permisiunile necesare de protecție prin parolă.

Exemplu:

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1
```

EXPORT. Exportarea setărilor aplicației

Exportați setările Kaspersky Endpoint Security într-un fișier. Fișierul va fi localizat în directorul C:\Windows\SysWOW64.

Sintaxa de comandă

```
EXPORT <profil> <nume fișier>
```

Profil	
<profil>	Numele profilului. Un *Profil* este o componentă, o activitate sau o caracteristică a aplicației Kaspersky Endpoint Security. Puteți vizualiza lista de profiluri disponibile executând comanda `HELP EXPORT`.

Fișier de exportat	
<nume fișier>	Numele fișierului în care vor fi exportate setările aplicației. Puteți exporta setările Kaspersky Endpoint Security într-un fișier de configurare DAT sau CFG, într-un fișier text TXT sau într-un document XML.

Exemple:

- `avp.com EXPORT ids ids_config.dat`
- `avp.com EXPORT fm fm_config.txt`

IMPORT. Importarea setărilor aplicației

Importă setările 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 **Configurare setări aplicație**.

Sintaxa de comandă

```
IMPORT <nume fișier> /login=<nume utilizator> /password=<parolă>
```

Fișier de importat	
`<nume fișier>`	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=<nume utilizator> /password=<parolă>`	Acreditări de cont de utilizator cu permisiunile necesare de protecție prin parolă.

Exemplu:
```
avp.com IMPORT config.dat /login=KLAdmin /password=!Password1
```

ADDKEY. Aplicarea unui fișier cheie

Aplicați fișierul cheie pentru a activa Kaspersky Endpoint Security. Dacă aplicația este deja activată, cheia va fi adăugată drept cheie de rezervă.

Sintaxa de comandă

```
ADDKEY <nume fișier> /login=<nume utilizator> /password=<parolă>
```

Fișier cheie	
`<nume fișier>`	Numele fișierului cheie.

Autentificare	
`/login=<nume utilizator> /password=<parolă>`	Acreditările contului de utilizator. Aceste acreditări trebuie introduse numai dacă funcția Protecție prin parolă este activată.

Exemplu:
```
avp.com ADDKEY file.key
```

LICENSE. Licențiere

Efectuați acțiuni cu cheile de licență Kaspersky Endpoint Security.

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 **Eliminare cheie**.

Sintaxa de comandă

```
LICENSE <funcționarea> [/login=<nume utilizator> /password=<parolă>]
```

Funcționare	
`/ADD <nume fișier>`	Aplicați fișierul cheie pentru a activa Kaspersky Endpoint Security. Dacă aplicația este deja activată, cheia va fi adăugată drept cheie de rezervă.
`/ADD <cod de activare>`	Activați Kaspersky Endpoint Security folosind un cod de activare. Dacă aplicația este deja activată, cheia va fi adăugată drept cheie de rezervă.
`/REFRESH <nume fișier>`	Reînnoiți-vă licența cu un fișier cheie. O cheie de rezervă este adăugată drept rezultat. Ea devine activă la expirarea licenței. Nu este posibil să adăugați o cheie activă executând această comandă.
`/REFRESH <cod de activare>`	Reînnoiți-vă licența cu un cod de activare. O cheie de rezervă este adăugată drept rezultat. Ea devine activă la expirarea licenței. Nu este posibil să adăugați o cheie activă executând această comandă.
`/DEL /login=<nume utilizator> /password=<parolă>`	Eliminați o cheie de licență. Cheia de rezervă va fi, de asemenea, eliminată.

Autentificare	
`/login=<nume utilizator> /password=<parolă>`	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 /login=KLAdmin /password=!Password1`

RENEW. Achiziționarea unei licențe

Deschideți site-ul web Kaspersky pentru a cumpăra sau reînnoi licența.

PBATESTRESET. Resetați rezultatele verificării discului înainte de criptarea discului

Resetați 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 Full Disk Encryption sau BitLocker de criptare a unităților.

EXIT. Ieșire din aplicație

Părăsește 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 **Ieșire din aplicație**.

Sintaxa de comandă

```
EXIT /login=<nume utilizator> /password=<parolă>
```

EXITPOLICY. Dezactivarea politicii

Dezactivează o politică 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 **Dezactivare politică Kaspersky Security Center**.

Sintaxa de comandă

```
EXITPOLICY /login=<user name> /password=<password>
```

STARTPOLICY. Activarea politicii

Activează o politică Kaspersky Security Center pe computer. Setările aplicației vor fi configurate în conformitate cu politica.

DISABLE. Dezactivarea protecției

Dezactivează aplicația 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.

SPYWARE. Detectarea programelor spyware

Activați/dezactivați detectarea programelor spyware. Componenta pentru detectarea programelor spyware este activată în mod implicit.

Sintaxa de comandă

```
SPYWARE on|off
```

MDRLICENSE. Activare MDR

Efectuați operații cu 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 fișierul BLOB, *consultați Ghidul de ajutor 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 ( ).

Sintaxa de comandă

```
MDRLICENSE <funcționare> [/login=<nume utilizator> /password=<parolă>]
```

Funcționare	
`/ADD <nume fișier>`	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=<nume utilizator> /password=<parolă>`	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=!Password1`

KSN. Tranziție Global/Private KSN

Selectarea unei soluții Kaspersky Security Network pentru determinarea reputației fișierelor sau a site-urilor web. Kaspersky Endpoint Security acceptă următoarele soluții de infrastructură KSN:

- *Global KSN* este soluția folosită de majoritatea aplicațiilor Kaspersky. Participanții KSN primesc informații de la Kaspersky Security Network și trimit informațiile Kaspersky despre obiecte detectate pe computerul utilizatorului pentru a fi analizate suplimentar de analiștii Kaspersky pentru a fi incluse în bazele de date privind reputația și în cele statistice ale Kaspersky Security Network.

- *Private KSN* este o soluție care permite utilizatorilor de computere care găzduiesc Kaspersky Endpoint Security sau alte aplicații Kaspersky să obțină acces la bazele de date de renume ale Kaspersky Security Network și la alte date statistice, fără a trimite date către KSN de la propriile lor computere. Private KSN 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.

Sintaxa de comandă

```
KSN /global | /private <nume fișier>
```

Fișier configurare Private KSN		
`<nume fișier>`	Numele fișierului de configurare care conține setările serverului proxy KSN Acest fișier are extensia PKCS7 sau PEM.	

Exemplu:

```
avp.com KSN /global

avp.com KSN /private C:\ksn_config.pkcs7
```

Comenzi KESCLI

Comenzile KESCLI vă permit să primiți informații despre starea protecției computerului, utilizând componenta OPSWAT, și vă permit să efectuați activități standard precum scanările pentru viruși și actualizarea bazelor de date.

Puteți vizualiza lista comenzilor KESCLI utilizând comanda `--help` sau comanda abreviată `-h`.

Pentru a gestiona Kaspersky Endpoint Security din linia de comandă:

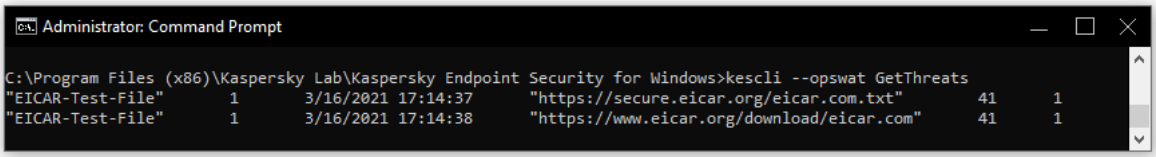
1. Executați interpretorul de linii de comandă (cmd.exe) ca administrator.

2. Deschideți directorul în care se află fișierul executabil Kaspersky Endpoint Security.

3. Pentru a executa o comandă, introduceți:

```
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 de viruși

Executați activitatea de scanare de viruși.

Sintaxa de comandă

```
--opswat Scan <domeniu scanare> <acțiune la detectarea amenințării>
```

Puteți verifica starea finalizării activității *Scanare completă* utilizând comanda `GetScanState` și puteți vizualiza data și ora când a fost finalizată ultima dată scanarea, utilizând comanda `GetLastScanTime`.

Domeniu de scanare	
`<fișiere de scanat>`	`;`-listă separată de fișiere și directoare. De ex. `C:\Program Files (x86)\Example Folder`.

Acțiune la detectarea amenințării	
`0`	Informare. Dacă este selectată această opțiune, Kaspersky Endpoint Security adaugă informațiile despre fișierele infectate în lista de amenințări active la detectarea acestor fișiere.
`1`	Dezinfectare; șterge dacă dezinfectarea nu reușește. Dacă selectezi această opțiune, Kaspersky Endpoint Security încearcă automat să dezinfecteze toate fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, Kaspersky Endpoint Security șterge fișierele. 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

Primiți informații despre starea finalizării activității *Scanare completă*:

- `1` – scanarea este în curs.
- `0` – scanarea nu se execută.

Sintaxa de comandă

```
--opswat GetScanState
```

Exemplu:

```
kescli --opswat GetScanState
```

GetLastScanTime. Determinarea orei finalizării scanării

Primiți informații despre data și ora finalizării ultimei activități *Scanare completă*.

Sintaxa de comandă

```
--opswat GetLastScanTime
```

Exemplu:

```
kescli --opswat GetLastScanTime
```

GetThreats. Obținerea datelor despe amenințările detectate

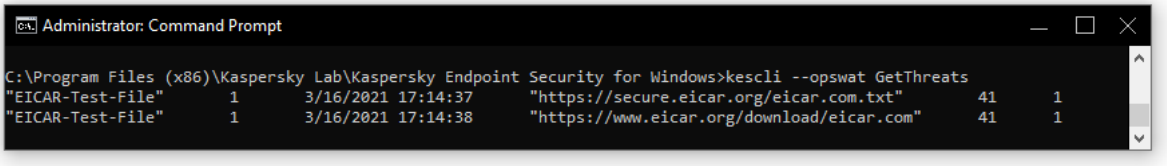
Primiți o listă cu amenințările detectate (*Raport amenințări*). Acest raport conține informații despre amenințări și activitatea virușilor din ultimele 30 de zile anterior creării raportului.

Sintaxa de comandă

```
--opswat GetThreats
```

Când este executată această comandă, Kaspersky Endpoint Security va trimite un răspuns în formatul următor:

`<numele obiect detectat>` `<tipul obiectului>` `<data și ora detectării>` `<calea către fișier>` `<acțiunea la detectarea amenințării>` `<nivelul de pericol al amenințării>`



Tip obiect	
0	Nu este cunoscut (Necunoscut).
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 (Arhivat).
20	Obiecte necunoscute (Xfiles).
21	Aplicații cunoscute (Software).
22	Fișiere mascate (Ascunse).
23	Aplicația necesită atenție (Pupware).
24	Comportament anormal (Anomalie).
30	Nedeterminat (Nedetectat).
40	Bannere publicitare (Banner).
50	Atac rețea (Atac).
51	Acces registry (Registry).
52	Activitate suspectă (Suspiciune).
60	Vulnerabilități (Vulnerabilitate).
70	Phishing
80	Atașare e-mail nedorită (Atașare).
90	Malware detectat de Kaspersky Security Network (Urgent).
100	Link necunoscut (URL suspicios).
110	Alt malware (Comportamental).

Acțiune la detectarea amenințării	
0	Nu este cunoscut (necunoscut).
1	Amenințarea a fost remediată (ok).
2	Obiectul a fost infectat și nu a fost dezinfectat (infectat).
5	Obiectul este într-o arhivăși nu a fost dezinfectat (arhivă).
9	Obiectul a fost dezinfectat (dezinfectat).

10	Obiectul nu a fost dezinfectat (nedezinfectat).
11	Obiectul a fost șters (șters).
13	A fost creată o copie de rezervă a obiectului (copiat de rezervă).
15	Obiectul a fost mutat în Copie de rezervă (carantinat).
23	Obiectul a fost șters la repornirea computerului (șterge la repornire).
25	Obiectul a fost dezinfectat la repornirea computerului (dezinfectează la repornire).
29	Obiectul a fost mutat în Copie de rezervă de către un utilizator (adăugat de utilizator).
30	Obiectul a fost adăugat la excluderi (adăugat la excluderi).
31	Obiectul a fost mutat În Copie de rezervă la repornirea computerului (carantinează la repornire).
36	Fals pozitiv (alarmă falsă).
38	Procesul a fost terminat (terminat).
40	Obiectul nu a fost detectat (negăsit).
41	Nu se poate soluționa amenințarea (netratabil).
42	Obiectul a fost restaurat (rulat înapoi).
43	Obiectul a fost creat ca rezultat al activității amenințării (produs de amenințare).
44	Obiectul a fost restaurat la repornirea computerului (derulează înapoi la repornire).
0xffffffff	Obiectul nu a fost procesat (înlăturat).

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

Executați activitatea *Actualizare* Kaspersky Endpoint Security utilizează sursa implicită: serverele de actualizare Kaspersky.

Sintaxa de comandă

```
--opswat UpdateDefinitions
```

Puteți vizualiza data și ora ultimei activități de *Actualizare* finalizată, utilizând comanda `GetDefinitionsetState`.

Exemplu:
```
kescli --opswat UpdateDefinitions
```

GetDefinitionState. Determinarea orei finalizării actualizării

Primiți informații despre data și ora finalizării ultimei activități *Actualizare*.

Sintaxa de comandă

```
--opswat GetDefinitionState
```

Exemplu:
```
kescli --opswat GetDefinitionState
```

EnableRTP. Activarea protecției

Enable Kaspersky Endpoint Security protection components on the computer: File Threat Protection, Web Threat Protection, Mail Threat Protection, Network Threat Protection, Host Intrusion Prevention.

Sintaxa de comandă

```
--opswat EnableRTP
```

Puteți verifica starea de funcționare a componentei File Threat Protection utilizând comanda `GetRealTimeProtectionState`.

Exemplu:
```
kescli --opswat EnableRTP
```

GetRealTimeProtectionState. Starea File Threat Protection

Primiți informații despre starea de funcționare a componentei File Threat Protection:

- `1` – componenta este activată.
- `0` – componenta este dezactivată.

Sintaxa de comandă

```
--opswat GetRealTimeProtectionState
```

Exemplu:
```
kescli --opswat GetRealTimeProtectionState
```

Version. Identificarea versiunii aplicației

Identificați versiunea Kaspersky Endpoint Security for Windows.

Sintaxa de comandă

```
--Version
```

Puteți utiliza, de asemenea, comanda abreviată `-v`.

Exemplu:
`kescli -v`

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, `Eroare: Nu se poate începe activitatea „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

Codul de eroare	Descriere
09479001	Cheia de licență pentru Kaspersky Endpoint Security este deja folosită pe acest computer.
0947901D	Licență expirată. Actualizarea bazei de date nu este disponibilă.
89479002	Cheia nu a fost găsită.
89479003	Semnătura digitală lipsește sau este deteriorată.
89479004	Datele sunt deteriorate.
89479005	Fișierul cheie este deteriorat.
89479006	Licența a expirat sau cheia de licență a expirat.
89479007	Fișier cheie nespecificat.
89479008	Nu se poate aplica fișierul cheie.
89479009	Salvarea datelor nu a reușit.
8947900A	Citirea datelor nu a reușit.
8947900B	Eroare I/O.
8947900C	Bazele de date nu au fost găsite.
8947900E	Biblioteca de licențiere nu a fost încărcată.
8947900F	Bazele de date sunt deteriorate sau actualizate manual.
89479010	Bazele de date sunt deteriorate.
89479011	Nu se poate utiliza fișierul cheie nevalid pentru a adăuga o cheie de rezervă.

89479012	Eroare de sistem.
89479013	Lista de chei respinse este alterată.
89479014	Semnătura digitală a fișierului nu se potrivește cu semnătura digitală a Kaspersky.
89479015	Nu se poate utiliza o cheie pentru licența necomercială ca cheie pentru licența comercială.
89479016	Licența beta este necesară pentru a utiliza versiunea beta a aplicației.
89479017	Fișier cheie nu este compatibil cu această aplicație.
89479018	Cheia a fost blocată de Kaspersky.
89479019	Aplicația a fost deja folosită sub o licență trial. Nu se poate adăuga din nou cheia trial.
8947901A	Fișierul cheie este deteriorat.
8947901B	Semnătura digitală lipsește, este deteriorată sau nu se potrivește cu semnătura digitală a Kaspersky.
8947901C	Nu se poate adăuga o cheie dacă licența necomercială corespunzătoare a expirat.
8947901E	Data la care fișierul cheie a fost creat sau utilizat nu este valabilă. Verificați data sistemului.
8947901F	Nu se poate adăuga o cheie pentru licența trial: o altă cheie pentru licența trial este deja activă.
89479020	Lista de chei respinse este alterată sau lipsește.
89479021	Descrierea actualizării lipsește sau este deteriorată.
89479022	Eroare în datele serviciilor cheie de licență.
89479023	Nu se poate utiliza fișierul cheie nevalid pentru a adăuga o cheie de rezervă.
89479025	Eroare la trimiterea solicitării către serverul de activare. Motive posibile: Eroare de conexiune la Internet sau probleme temporare pe serverul de activare. Încercați să activați mai târziu aplicația folosind codul de activare. Dacă această eroare persistă, contactați furnizorul de internet.
89479026	Eroare în răspunsul de la serverul de activare.
89479027	Nu se poate obține starea răspunsului.
89479028	A apărut o eroare la salvarea fișierului temporar.
89479029	Codul de activare a fost introdus incorect sau data sistemului este incorectă. Verificați data sistemului pe computer.
8947902A	Fișierul cheie nu este compatibil cu această aplicație sau licența a expirat. Nu puteți activa Kaspersky Endpoint Security utilizând un fișier cheie pentru o altă aplicație.
8947902B	Primirea fișierului 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	Serverul de activare a returnat eroarea 404.
89479030	Serverul de activare a returnat eroarea 405.
89479031	Serverul de activare a returnat eroarea 406.
89479032	Este necesară autentificarea pe serverul proxy. Verificați setările rețelei.
89479033	Timpul de solicitare a expirat.

89479034	Serverul de activare a returnat eroarea 409.
89479035	Serverul de activare a returnat eroarea 410.
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.
8947903A	Serverul de activare a returnat eroarea 415.
8947903C	Eroare internă server.
8947903D	Funcționalitatea nu este acceptată.
8947903E	Răspuns nevalid de la gateway. Verificați setările rețelei.
8947903F	Serviciu indisponibil (eroare HTTP 503).
89479040	Intervalul de timp pentru răspuns de la gateway a expirat. Verificați setările rețelei.
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	Eroare la convertirea parametrilor la șirul ANSI (adresă URL, director, agent).
8947904A	Eroare la crearea firului de lucru.
8947904B	Firul de lucru se execută deja.
8947904C	Firul de lucru nu se execută.
8947904D	Fișierul cheie nu a fost găsit pe serverul de activare.
8947904E	Cheia este blocată.
8947904F	Eroare internă a serverului de activare.
89479050	Date insuficiente în solicitarea de activare.
89479053	Cheia de licență a expirat.
89479054	Pe computer este setată o dată incorectă a sistemului.
89479055	Licența trial a expirat.
89479056	Licență expirată.
89479057	Limita activărilor aplicației a fost depășită pentru codul specificat.
89479058	Procedura de activare s-a încheiat cu o eroare de sistem.
89479059	Nu se poate utiliza o cheie pentru licența necomercială ca cheie pentru licența comercială.
8947905C	Codul de activare este necesar.
89479062	Conectare la serverul de activare nu se poate realiza.
89479064	Serverul de activare este indisponibil. Vă rugăm să verificați setările conexiunii la Internet și să

	încercați din nou activarea.
89479065	Data lansării bazei de date a aplicației depășește data de expirare a licenței.
89479066	Nu se poate înlocui cheia activă cu o cheie expirată.
89479067	Nu se poate adăuga o cheie rezervă dacă aceasta expiră înainte de licența curentă.
89479068	Cheia abonamentului actualizată lipsește.
8947906A	Cod de activare incorect (suma de control nu se potrivește).
8947906B	Cheia este deja activă.
8947906C	Tipurile de licențe care corespund cheilor active și de rezervă nu se potrivesc.
8947906D	Componenta nu este acceptată de licență.
8947906E	Nu s-a putut adăuga cheia abonamentului drept cheie de rezervă.
89479213	Eroare generală a stratului de transport.
89479214	Conectarea la serverul de activare nu a reușit.
89479215	Format URL nevalid.
89479216	Conversia adresei serverului proxy nu a reușit.
89479217	Conversia adresei serverului nu a reușit. Verificați setările conexiunii la Internet.
89479218	Conectarea la serverul de activare sau la serverul proxy nu a reușit.
89479219	Accesul de la distanță a fost refuzat.
8947921A	Intervalul de timp pentru răspuns a expirat.
8947921B	Eroare la trimiterea solicitării HTTP.
8947921C	Eroare de conexiune SSL.
8947921D	Operațiunea a fost întreruptă de apelarea inversă.
8947921E	Prea multe încercări de redirecționare.
8947921F	Verificarea destinatarului a eșuat.
89479220	Răspuns gol de la serverul de activare.
89479221	Eroare la trimiterea datelor.
89479222	Eroare la primirea datelor.
89479223	Eroare de certificare SSL locală.
89479224	Eroare de criptare SSL.
89479225	Eroare de certificare SSL server.
89479226	Conținut nevalid al pachetului de rețea.
89479227	Accesul utilizatorului a fost refuzat.
89479228	Fișier de certificare SSL nevalid.
89479229	Stabilirea conexiunii SSL nu a reușit.
8947922A	Trimiterea sau primirea pachetului de rețea nu a reușit. Vă rugăm să încercați din nou mai târziu.
8947922B	Fișier nevalid cu certificate revocate.
8947922C	Eroare solicitare certificat SSL.

89479401	Eroare server necunoscută.
89479402	Eroare internă server.
89479403	Nu a fost introdusă nicio cheie de licență disponibilă pentru codul de activare.
89479404	Cheia activă a fost blocată.
89479405	Parametrii necesari ai solicitării de activare a aplicației lipsesc.
89479406	Nume de utilizator sau parolă incorecte.
89479407	Cod de activare incorect trimis serverului.
89479408	Codul de activare nu este valabil pentru Kaspersky Endpoint Security. Nu puteți activa Kaspersky Endpoint Security utilizând un fișier cheie pentru o aplicație necunoscută.
89479409	Solicitării îi lipsește un cod de activare.
8947940B	Licența a expirat (conform datelor de la serverul de activare).
8947940C	Numărul de activări cu acest cod a fost depășit.
8947940D	Format nevalid al ID-ului solicitării.
8947940E	Codul de activare nu este valabil pentru Kaspersky Endpoint Security. Codul de activare este pentru o altă aplicație Kaspersky.
8947940F	Nu se poate actualiza cheia de licență.
89479410	Codul de activare nu este valid pentru această regiune.
89479411	Codul de activare nu este valabil pentru versiunea de limbă a Kaspersky Endpoint Security.
89479412	Este necesar acces suplimentar la serverul de activare.
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	Formatul codului de activare nu este acceptat de serverul de activare.
89479418	Formatul codului de activare nu este valabil.
89479419	Pe computer este setată o oră incorectă a sistemului.
8947941A	Codul de activare nu este valabil pentru versiunea Kaspersky Endpoint Security.
8947941B	Abonamentul a expirat.
8947941C	Numărul de activări a fost depășit pentru această cheie de licență.
8947941D	Semnătură digitală nevalidă a cheii de licență.
8947941E	Sunt necesare date suplimentare.
8947941F	Verificarea datelor utilizatorului nu a reușit.
89479420	Abonament inactiv.
89479421	Serverul de activare este în întreținere.
89479501	Eroare necunoscută a Kaspersky Endpoint Security.
89479502	Parametru nevalid transferat (de exemplu, o listă goală de adrese a serverelor de activare).

89479503	Cod de activare incorect.
89479504	Nume de utilizator nevalid.
89479505	Parolă utilizator nevalidă.
89479506	Răspuns nevalid de la serverul de activare.
89479507	Cererea 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`, `STARE`, `STATISTICI`, `EXPORT` și `IMPORT`. 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.
- `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.
- `Mail_Monitoring` sau `EM` – Mail Threat Protection.
- `Rollback` – derulare înapoi a actualizării.
- `Scan_ContextScan` – Scanare din meniu contextual.
- `Scan_IdleScan` – Scanare în fundal.
- `Scan_Memory` - Scanare memorie nucleu.
- `Scan_My_Computer` – Scanare completă.
- `Scan_Objects` – Scanare particularizată.

- `Scan_Qscan` - Scanare obiecte care sunt încărcate la pornirea sistemului de operare.
- `Scan_Removable_Drive` – Scanare unități amovibile.
- `Scan_Startup` sau `STARTUP` – Scanare zone critice.
- `Updater` – Actualizare.
- `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.

DESCHIDEȚI 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.

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=<nume utilizator>`

     Nume de utilizator pentru gestionarea aplicației folosind REST API. Introduceți numele de utilizator în formatul `<DOMENIU>\<NumeUtilizator>` (de exemplu, `RESTAPI_User=COMPANIE\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 folosit pentru schimbul de date. Parametru opțional. Portul 6782 este selectat în mod implicit.
   - `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.

Puteți defini setările pentru lucrul cu API REST numai în timpul instalării aplicației. Nu este posibilă modificarea setărilor după instalarea aplicației. Dacă doriți să modificați setările, dezinstalați Kaspersky Endpoint Security și reinstalați-l cu noile setări 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 /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
```

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.

DESCHIDEȚI 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. Pentru aceasta, trimiteți o solicitare POST. Folosiți structura setărilor primită ca răspuns la solicitarea GET.

   Exemplu:

```
POST http://localhost:6782/kes/v1/settings/ExploitPrevention
{
"action": 0,
"enableSystemProcessesMemoryProtection": false,
"enabled": true
}
```

4. Aplicația va aplica modificările în setări și va trimite un răspuns care conține rezultatele configurației aplicației.

Surse de informații despre aplicație

Pagina Kaspersky Endpoint Security pe site-ul Web Kaspersky

În pagina Kaspersky Endpoint Security, poți vedea informații generale despre aplicație și despre funcțiile și caracteristicile ei.

Pagina Kaspersky Endpoint Security conține un link către magazinul online. Aici poți să achiziționezi sau să îți reînnoiești licența pentru aplicație.

Pagina Kaspersky Endpoint Security din baza de cunoștințe

Baza de cunoștințe este o secțiune de pe site-ul Web de Asistență tehnică.

În pagina Kaspersky Endpoint Security din Baza de cunoștințe, poți citi articole care oferă informații folositoare, recomandări și răspunsuri la întrebări frecvente despre cum să achiziționezi, să instalezi și să utilizezi aplicația.

Articolele din Baza de cunoștințe pot răspunde la întrebări care nu sunt legate doar de Kaspersky Endpoint Security, ci și de alte aplicații Kaspersky. Articolele din Baza de cunoștințe pot conține, de asemenea, noutăți de la serviciul de Asistență tehnică.

Discutarea aplicațiilor Kaspersky în comunitatea utilizatorilor

Dacă întrebarea dvs. nu necesită un răspuns urgent, o puteți discuta cu experții Kaspersky și cu alți utilizatori din funcționalitatea Comunitate.

În comunitate, puteți să vizualizați subiectele existente, să postați propriile comentarii și să creați noi subiecte de discuție.

Contactarea Suportului tehnic

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 permite urmărirea procesului prin care se execută comenzile aplicației pas cu pas și se stabilește etapa din funcționarea aplicației în 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.
- Ajustarea unor setări ale componentelor individuale ale aplicației care nu sunt disponibile în interfața 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. Modificările nesupravegheate în setările aplicației efectuate altminteri decât este descris în Ghidul administratorului sau în instrucțiunile specialiștilor departamentului de Asistență tehnică pot duce la încetinirea sau blocarea sistemului de operare, pot afecta securitatea computerului sau pot compromite disponibilitatea și integritatea datelor 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\Traces.

Fișierele de urmărire sunt denumite după cum urmează: `KES<număr versiune serviciu_dataXX.XX_oraXX.XX_pidXXX.><tip fișier urmărire>.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.

Kaspersky Endpoint Security salvează parolele utilizatorilor într-un fișier de urmărire numai în formă criptată.

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<număr versiune_dataXX.XX_oraXX.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 solicitări din aplicații 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 se stochează pe computerul pe care este implementată Kaspersky Security Center 12 Web Console, în directorul Program Files\Kaspersky Lab\Kaspersky Security Center Web Console 12\logs.

Fișierele de urmărire ale plug-inului web al aplicației sunt denumite după cum urmează: `logs-kes_windows-<tip fișier urmărire>.DESKTOP-<dată actualizare fișier>.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 aplicație*.
- 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 Informații volum sistem 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 aplicațiilor

Urmărirea aplicațiilor reprezintă înregistrări detaliate ale acțiunilor efectuate de aplicație și mesaje despre evenimente apărute în cursul funcționării aplicației.

Urmărirea aplicațiilor trebuie efectuată sub supravegherea Serviciul de asistență tehnică al Kaspersky.

Pentru a crea un fișier de urmărire a aplicațiilor:

1. În fereastra principală a aplicației, faceți clic pe butonul .

   Se deschide fereastra **Asistență**.

2. În fereastra **Asistență**, faceți clic pe butonul **Instrumente de suport**.

3. Utilizați comutatorul **Activare urmărire aplicații** pentru a activa sau dezactiva urmărirea funcționării aplicației.

4. În lista derulantă **Urme**, selectați un mod de urmărire a aplicației:

   - **cu rotație**. 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 numărul maxim de fișiere pentru rotație și dimensiunea maximă pentru fiecare fișier.

   - **Scrie într-un singur fișier**. Salvați un fișier de urmărire (fără limită de dimensiune).

5. În lista verticală **Nivel**, selectați nivelul de urmărire.

   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 (500)**.

6. Repornește Kaspersky Endpoint Security.

7. Pentru a opri procesul de urmărire, reveniți la fereastra **Asistență** și dezactivați urmărirea.

Poți crea, de asemenea, fișiere de urmărire la instalarea aplicației din linia de comandă, inclusiv prin utilizarea fișierului setup.ini.

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\Traces. În mod implicit, urmărirea este dezactivată.

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 Serviciul de asistență tehnică al Kaspersky.

Pentru a crea un fișier de urmărire a performanței:

1. În fereastra principală a aplicației, faceți clic pe butonul .

   Se deschide fereastra **Asistență**.

2. În fereastra **Asistență**, faceți clic pe butonul **Instrumente de suport**.

3. Utilizați comutatorul **Activare urmărire performanță** pentru a activa sau dezactiva urmărirea performanței aplicației.

4. În lista derulantă **Urme**, selectați un mod de urmărire a aplicației:

   - **cu rotație**. 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.

   - **Scrie într-un singur fișier**. Salvați un fișier de urmărire (fără limită de dimensiune).

5. În lista verticală **Nivel**, selectați nivelul de urmărire:

   - **Ușor**. Kaspersky Endpoint Security analizează principalele 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 **Asistență** și dezactivați urmărirea.

Drept urmare, va fi creat un fișier de urmărire a performanței în directorul %ProgramData%\Kaspersky Lab\KES\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 computer cât timp aplicația este în uz și sunt permanent șterse atunci când aplicația este eliminată. Fișierele de imagine sunt stocate în directorul %ProgramData%\Kaspersky Lab\KES\Traces.

Pentru a activa sau a dezactiva scrierea fișierelor de imagine:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.

2. În fereastra de setări a aplicației, selectați secțiunea **General**.

3. În blocul **Informații depanare**, utilizați caseta de selectare **Activare scriere imagine** 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.

Pentru a activa și a dezactiva protecția pentru fișierele imagine și de urmărire:

1. În partea de jos a ferestrei principale a aplicației, faceți clic pe butonul ⚙.

2. În fereastra de setări a aplicației, selectați secțiunea **General**.

3. În blocul **Informații depanare**, utilizați caseta de selectare **Activare protecție fișiere 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.

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.

- 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.

- La actualizarea de la Kaspersky Endpoint Security 10 Service Pack 2 for Windows (versiunea 10.3.0.6294), componenta Host Intrusion Prevention este activată.

- Atunci când actualizați Kaspersky Endpoint Security 10 for Windows Service Pack 2 (versiunea 10.3.0.6294), fișierele care au fost plasate în Copie de rezervă sau în Carantină în versiunea precedentă a aplicației vor fi transferate în Copie de rezervă în noua versiune a aplicației. Aceste fișiere nu sunt transferate pentru versiuni anterioare Kaspersky Endpoint Security 10 for Windows Service Pack 2 (versiunea 10.3.0.6294). Pentru a le salva, trebuie să restaurați fișierele din Carantină și Copie de rezervă înainte de a face upgrade aplicației. După finalizarea actualizării, scanați din nou fișierele restaurate.

- 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 încercați să instalați orice versiune a modulului de criptare AES pe un computer care are Kaspersky Endpoint Security for Windows 11.6.0, dar nu are componente de criptare instalate, instalarea modulului de criptare se va încheia cu un mesaj de eroare care afirmă că este instalată o versiune mai nouă a aplicației. Începând cu Kaspersky Endpoint Security 10 for Windows Service Pack 2 (versiunea 10.3.0.6294), nu există un fișier de instalare separat pentru modulul de criptare. Bibliotecile de criptare sunt incluse în pachetul de distribuție a aplicației. Kaspersky Endpoint Security 11.6.0 este incompatibil cu modulele de criptare AES. Bibliotecile necesare pentru criptare sunt instalate automat atunci când este selectată componenta Full Disk Encryption (FDE) sau File Level Encryption (FLE).

- 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.

- Începând cu versiunea 11.0.0 a aplicației, puteți 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, ștergeți plug-inul actual și instalați o versiune anterioară a acestuia.

- La actualizarea Kaspersky Endpoint Security 11.0.0 sau 11.0.1 for Windows, setările de planificare a activităților locale pentru activitățile de *Actualizare*, *Scanare zone critice*, *Scanare personalizată* și *Verificare integritate* nu sunt salvate.

- Dacă ați anulat eliminarea aplicației, începeți recuperarea acesteia după repornirea computerului.

- 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.

- Dacă actualizați o versiune anterioară a aplicației la versiunea 11.6.0, pentru a instala Kaspersky Endpoint Agent, reporniți computerul și conectați-vă la sistem utilizând un cont cu drepturi de administrator local. În caz contrar, Kaspersky Endpoint Agent nu va fi instalat în timpul procedurii de actualizare.

- 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.

- Dacă faceți upgrade pentru Kaspersky Endpoint Security 10 for Windows Service Pack 2 Maintenance Release 4 cu componenta File Level Encryption (FLE) instalată pe computere care execută Windows 10 versiunile 1809, 1903 și 1909, driverele FDE nu vor fi instalate în imaginea WinRE.

- 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.

- După ce aplicația este actualizată de la versiuni anterioare Kaspersky Endpoint Security 11 for Windows, computerul trebuie repornit.

Compatibilitate pentru platforme de servere

- Sistemul de fișiere ReFS este acceptat cu limitări:
  - După pornirea verificării antivirus a serverului, excluderile de la scanare adăugate cu iChecker sunt resetate atunci când serverul este repornit.
  - 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.
- Configurațiile Server Core și Cluster Mode nu sunt acceptate.
- Tehnologiile File Level Encryption (FLE) și Kaspersky Disk Encryption (FDE) nu sunt acceptate pe platformele de tip server.
- Componenta Control dispozitive nu este acceptată pe platformele serverelor.
- 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.
- Dacă ați inițiat câteva sesiuni active pe serverul terminalului, Kaspersky Endpoint Security ar putea întâmpina probleme la afișarea de notificări. De exemplu: utilizatorul din sesiunea cu numărul 1 rulează o verificare a reputației unui fișier în KSN. Kaspersky Endpoint Security va afișa utilizatorului din sesiunea cu numărul 2 o notificare cu rezultatele verificării.

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 consideră Windows 10 Enterprise multi-session ca fiind un sistem de operare pentru servere. Prin urmare, se acceptă Windows 10 Enterprise multi-session, cu limitări de server specifice platformei. De exemplu, serverele nu pot utiliza unele componente din cadrul Kaspersky Endpoint Security. De asemenea, aplicația utilizează o cheie de licență pentru servere, în locul unei chei de licență pentru stații de lucru.
  - 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 **Asigurare compatibilitate 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\**\*"
  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.

Compatibilitate cu Kaspersky Security Center

- Puteți gestiona componenta Control adaptiv al anomaliilor numai în Kaspersky Security Center versiunea 11 sau ulterioară.
- Este posibil ca raportul de amenințări al Kaspersky Security Center 11 să nu afișeze informații despre acțiunile întreprinse asupra amenințărilor detectate de componenta Protecție AMSI.
- Starea de funcționare a componentelor Protecție AMSI și Control adaptiv al anomaliilor este disponibilă numai în Kaspersky Security Center versiunea 11 sau ulterioară. Puteți vedea starea de funcționare în Kaspersky Security Center Console, în proprietățile computerului, din secțiunea **Activități**. Rapoartele pentru aceste componente sunt disponibile și în Kaspersky Security Center versiunea 11 sau ulterioară.

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.
- Aplicația nu poate fi activată cu un abonament prin Kaspersky Security Center dacă licența a expirat sau dacă o licență pentru versiunea trial este activă pe computer. Pentru a înlocui o licență de versiune trial sau o licență care va expira în curând cu o licență de abonament, utilizați activitatea de distribuire a licenței.
- 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 se datorează faptului că aplicația se instalează mai întâi și încearcă să activeze licența de versiune trial încorporată, care necesită acces la Internet pentru activare în timpul procedurii de instalare.
- 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 se datorează faptului că aplicația instalează și încearcă din nou să activeze licența de versiune trial încorporată, care necesită acces la Internet pentru activare la instalarea unui upgrade.
- 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 11.6.0, 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.

Remediation Engine

- Aplicația restaurează fișiere numai pe dispozitive care au sistemul de fișiere NTFS sau FAT32.
- 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.
- Aplicația nu monitorizează modificările aduse fișierelor printr-o interfață de rețea (de exemplu, dacă un fișier este stocat într-un director partajat și un proces este pornit de la distanță de pe alt computer).

Firewall

- 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.
- În versiunile aplicației 11.0.0 și 11.0.1, adresele MAC definite sunt aplicate incorect. Setările adresei MAC pentru versiunile 11.0.0, 11.0.1 și 11.1.0 sau mai recente nu sunt compatibile. După actualizarea aplicației sau a plug-inului de la aceste versiuni la versiunea 11.1.0 sau una ulterioară, trebuie să verificați și să reconfigurați adresele MAC definite în regulile Firewall.
- La actualizarea aplicației de la versiunile 11.1.1 și 11.2.0 la versiunea 11.6.0, stările permisiunilor pentru următoarele reguli Firewall nu sunt migrate:
  - Solicitări către serverul DNS prin TCP.
  - Solicitări către serverul DNS prin UDP.
  - Orice activitate de rețea.
  - Răspunsuri de intrare ICMP Destination Unreachable.
  - Flux ICMP de intrare.
- 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 puteți 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.
- A apărut eroare la Kaspersky Endpoint Security for Windows 11.5.0–11.6.0 în timpul importării unei liste cu reguli de pachete Firewall. Acest lucru poate avea ca rezultat ștergerea adreselor locale su la distanță definite de utilizator dintr-o regulă. Pentru a remedia eroarea, contactați Suportul tehnic. Suportul tehnic vă va furniza o actualizare corectată pentru plug-in. Sau puteți actualiza aplicația la următoarea versiune, după lansarea acesteia.
- Când se importă o listă cu reguli de pachet Firewall, Kaspersky Endpoint Security poate modifica numele regulilor. Aplicația identifică regulile care au același set de parametri principali, cum ar fi protocolul, direcția, porturile locale și la distanță și timpul de viață al pachetului (TTL). Dacă acest set de parametri principali este identic pentru mai multe reguli, aplicația atribuie același nume acestor reguli sau adaugă o etichetă cu parametrul la nume. Aceasta înseamnă că Kaspersky Endpoint Security importă toate regulile de pachete, dar numele regulilor care au parametri principali identici pot fi modificate.
- Când este declanșată o regulă pentru pachetele de rețea în Kaspersky Endpoint Security 11.6.0 sau anterior, 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 coloanei **Nume aplicație** rămâne goală.

Application Control

- 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.
- Când aplicațiile web progresive (PWA) sunt blocate de componenta Application Control, appManifest.xml este indicat ca aplicație blocată în raport.

Control dispozitive

- 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.
- 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.

Control Web

- Formatele OGV și WEBM nu sunt acceptate.
- Protocolul RTMP nu este acceptat.

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.

Criptare unitate (FDE)

- 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.
- Pentru detalii despre restaurarea unui sistem de operare dintr-o copie de rezervă pe un dispozitiv GPT criptat, vizitați Baza de cunoștințe a suportului tehnic.
- Mai mulți agenți de descărcare nu pot coexista pe un computer criptat.
- 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 `<domeniu>/<nume cont Windows>`, 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 și a directoarelor nu este acceptată în sistemele de operare ale familiei Microsoft Windows Embedded.
- După ce ați instalat aplicația, trebuie să reporniți sistemul de operare astfel încât criptarea fișierelor și a directoarelor să funcționeze corect.
- 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.
- 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.
- 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.
- Componenta Manager de fișiere portabil nu poate fi utilizată pentru a obține acces la o unitate amovibilă dacă sunt îndeplinite simultan următoarele condiții:
  - 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.

  În acest caz, 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.
- 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 (CSC) 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. Pentru detalii privind asistența pentru cache-ul în partea clientului (CSC) atunci când se utilizează criptarea, consultați Baza de cunoștințe a suportului tehnic.
- 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.
- Când unitățile amovibile sunt criptate cu compatibilitate pentru modul portabil, controlul vârstei parolei nu poate fi dezactivat.
- 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.
- Criptarea fișierelor în directoare de sincronizare OneDrive nu este acceptată. Adăugarea de directoare cu fișiere deja criptate în lista de sincronizare OneDrive poate duce la pierderea datelor din fișierele criptate.
- Când este instalată componenta de criptare la nivel de fișier, gestionarea utilizatorilor și a grupurilor nu funcționează în modul WSL (subsistemul Windows pentru Linux).
- Când este instalată componenta de criptare la nivel de fișier, POSIX (Portable Operating System Interface) pentru redenumirea și ștergerea fișierelor nu este acceptat.

- După actualizarea Kaspersky Endpoint Security for Windows versiunea 11.0.1 sau anterioară, pentru a accesa fișierele criptate după repornirea computerului, asigurați-vă că Agentul de rețea se execută. Agentul de rețea are o pornire întârziată, așa că nu puteți accesa fișierele criptate imediat după încărcarea sistemului de operare. Nu este nevoie să așteptați ca Agentul de rețea să pornească după următoarea pornire a computerului.

Alte limitări

- În sistemele de operare server, nu se afișează nicio avertizare cu privire la necesitatea dezinfectării avansate.
- Adresele web adăugate la lista de încredere pot fi procesate incorect.
- 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 nu acceptă standardul RFC9218 pentru protocolul HTTP/2. Dacă Kaspersky Endpoint Security detectează acest format de schimb de date în trafic, aplicația blochează această conexiune, iar browserul afișează eroarea ERR_HTTP2_PROTOCOL_ERROR. Dacă trebuie să accesezi această resursă web, poți să excluzi resursa web de la scanările conexiunii criptate sau poți contacta departamentul Suport tehnic pentru o corecție.
- Monitorizare sistem. Informațiile complete despre procese nu sunt afișate.
- 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.
- 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).
- Activitatea *Scanare de viruși* nu acceptă versiunea pe 64 de biți a Microsoft Outlook. Aceasta înseamnă că Kaspersky Endpoint Security nu verifică fișierele Outlook x64 (fișierele PST și OST) chiar dacă e-mailul este inclus în domeniul de scanare.
- În Kaspersky Security Center 10, când treceți de la utilizarea rețelei globale Kaspersky Security Network la utilizarea rețelei private Kaspersky Security Network sau viceversa, 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.
- 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 produsului și în raportul Kaspersky Security Center 10.
- Componenta Senzor Endpoint nu poate fi instalată în Microsoft Windows Server 2008.
- Raportul Kaspersky Security Center 10 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.
- 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, utilizați opțiunea Ready Boot sau creșteți timpul de expirare al sistemului de operare pentru pornirea serviciilor.
- Aplicația nu poate funcționa în modul de siguranță.
- Pentru a vă asigura că Kaspersky Endpoint Security for Windows versiunile 11.5.0 și 11.6.0 pot funcționa corect cu software-ul Cisco AnyConnect, trebuie să instalați Modulul de conformitate versiunea 4.3.183.2048 sau ulterioară. Aflați mai multe despre compatibilitatea cu Cisco Identity Services Engine în documentația Cisco.
- Nu putem garanta că controlul audio va funcționa până la prima repornire după instalarea aplicației.
- 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.
- Activitatea de verificare a disponibilității KSN nu mai este acceptată.
- Dezactivarea opțiunii „Dezactivare gestionare externă a serviciului de sistem" nu vă va permite să opriți serviciul aplicației care a fost instalată cu parametrul `AMPPL=1` (în mod implicit, valoarea parametrului este setată la `1` începând cu versiunea de sistem de operare Windows 10RS2). 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\.
- La actualizarea aplicației de la versiunea 11.1.0 la 11.6.0, setările componentei Protecție AMSI vor fi resetate la valorile lor implicite.
- Dacă utilizați politicile de restricționare a software-ului (SRP), computerul poate să nu se încarce (ecran negru). Vă sfătuim să modificați setările SRP după cum urmează: setați valoarea **Toate fișierele software cu excepția bibliotecilor (cum ar fi DLL)** pentru parametrul **Aplicare politici de restricționare a software-ului la următoarele obiecte** și adăugați reguli cu nivelul de securitate **Nerestricționat** pentru căile către fișierele aplicației (`C:\Program Files\Common Files\Kaspersky Lab` și `C:\Program Files\Kaspersky Lab`). Pentru detalii despre utilizarea SRP, consultați *documentația Microsoft*.
- 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 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.

- 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.

- Când se scanează o conexiune criptată, Kaspersky Endpoint Security forțează HTTP/1.

- Când aplicația Kaspersky Endpoint Security este instalată pe serverul Windows Server 2019 este compatibilă cu Docker. Implementarea containerelor Docker pe un computer cu Kaspersky Endpoint Security cauzează o eroare (BSOD).

Glosar

Activitate

Funcții efectuate de aplicația Kaspersky ca activități, de exemplu: Protecție în timp real pentru fișiere, Scanare completă dispozitive, 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.

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.

Cheie suplimentară

O cheie care certifică dreptul de utilizare a aplicației, însă care nu este utilizată în prezent.

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.

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.

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 din directorul denumit `Folder` și din subdirectoarele sale. 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.

- Caracterul `?` (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.

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 împiedici infectarea sistemului de fișiere al computerului. În mod implicit, componenta File Threat Protection de își are originea permanentă în memoria RAM a computerului. Componenta scanează fișierele de pe toate unitățile computerului, precum și 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 utilizator sau 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 încercați să accesați un fișier al cărui conținut este stocat în stocarea 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, Kaspersky Endpoint Security 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, Kaspersky Endpoint Security scanează numai fișierele infectabile. Formatul fișierului se determină în funcție de extensia sa.
Domeniu de protecție	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. De asemenea, puteți exclude un obiect (cum ar fi unități amovibile) din scanări.
Tehnologia Machine 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	**Dezinfectare; șterge dacă dezinfectarea nu reușește**. Dacă selectați această opțiune, Kaspersky Endpoint Security încearcă automat să dezinfecteze toate fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, Kaspersky Endpoint Security șterge fișierele. **Dezinfectare. Blochează dacă dezinfectarea nu reușește**. Dacă selectați această opțiune, Kaspersky Endpoint Security încearcă automat să dezinfecteze toate fișierele infectate care sunt detectate. Dacă nu este posibilă dezinfectarea, Kaspersky Endpoint Security adaugă informațiile despre fișierele infectate detectate în lista de amenințări active. **Blocare**. Dacă selectezi această opțiune, componenta File Threat Protection blochează automat toate fișierele infectate, fără a încerca să le dezinfecteze.

	Înainte de a încerca să dezinfectați sau să ștergeți un fișier infectat, Kaspersky Endpoint Security creează o copie de rezervă a fișierului în cazul în care trebuie să restaurați fișierul sau dacă acesta poate fi dezinfectat în viitor.
Scanare 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.
Scanare arhive	Scanează arhivele în următoarele formate: RAR, ARJ, ZIP, CAB, LHA, JAR, și ICE.
Scanare pachete de distribuție	Această casetă de selectare activează/dezactivează scanarea pachetelor de distribuție terțe.
Scanare fișiere în formate Microsoft Office	Scanează fișierele Microsoft Office (DOC, DOCX, XLS, PPT și alte extensii Microsoft). Fișierele în format Office includ și obiecte OLE.
Nu dezarhiva fișiere 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 mari extrase din arhive, indiferent dacă această casetă de selectare este bifată sau nu.
Dezarhivare fișiere 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.
Mod 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.
Tehnologie 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 scanare 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.
Tehnologie 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).
Punere 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.

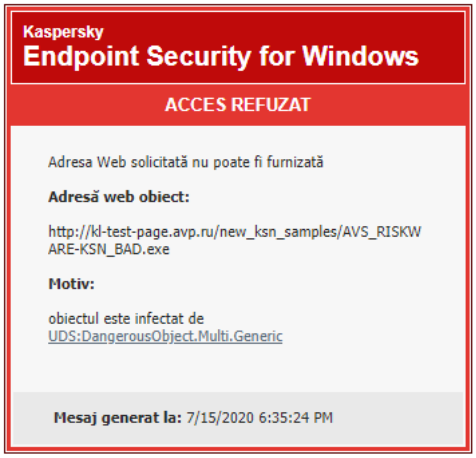
Web Threat Protection

Componenta Web Threat Protection previne descărcarea de pe Internet a fișierelor dăunătoare și, de asemenea, blochează site-urile web dăunătoare 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. Puteți specifica porturile pe care Kaspersky Endpoint Security le va monitoriza sau puteți selecta toate porturile.

Pentru monitorizarea traficului HTTPS, trebuie să activați scanarea conexiunilor securizate.

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 (vedeți figura de mai jos).



Mesaj privind respingerea accesului la site-ul web

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, Kaspersky Endpoint Security poate aplica diferite grupuri de setări. Aceste grupuri de setări care sunt stocate în aplicație sunt denumite *niveluri de securitate*: • **Ridicat**. Nivelul de securitate în care componenta Web Threat Protection efectuează un control maxim asupra scanării traficului Web primit de computer 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 Kaspersky Endpoint Security și securitatea traficului Web. Componenta Web Threat Protection efectuează analiza euristică la nivelul **Scanare normală**. 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 descărcarea**. 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. **Informare**. 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 URL în baza de date cu adrese URL 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.

(disponibil numai în Consola de administrare (MMC) și în interfața Kaspersky Endpoint Security)	
Utilizare 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. 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.
Verifică adresa URL în baza de date cu adrese URL 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 URL de încredere	Dacă această casetă de selectare este bifată, 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.

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 scanează, de asemenea, mesajele pentru detectarea link-urilor periculoase și de phishing. În mod implicit, componenta Mail Threat Protection își are originea permanent în memoria RAM a computerului și scanează toate mesajele primite sau trimise utilizând protocoalele POP3, SMTP, IMAP sau NNTP sau clientul de mail Microsoft Office Outlook (MAPI). Componenta oferă protecție computerului cu ajutorul bazelor de date antivirus, a serviciului cloud Kaspersky Security Network și a analizei euristice.

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 redenumește subiectul mesajului după cum urmează: `[Mesajul este infectat] <subiect mesaj>` sau `[Obiectul infectat a fost șters] <subiect mesaj>`.

Această componentă interacționează cu clienții de e-mail instalați pe computer. Pentru clientul de mail Microsoft Office Outlook, este furnizată o extensie cu parametri suplimentari. Extensia Mail Threat Protection este încorporată în clientul de e-mail Microsoft Office Outlook în cursul instalării aplicației Kaspersky Endpoint Security.

Setările componentei Mail Threat Protection

Parametru	Descriere
Nivel de securitate *(disponibil numai în Consola de administrare (MMC) și în interfața Kaspersky Endpoint Security)*	Pentru Mail 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 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 Kaspersky Endpoint Security 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 de securitate pentru e-mail **Redus** 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	**Dezinfectare; șterge dacă dezinfectarea nu reușește**. Când un obiect infectat este detectat într-un mesaj de intrare sau de ieșire, Kaspersky Endpoint Security încearcă să dezinfecteze obiectul detectat. Utilizatorul va putea accesa mesajul cu o atașare sigură. Dacă obiectul nu poate fi dezinfectat, Kaspersky Endpoint Security șterge obiectul infectat. Kaspersky Endpoint Security adaugă informații despre acțiunea efectuată la subiectul mesajului: `[Obiectul infectat a fost șters] <subiect mesaj>`.

	Dezinfectare; blocare dacă dezinfectarea nu reușește. Când un obiect infectat este detectat într-un mesaj de intrare, Kaspersky Endpoint Security încearcă să dezinfecteze obiectul detectat. Utilizatorul va putea accesa mesajul cu o atașare sigură. Dacă obiectul nu poate fi dezinfectat, Kaspersky Endpoint Security adaugă un avertisment la subiectul mesajului: `[Mesaj infectat] <subiect mesaj>`. Utilizatorul va putea accesa mesajul cu atașarea originală. Când un obiect infectat este detectat într-un mesaj de ieșire, Kaspersky Endpoint Security încearcă să dezinfecteze obiectul detectat. Dacă obiectul nu poate fi dezinfectat, Kaspersky Endpoint Security blochează transmiterea mesajului, iar clientul de e-mail afișează o eroare. **Blocare**. Dacă un obiect infectat este detectat într-un mesaj de intrare, Kaspersky Endpoint Security adaugă un avertisment la subiectul mesajului: `[Mesaj infectat] <subiect mesaj>`. Utilizatorul va putea accesa mesajul cu atașarea originală. Dacă un obiect infectat este detectat într-un mesaj de ieșire, Kaspersky Endpoint Security 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.
Scanare trafic POP3/SMTP/NNTP/IMAP	Această casetă de selectare activează/dezactivează scanarea de către componenta Mail Threat Protection a traficului transferat prin protocoalele POP3, SMTP, NNTP și IMAP.
Conectare extensie 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 Exchange în cache. 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.
Scanare arhive atașate	Scanează arhivele în următoarele formate: RAR, ARJ, ZIP, CAB, LHA, JAR, și ICE. Dacă în timpul scanării, Kaspersky Endpoint Security 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. Arhiva 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.

Scanare formate Office atașate	Scanează fișierele Microsoft Office (DOC, DOCX, XLS, PPT și alte extensii Microsoft). Fișierele în format Office includ și obiecte OLE.
Nu scana arhive mai mari de N MO	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.
Nu scana arhive mai mult de 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 atașare	Filtrarea atașărilor nu se aplică mesajelor de e-mail expediate. **Dezactivare filtrare**. Dacă este selectată această opțiune, componenta Mail Threat Protection nu filtrează fișierele atașate la mesaje de e-mail. **Redenumire tipuri de atașări 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. **Ștergere atașări 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 scanează traficul de rețea de la intrare, căutând activitate tipică atacurilor de rețea. Când Kaspersky Endpoint Security detectează o încercare de atac asupra rețelei pe computerul utilizatorului, acesta 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 Kaspersky Endpoint Security. 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
Detectare atacuri Scanare porturi și ISupraîncărcare 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. Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security monitorizează traficul de rețea pentru a detecta aceste atacuri. Când este detectat un atac, aplicația filtrează și blochează traficul asociat cu atacul. În acest fel, dacă un atac de tip Supraîncărcare rețea este lansat împotriva computerului, aplicația reduce încărcarea resursei atacate. Dacă un atac de tip Scanare port este lansat împotriva computerului, Kaspersky Endpoint Security previne sustragerea datelor din computer. 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.
Adăugare computer agresor la lista de computere blocate pentru N minute	Dacă această casetă de selectare este bifată, componenta Network Threat Protection adaugă computerul agresor 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. 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.
Excluderi	Lista conține adrese IP de la care componenta Network Threat Protection nu va bloca atacuri de rețea. Kaspersky Endpoint Security nu înregistrează în jurnal informații despre atacurile de rețea de la adrese IP care se găsesc în lista de excluderi.
Protecție împotriva falsificării 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

Firewall blochează conexiunile neautorizate la computer în timp ce lucrați pe Internet sau în rețeaua 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, consultați *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 rețea ale aplicației*. 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 din *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 puteți schimba grupul de încredere numai pentru 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 după cum urmează: o regulă de rețea pentru aplicații include reguli de acces bazate pe starea rețelei: *publică*, *locală* sau *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.

Stările conexiunii de rețea

Firewall-ul vă permite să controlați activitatea rețelei în funcție de starea conexiunii de rețea. Kaspersky Endpoint Security primește starea conexiunii de rețea de la sistemul de operare al computerului. Starea conexiunii de rețea în sistemul de operare este setată de utilizator atunci când configurează conexiunea. Puteți schimba starea conexiunii de rețea în setările Kaspersky Endpoint Security. Firewall-ul va monitoriza activitatea rețelei în funcție de starea rețelei în setările Kaspersky Endpoint Security și nu în sistemul de operare.

Conexiunea de rețea poate avea una dintre următoarele patru tipuri de stare:

- **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 starea *Rețea publică* întregului Internet. Nu poți modifica starea 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	Tabel cu o listă de reguli pentru pachetul de rețea. Regulile pentru pachete de rețea servesc

pentru pachetele de rețea	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.
Conexiuni rețea	Acest tabel conține informații despre conexiunile de rețea detectate de componenta Firewall pe computer. Starea *Rețea publică* este atribuită în mod implicit pentru Internet. Nu poți modifica starea pentru Internet.
Reguli rețea	**Anexe** 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 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 unei aplicații. 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 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 virtuală dacă este disponibilă (consultați figura de mai jos). Această procedură este cunoscută sub numele de Autorizare tastatură.

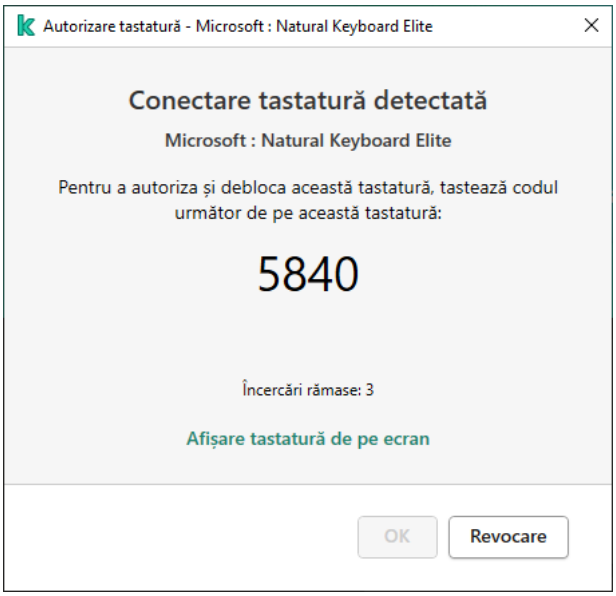
Dacă a fost introdus corect codul, aplicația salvează parametrii de identificare – VID/PID pentru tastatură și numărul portului la care a fost conectată – în lista de tastaturi autorizate. Autorizarea nu trebuie repetată atunci când tastatura este reconectată sau după repornirea sistemului de operare.

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. Sunt disponibile trei încercări pentru introducerea codului numeric. Dacă este introdus în mod incorect codul numeric de trei ori la rând sau dacă fereastra **<Nume tastatură> autorizare tastatură** este închisă, aplicația blochează introducerea de la această tastatură. Atunci când tastatura este reconectată 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

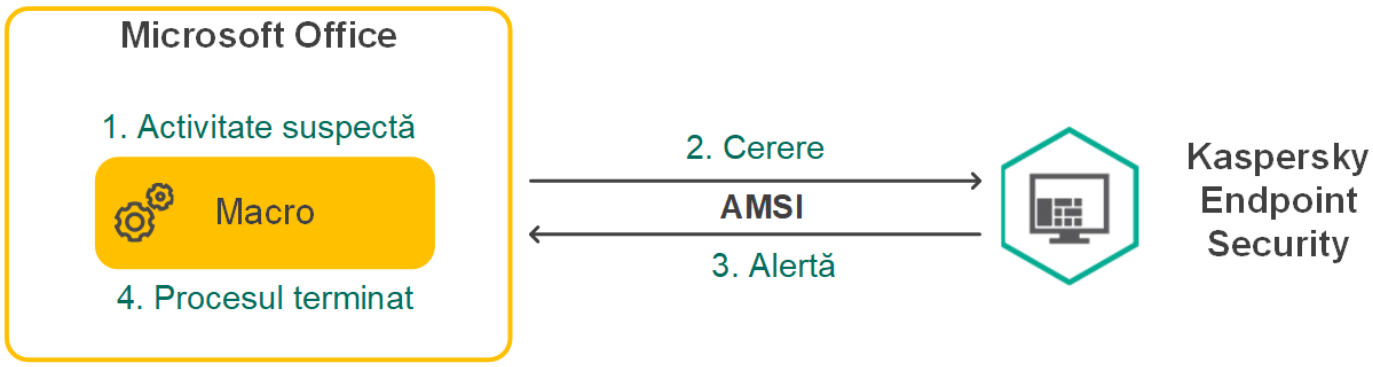
Setările componentei BadUSB Attack Prevention

Parametru	Descriere
Interzicere utilizare tastatură vizuală pentru autorizarea dispozitivelor USB	Dacă această casetă de selectare este bifată, aplicația blochează utilizarea tastaturii virtuale pentru autorizarea unui dispozitiv USB, de la care un cod de autorizare nu va mai putea fi introdus.

Protecție AMSI

Componenta Protecție AMSI are rol de suport pentru 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. Aplicația terță, după primirea unei notificări despre o amenințare, nu permite efectuarea de acțiuni rău intenționate (de exemplu, terminări).



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 Protecție AMSI nu refuză solicitări de la aplicațiile terțe pentru care caseta de selectare **Nu se blochează interacțiunea cu Furnizorul de protecție AMSI** este bifată

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;
- Windows Server 2016 Essentials/Standard/Datacenter;
- Windows Server 2019 Essentials/Standard/Datacenter.

Setările componentei Furnizor de protecție AMSI

Parametru	Descriere
Scanare arhive	Scanează arhivele în următoarele formate: RAR, ARJ, ZIP, CAB, LHA, JAR, și ICE.
Scanare pachete de distribuție	Această casetă de selectare activează/dezactivează scanarea pachetelor de distribuție terțe.
Scanare fișiere în formate Microsoft Office	Scanează fișierele Microsoft Office (DOC, DOCX, XLS, PPT și alte extensii Microsoft). Fișierele în format Office includ și obiecte OLE.
Nu dezarhiva fișiere 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 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 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.

Setările componentei Exploit Prevention

Parametru	Descriere
La detectarea exploatării	• **Blocare operațiune**. Dacă această opțiune este selectată, la detectarea unui exploit, Kaspersky Endpoint Security blochează acțiunile încercate de exploit. • **Informare**. Dacă această opțiune este selectată și este detectat un exploit, Kaspersky Endpoint Security nu blochează acțiunile exploitului, dar adaugă informațiile despre acest exploit în lista de amenințări 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. Pe baza semnăturilor de flux de comportamental, Kaspersky Endpoint Security oferă o apărare proactivă pentru computer.

Setările componentei Behavior Detection

Parametru	Descriere
La detectarea activității programelor malware	• **Ștergere fișier**. 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. • **Oprește forțat aplicația**. Dacă această opțiune este selectată, la detectarea unei activități rău intenționate Kaspersky Endpoint Security termină această aplicație. • **Informare**. 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.

Activează protecția directoarelor partajate împotriva criptării externe	În cazul în care caseta de selectare este bifată, Kaspersky Endpoint Security analizează activitatea în 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. • **Informare**. Dacă această opțiune este selectată, la detectarea unei încercări de modificare a fișierelor în directoarele partajate, Kaspersky Endpoint Security adaugă informații despre această încercare de modificare a fișierelor din directoarele partajate în lista de amenințări active. • **Blocare conexiune**. Dacă această opțiune este selectată, la detectarea unei încercări de modificare a fișierelor în directoarele partajate, Kaspersky Endpoint Security blochează activitatea de rețea care își are originea pe computerul care încearcă să modifice fișierele și creează copii de rezervă ale fișierelor modificate. Dacă este activată componenta Remediation Engine și este selectată opțiunea **Blocare conexiune**, Kaspersky Endpoint Security restaurează fișierele modificate din copiile de rezervă.
Blochează conexiunea pentru N minute	Perioada de timp pentru care Kaspersky Endpoint Security blochează activitatea de rețea a computerului la distanță care execută criptarea directoarelor partajate.
Excluderi	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*.

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 (cum ar fi fișiere și aplicații)

Activitatea de rețea a aplicațiilor este controlată de 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 din *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 puteți schimba grupul de încredere numai pentru 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 de aplicație	**Aplicații** 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 registru de sistem**. Acest tabel conține drepturile aplicațiilor din cadrul unui grup de încredere de a accesa resursele sistemului de operare și datele cu caracter personal.

	• **Drepturi**. Acest tabel conține drepturile aplicațiilor dintr-un grup de încredere de a accesa procesele și resursele sistemului de operare. • **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	**Nume** 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. **Aplicații** Tabelul aplicațiilor monitorizate de componenta Host Intrusion Prevention pentru resursa selectată. 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.
Grup de încredere pentru aplicațiile lansate înainte de pornirea Kaspersky Endpoint Security	Un grup de încredere în care Kaspersky Endpoint Security va plasa aplicațiile pornite înainte de Kaspersky Endpoint Security.
Reguli de actualizare pentru aplicații necunoscute anterior de la baza de date 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.
Încredere în aplicații cu semnătură digitală	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.
Ștergere drepturi pentru aplicațiile care nu sunt pornite mai mult de N zile	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 putut fi alocate 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 restaureze 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 registru**

  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 de 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 a acțiunilor unui malware poate fi pornită de componenta File Threat Protection sau Behavior Detection ori în cursul unei scanări de viruși.

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.

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 oferă Kaspersky Endpoint Security informații despre categoria și reputația fișierelor scanate, precum și informații despre reputația adreselor web scanate.

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.

Pentru a reduce încărcarea serverelor KSN, experții Kaspersky pot să lanseze actualizări ale aplicațiilor care dezactivează temporar sau restricționează parțial solicitările către Kaspersky Security Network. În acest caz, starea conexiunii la KSN în interfața locală a aplicației este *Activată cu restricții*.

Infrastructura KSN

Kaspersky Endpoint Security acceptă următoarele soluții de infrastructură KSN:

- *Global KSN* este soluția folosită de majoritatea aplicațiilor Kaspersky. Participanții KSN primesc informații de la Kaspersky Security Network și trimit informațiile Kaspersky despre obiecte detectate pe computerul utilizatorului pentru a fi analizate suplimentar de analiștii Kaspersky pentru a fi incluse în bazele de date privind reputația și în cele statistice ale Kaspersky Security Network.

- *Private KSN* este o soluție care permite utilizatorilor de computere care găzduiesc Kaspersky Endpoint Security sau alte aplicații Kaspersky să obțină acces la bazele de date de renume ale Kaspersky Security Network și la alte date statistice, fără a trimite date către KSN de la propriile lor computere. Private KSN 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.

În mod implicit, Kaspersky Security Center utilizează Global KSN. Puteți configura utilizarea tehnologiei Private KSN în Consola de administrare (MMC), în Kaspersky Security Center 12 Web Console și în linia de comandă. Nu este posibil să configurați utilizarea tehnologiei Private KSN în Kaspersky Security Center Cloud Console.

Pentru mai multe detalii despre Private KSN, consultați *documentația cu privire la Kaspersky Private Security Network*.

Proxy KSN

Computerele utilizatorilor administrate de Serverul de administrare Kaspersky Security Center pot interacționa cu KSN prin serviciul Proxy KSN.

Serviciul Proxy KSN oferă următoarele funcționalități:

- Computerul utilizatorului poate interoga KSN și poate trimite informații către KSN, chiar și fără acces direct la Internet.
- Serviciul Proxy KSN stochează în memoria cache datele procesate, reducând astfel încărcarea asupra canalului de comunicare în rețeaua externă și accelerând recepția informațiilor solicitate de computerul utilizatorului.

Pentru mai multe detalii despre serviciul KSN Proxy, consultați *Ghidul de ajutor pentru Kaspersky Security Center*.

Setări pentru Kaspersky Security Network

Parametru	Descriere
Activare mod 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.
Activare mod 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.
Utilizare 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.
Utilizare servere KSN atunci când serverul proxy KSN nu este disponibil *(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 Proxy KSN este indisponibil. Serverele KSN pot fi localizate atât la Kaspersky (atunci când se folosește Global KSN), cât și la terți (atunci când se folosește Private KSN).

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).

Kaspersky Endpoint Security monitorizează doar traficul HTTP- și HTTPS.

Pentru monitorizarea traficului HTTPS, trebuie să activați scanarea conexiunilor securizate.

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 sociale" sau la alte categorii.

- **Tipul de date**. Puteți restricționa accesul utilizatorilor la datele de pe un site web și puteți ascunde imaginile grafice, 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 „Fișiere grafice".

- **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, puteți restricționa accesul la tipul de date „Fișiere Office" doar pentru categoria de site-uri web „E-mail 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.

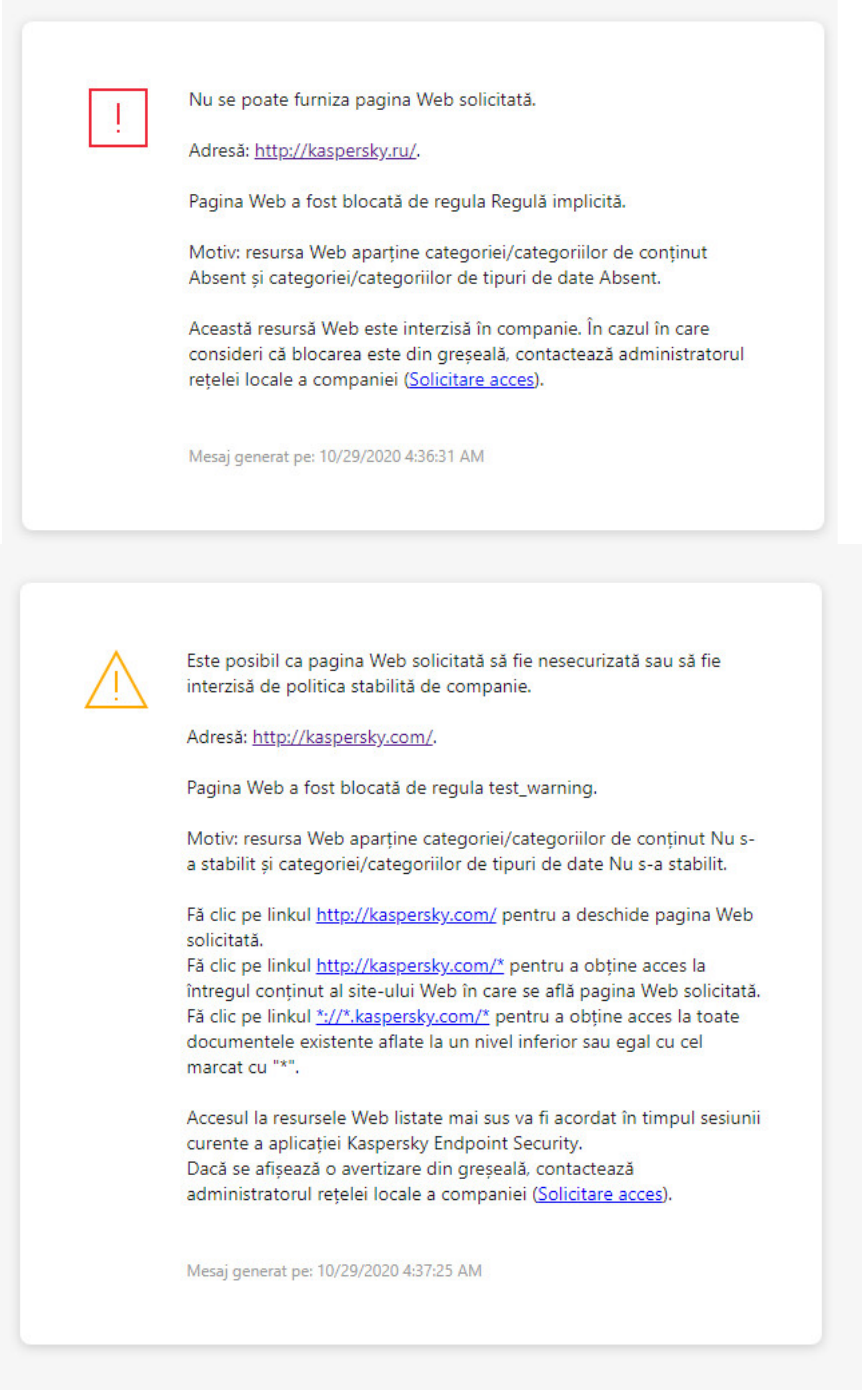
  De exemplu, puteți restricționa accesul la Internet printr-un browser pentru toți utilizatorii companiei, cu excepția departamentului IT.

- 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 sociale" 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

Setările 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.

Șabloane de mesaje	• **Avertizare**. 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 intrare conține șablonul mesajului care apare dacă se declanșează o regulă care blochează accesul la o resursă Web. • **Mesaj către administrator**. Câmpul de intrare conține șablonul de mesaj care va fi trimis administratorului rețelei LAN în cazul în care utilizatorul consideră că blocarea s-a făcut din greșeală.
Înscrierea în jurnal a deschiderii 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 . Monitorizarea activității pe Internet a utilizatorului poate necesita mai multe resurse ale computerului atunci când se decriptează traficul HTTPS.

Control dispozitive

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 dispozitive gestionează accesul utilizatorilor la dispozitivele instalate sau conectate la computer (de exemplu, hard diskuri, camere video sau module Wi-Fi). Acest lucru îți permite să protejezi computerul de infecții atunci când sunt conectate astfel de dispozitive și să împiedici pierderea sau scurgerea de date.

Nivelurile de acces ale dispozitivului

Componenta Control dispozitive controlează accesul la următoarele niveluri:

- **Tip dispozitiv**. De exemplu, imprimante, unități amovibile și unități CD/DVD.

  Poți configura accesul la dispozitive după cum urmează:

  - Permitere – .
  - Blocare – .
  - Depinde de magistrala de conectare (exceptând Wi-Fi) – .
  - Blocare cu excepții (numai Wi-Fi) – .

- **Magistrală de conectare**. O *magistrală de conectare* este o interfață utilizată pentru conectarea dispozitivelor la computer (de exemplu, USB sau FireWire). Prin urmare, poți restricționa conectarea tuturor dispozitivelor, de exemplu, prin USB.

  Poți configura accesul la dispozitive după cum urmează:

  - Permitere – ✓.
  - Blocare – ⊘.

- **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 de model**. 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.

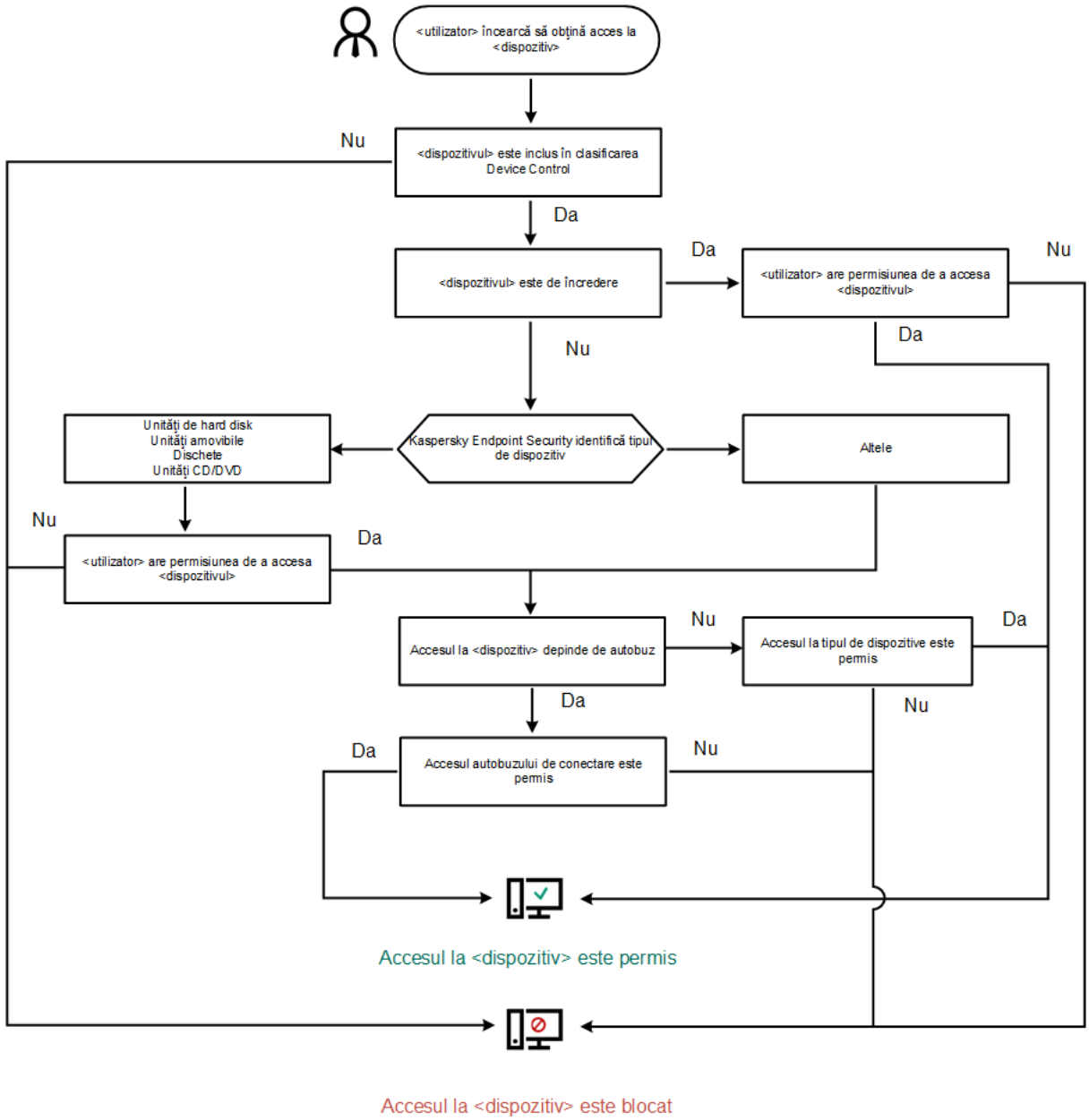
Dacă accesul la un dispozitiv depinde de magistrala de conectare (starea ◔), Kaspersky Endpoint Security nu salvează evenimente de conectare/deconectare a dispozitivului. Pentru a permite Kaspersky Endpoint Security să salveze evenimente de conectare/deconectare a dispozitivului, permite accesul la tipul 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.

Setările componentei Control dispozitive

Parametru	Descriere
Permitere solicitări de acces 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. Fă clic pe acest buton pentru a deschide fereastra **Solicitare acces la dispozitive**. În această fereastră 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.
Dispozitive de încredere	Lista dispozitivelor de încredere și a utilizatorilor cărora li se acordă acces la aceste dispozitive.
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.

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*), hash-ul de fișiere, vânzătorul aplicației 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.

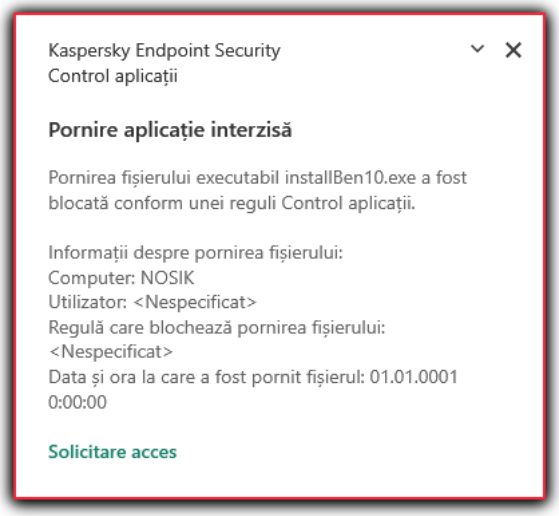
3. Selectarea modului Application Control.

   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.

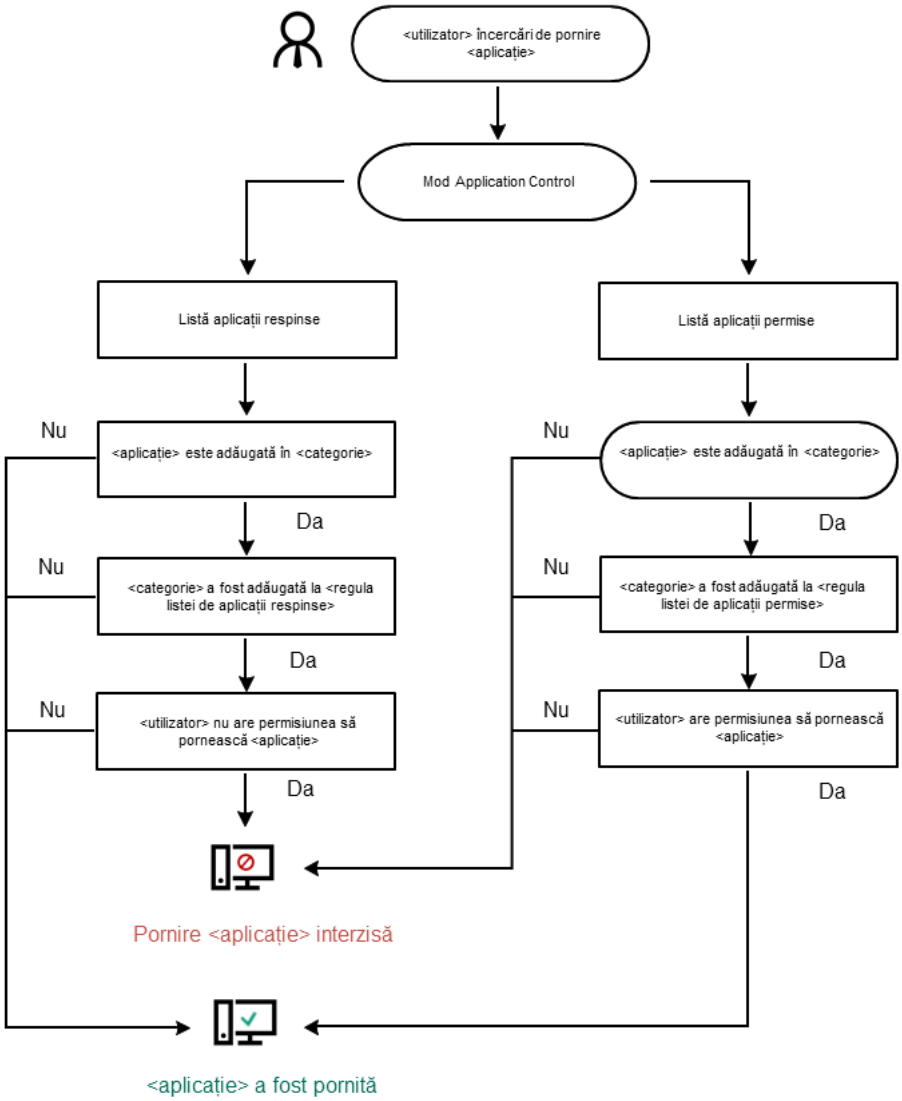
  Regulile Application Control create în Consola de administrare Kaspersky Security Center se bazează pe categorii tale particularizate de aplicații și nu pe condițiile de includere și de excludere, ca în cazul interfeței locale Kaspersky Endpoint Security.

- 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

Setările componentei Application Control

Parametru	Descriere
Mod testare	Dacă acest buton de comutare este pornit, Kaspersky Endpoint Security permite pornirea aplicației care este blocată în modul curent pentru Application Control, dar înregistrează informația despre pornirea sa în raport.
Mod Application Control	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 din 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 din 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.
Control 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 „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.
Șabloane de mesaje	**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.

Control anomalie adaptivă

Această componentă este disponibilă numai pentru Kaspersky Endpoint Security for Business Advanced și Kaspersky Total Security for Business. Pentru mai multe detalii despre Kaspersky Endpoint Security for Business, vizitați *site-ul web Kaspersky*.

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 necaracteristic (de exemplu, regula *Pornire Microsoft PowerShell din aplicația de birou*). 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 Raport declanșare regulă și în depozitul **Declanșarea regulilor în modul Instruire inteligentă**.

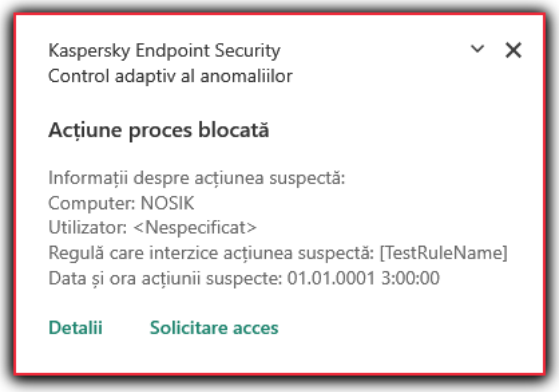
2. Analizarea raportului declanșării regulii.

   Administratorul analizează raportul declanșării regulii sau conținutul depozitului **Declanșarea regulilor în modul Instruire inteligentă**. 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. Componenta Control adaptiv al anomaliilor este configurată prin următoarele metode:

- Componenta Control adaptiv al anomaliilor începe automat să blocheze acțiunile asociate regulilor 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 de declanșare a regulilor și conținutul depozitului **Declanșarea regulilor în modul Instruire inteligentă**. Se recomandă analizarea raportului declanșării regulii sau conținutul depozitului **Declanșarea regulilor în modul Instruire inteligentă**.

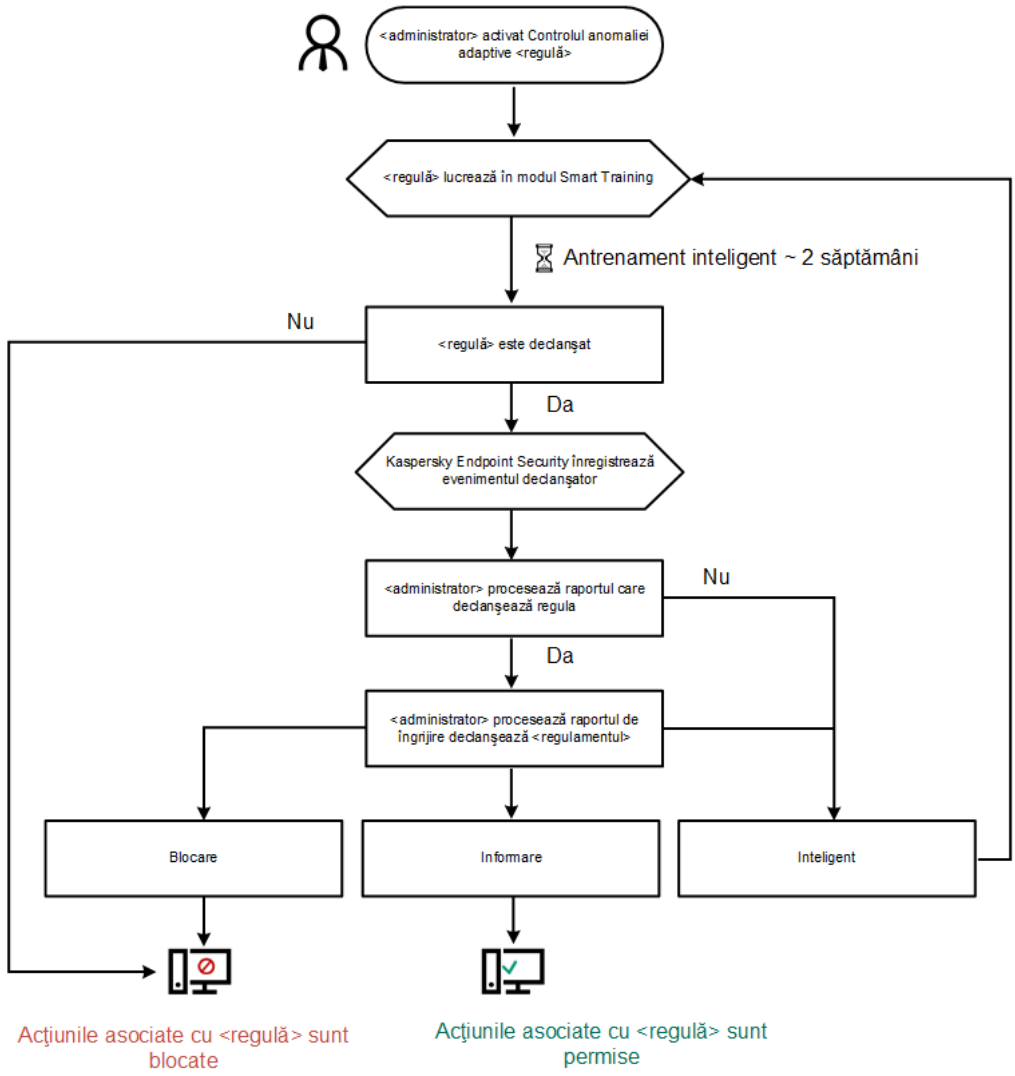
Când o aplicație periculoasă încearcă să efectueze o acțiune, Kaspersky Endpoint Security va bloca acțiunea și va afișa o notificare (consultați figura de mai jos).



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 stare reguli	Acest raport conține informații despre starea regulilor de detectare ale componentei Control adaptiv al anomaliilor (de exemplu, *Oprit* sau *Blocare*). Raportul se generează

(disponibil numai în consola Kaspersky Security Center)	pentru toate grupurile de administrare.
Raport declanșare regulă *(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.
Reguli	Tabel cu regulile componentei Control adaptiv al anomaliilor. Regulile sunt create de specialiștii Kaspersky pe baza scenariilor tipice de activitate potențial 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.

Senzor Endpoint

Componenta Senzor Endpoint nu este inclusă în Kaspersky Endpoint Security 11.4.0.

Puteți gestiona Senzorul Endpoint în Kaspersky Security Center 12 Web Console și în Consola de administrare Kaspersky Security Center. Nu este posibil să gestionați aplicația Senzor Endpoint în Kaspersky Security Center Cloud Console.

Senzor Endpoint 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 două blocuri funcționale: Kaspersky Anti Targeted Attack (denumit în continuare „*KATA*") și Kaspersky Endpoint Detection and Response (denumit în continuare „*KEDR*"). Puteți cumpăra KEDR separat. Pentru informații detaliate despre soluție. *consultați secțiunea Ajutor Kaspersky Anti Targeted Attack Platform* .

Gestionarea Senzorului Endpoint are următoarele limitări:

- Puteți configura setările Senzorului Endpoint 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 Senzorului Endpoint folosind 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 Senzorului Endpoint in politică.

Componenta Senzor Endpoint este instalată pe computere client. Pe aceste computere, componenta monitorizează constant procesele, conexiunile de rețea active și fișierele modificate. Senzorul Endpoint 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 Ghidul de ajutor pentru Kaspersky Anti Targeted Attack Platform*.

Full Disk Encryption

Poți selecta o tehnologie de criptare: Kaspersky Disk Encryption sau BitLocker Drive Encryption (denumită și „BitLocker").

Kaspersky Disk Encryption

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. Puteți utiliza, de asemenea, tehnologia Single Sign-On (SSO), care vă permite să vă conectați automat la sistemul de operare folosind numele de utilizator și parola din contul 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 vă permite să controlați și să gestionați Bitlocker folosind Kaspersky Security Center. BitLocker criptează volumele logice. BitLocker nu poate fi utilizat pentru criptarea unităților amovibile. Pentru detalii suplimentare despre BitLocker, consultați documentația Microsoft.

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 unei unități, BitLocker creează o cheie principală. Kaspersky Endpoint Security trimite cheia principală către Kaspersky Security Center pentru a putea restabili accesul la disc, de exemplu, dacă un utilizator a uitat parola.

Dacă un utilizator criptează un disc folosind BitLocker, Kaspersky Endpoint Security va trimite informații despre criptarea discului către Kaspersky Security Center. Cu toate acestea, Kaspersky Endpoint Security nu va trimite cheia principală către Kaspersky Security Center, astfel încât va fi imposibil să restaurați accesul la disc utilizând Kaspersky Security Center. Pentru ca BitLocker să funcționeze corect cu Kaspersky Security Center, decriptați unitatea și re-criptați-o folosind o politică. Puteți decripta o unitate local sau utilizând o politică.

După criptarea hard disk-ului sistemului, utilizatorul trebuie să parcurgă procesul de autentificarea BitLocker pentru a porni sistemul de operare. După procedura de autentificare, BitLocker va permite utilizatorilor să se conecteze. BitLocker nu acceptă tehnologia de conectare unică (SSO).

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 este selectat acest element, 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 hard disk**. Dacă este selectat acest element, 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 crearea contului Agent de Autentificare	**Toate conturile de pe computer**. Dacă această casetă de selectare este bifată, atunci când se execută activitatea Full Disk Encryption, Kaspersky Endpoint Security creează conturi de Agent de Autentificare pentru toate conturile de pe computer care au fost vreodată active. **Toate conturile de domeniu de pe computer**. Dacă această casetă de selectare este bifată, atunci când se execută activitatea Full Disk Encryption, Kaspersky Endpoint Security creează conturi de Agent de Autentificare pentru toate conturile de pe computer care aparțin unui anumit domeniu și care au fost vreodată active. **Toate conturile locale de pe computer**. Dacă această casetă de selectare este bifată, atunci când se execută activitatea Full Disk Encryption, Kaspersky Endpoint Security creează conturi de Agent de Autentificare pentru toate conturile locale de pe computer care au fost vreodată active. **Administrator local**. Dacă această casetă de selectare este bifată, atunci când se execută activitatea Full Disk Encryption, Kaspersky Endpoint Security creează un cont de administrator local. **Manager computer**. Dacă această casetă de selectare este bifată, atunci când se execută activitatea Full Disk Encryption, Kaspersky Endpoint Security creează un cont de Agent de Autentificare pentru contul ale cărui proprietăți în Active Directory arată că este un cont de gestionare. **Cont activ**. Dacă această casetă de selectare este bifată, atunci când se execută activitatea Full Disk Encryption, Kaspersky Endpoint Security creează un cont de Agent de Autentificare pentru contul de computer care este activ în cursul activității.
Creează automat conturi Agent de autentificare pentru to'i utilizatorii acestui computer dup[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.
Salvare 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.
Criptează doar spațiul de disc utilizat	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 **Criptare 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. Această casetă de selectare nu este bifată în mod implicit.
Utilizare Legacy USB Support	Această casetă de selectare activează/dezactivează funcția 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 simboluri 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. Puteți activa, de asemenea, utilizarea tehnologiei 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.
Texte pentru ajutor	**Autentificare**. Text pentru ajutor care apare în fereastra Agent de Autentificare atunci când introduceți acreditările contului. **Schimbare parolă** . 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 este selectat acest element, 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 hard disk**. Dacă este selectat acest element, 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 utilizarea autentificării BitLocker ce solicită intrarea de la tastatură înaintea preîncărcării sistemului pe tablete	Această casetă de selectare activează/dezactivează utilizarea autentificării 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. Se recomandă să folosești această setare 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	Dacă această casetă de selectare este bifată, aplicația folosește criptarea hardware. Acest lucru îți permite să sporești 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 **Criptare 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. Această casetă de selectare nu este bifată în mod implicit.
Setări autentificare	**Utilizează 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). **Utilizare 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. Puteți permite utilizatorului să utilizeze codul PIN îmbunătățit. *Codul PIN îmbunătățit* permite utilizarea altor caractere în plus față de caracterele numerice: majuscule și litere mici din alfabetul latin, caractere speciale și spații. • **Utilizare Trusted Platform Module (TPM); dacă este indisponibil, se utilizează parola**. Dacă această casetă de selectare este bifată, 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.

File Level Encryption

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.

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.

Setările componentei File Level Encryption

Parametru	Descriere
Gestionare criptare	**Lasă nemodificat**. Dacă este selectat acest element, Kaspersky Endpoint Security lasă fișierele și directoarele nemodificate, fără a le cripta sau a le decripta. **Criptare conform regulilor**. 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. **Decriptare toate**. Dacă este selectat acest element, Kaspersky Endpoint Security decriptează toate fișierele și directoarele criptate.
Reguli 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). • **Directoare**. 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. Puteți utiliza setul `\..\` (de exemplu, `C:\Users\..\UserFolder\`). Setul `\..\` denumește trecerea la directorul părinte. 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.
Reguli decriptare	Această filă prezintă regulile de decriptare pentru fișiere stocate pe unitățile locale.
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.
Setări parolă pachet criptat	Cerințe privind complexitatea parolei care trebuie îndeplinite la crearea pachetelor criptate.

Criptare unități amovibile

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

Criptarea setărilor componentelor unităților amovibile

Parametru	Descriere
Gestionare criptare	**Criptare 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. **Criptare 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. **Criptare 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. **Decriptare 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.

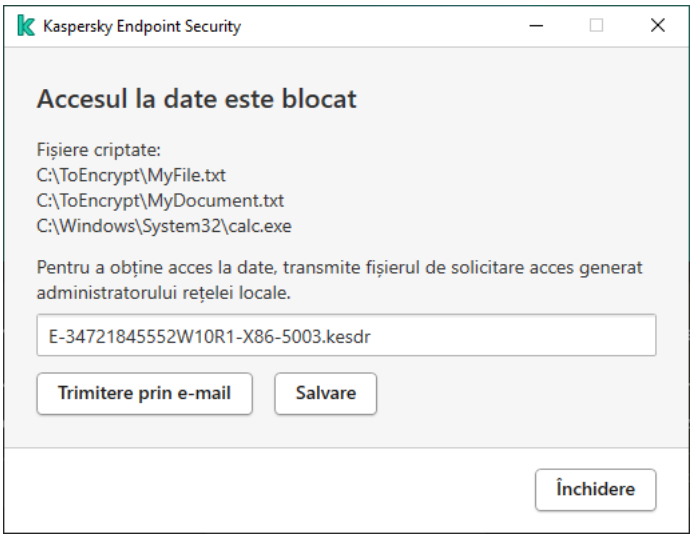
	Modul portabil este disponibil pentru modurile **Criptare toate fișierele** sau **Criptare numai fișiere noi**.
Criptează doar spațiul de disc utilizat	Această casetă de selectare activează/dezactivează modul de criptare în care sunt criptate numai sectoarele de disc ocupate. Acest mod este recomandat 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 **Criptare 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 de criptare pentru dispozitivele selectate	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 (ID hardware sau HWID)
	
	  • După modelul dispozitivului: ID-ul vânzătorului (VID) și ID-ul produsului (PID)

Permite 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 mod 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.
- **Mesaj**. 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.

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 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.

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.
- Activități de scanare.

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 scanează 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. Cu toate acestea, o aplicație care a fost adăugată la lista de aplicații de încredere este exclusă de la scanări de către Kaspersky Endpoint Security.

De exemplu, dacă presupui obiectele utilizate de aplicația Microsoft Windows Notepad standard ca fiind sigure fără scanare, ceea ce înseamnă că ai încredere în această aplicație, poți adăuga Microsoft Windows Notepad în lista de aplicații de încredere. Scanarea va omite atunci obiectele utilizate de această aplicație.

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.

Excluderea aplicațiilor de încredere din scanare permite evitarea conflictelor de compatibilitate dintre Kaspersky Endpoint Security și alte programe (de exemplu, problema scanării duble a traficului de rețea al unui computer terț de către Kaspersky Endpoint Security și de altă aplicație antivirus), crescând astfel performanțele computerului, aspect critic în cazul utilizării aplicațiilor server.

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 din 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. Ei pot determina pagube grave computerului. • Viruși și viermi

Subcategorie: viruși și viermi (Viruses_and_Worms)

Nivel amenințare: 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 cu *suprascriere* își scriu codul peste o parte din codul fișierului infectat, ștergând astfel o parte din conținutul fișierului. Fișierul infectat nu mai funcționează și nu poate fi restaurat. Virușii *paraziți* modifică fișiere, lăsându-le complet sau parțial funcționale. *Virușii de companie* 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.

Viermi

La fel ca un virus clasic, codul unui vierme se activează și efectuează acțiuni periculoase 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	Nume	Descriere
Viermi e-mail	Viermi 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	Clienți de IM	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 Internet	Se răspândesc prin camerele de 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.
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 de mai sus pentru a se răspândi (de exemplu, viermi care se răspândesc prin telefoane celulare).

- Troieni

Subcategoria: Troieni

Nivel amenințare: 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	Nume	Descriere
Troian-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 descriși în tabel. • **Troieni versatili**. Aceste programe au caracteristici avansate, tipice pentru anumite tipuri de troieni.
Trojan-	Troieni de	Ei țin „ostatice" informațiile utilizatorului,

Ransom	recompensă	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 clic	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.
Troian-program de descărcare	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. Intruși 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	Programele care sustrag parole sunt un tip de troieni care fură conturi de utilizator, de exemplu date de înregistrare software. Acești troieni

	sustragerii de parole	găsesc date confidențiale în fișierele de sistem și în registru și le trimit „stăpânului" 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	Ei fură acreditări de cont de la utilizatorii de jocuri online, după care trimit datele intrusului pe e-mail,

	informații de la utilizatorii de jocuri online	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. Intrușii pot trimite spam către adresele pe care le-au colectat.

- instrumente periculoase

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	Nume	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 cod de program care folosește vulnerabilități din aplicația 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 computere.
FileCryptor	Programe de	Ele criptează alte aplicații rău intenționate,

	criptare	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"	Ele trimit numeroase mesaje SMS către telefoane celulare.

	traficul cu mesaje SMS	

- Adware

  Subcategorie: software de advertising (Adware);

  Nivel amenințare: 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

Subcategorie: software legal care ar putea fi utilizat de infractori 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 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	Nume	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.
Dialer	Programe de apelare automată	Ei pot stabili conexiuni telefonice către un modem în mod ascuns.
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. Intruşii le instalează pe computerul utilizatorului pentru a trimite spam în numele utilizatorului.
Server-Telnet	Servere Telnet	Ele funcționează ca servere Telnet. Intruşii le instalează pe computerul utilizatorului pentru a deschide accesul la distanță prin Telnet.
Server-Web	Servere Web	Ele funcționează ca servere Web. Intruşii 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. Intruşii 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.

- Detectează alt software care poate fi utilizat de infractori pentru a aduce daune computerului sau datelor personale.

Subcategorie: software legal care ar putea fi utilizat de infractori 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 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	Nume	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.
Dialer	Programe de apelare automată	Ei pot stabili conexiuni telefonice către un modem în mod ascuns.
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. Intruşii le instalează pe computerul utilizatorului pentru a trimite spam în numele utilizatorului.
Server-Telnet	Servere Telnet	Ele funcționează ca servere Telnet. Intruşii le instalează pe computerul utilizatorului pentru a deschide accesul la distanță prin Telnet.
Server-Web	Servere Web	Ele funcționează ca servere Web. Intruşii 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. Intruşii 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 cod rău intenționat

Kaspersky Endpoint Security scanează obiecte comprimate și modulul de dezarhivare din arhive SFX (cu autoextragere).

Pentru a ascunde programe periculoase de aplicații antivirus, intrușii le arhivează folosind arhivatoare speciale sau creează fișiere împachetate multiplu.

Analiștii de viruși de la Kaspersky au identificat arhivatoarele care sunt cele mai populare în rândul hackerilor.

În cazul în care Kaspersky Endpoint Security detectează un astfel de arhivator într-un fișier, fișierul conține cel mai probabil o aplicație rău intenționată sau o aplicație care poate fi folosită de infractori pentru a dăuna computerului sau datelor personale.

Kaspersky Endpoint Security identifică următoarele tipuri de programe:

- *Fișiere împachetate care pot fi dăunătoare* – folosite pentru a ambala programe malware, cum ar fi viruși, viermi și troieni.
- *Fișiere împachetate multiplu* (nivel de amenințare mediu) – obiectul a fost arhivat de trei ori cu unul sau cu mai multe arhivatoare.

- **Fișiere împachetate multiplu**

Kaspersky Endpoint Security scanează obiecte comprimate și modulul de dezarhivare din arhive SFX (cu autoextragere).

Pentru a ascunde programe periculoase de aplicații antivirus, intrușii le arhivează folosind arhivatoare speciale sau creează fișiere împachetate multiplu.

Analiștii de viruși de la Kaspersky au identificat arhivatoarele care sunt cele mai populare în rândul hackerilor.

În cazul în care Kaspersky Endpoint Security detectează un astfel de arhivator într-un fișier, fișierul conține cel mai probabil o aplicație rău intenționată sau o aplicație care poate fi folosită de infractori pentru a dăuna computerului sau datelor personale.

Kaspersky Endpoint Security identifică următoarele tipuri de programe:

- *Fișiere împachetate care pot fi dăunătoare* – folosite pentru a ambala programe malware, cum ar fi viruși, viermi și troieni.
- *Fișiere împachetate multiplu* (nivel de amenințare mediu) – obiectul a fost arhivat de trei ori cu unul sau cu mai multe arhivatoare.

Excluderi

Acest tabel conține informații despre excluderile de la scanare.

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 din directorul denumit `Folder` și din subdirectoarele sale. Masca trebuie să includă cel puțin un nivel de imbricare. Masca `C:\**\*.txt` nu este o mască validă. • Caracterul `?` (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. • 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.
Aplicații de încredere	Acest tabel listează aplicațiile de încredere a căror activitate nu este monitorizată de Kaspersky Endpoint Security în cursul funcționării sale. Componenta Application Control monitorizează pornirea fiecărei aplicații, indiferent dacă aplicația este inclusă sau nu în tabelul de aplicații de încredere.
Îmbinare valori 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.
Permite utilizarea excluderilor locale / Permite utilizarea aplicațiilor de încredere locale	*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.

(disponibil numai în consola Kaspersky Security Center)	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. Dacă au fost generate liste locale, după ce această funcționalitate este dezactivată, Kaspersky Endpoint Security continuă să excludă obiectele listate din scanări.
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

Setări aplicație

Parametru	Descriere
Pornire Kaspersky Endpoint Security la pornirea computerului	Atunci când caseta de selectare este bifată, Kaspersky Endpoint Security este pornit după încărcarea sistemului de operare, protejând computerul pe parcursul întregii sesiuni. Atunci când caseta de selectare 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.
Activare tehnologie dezinfectare avansată	Dacă această casetă de selectare este bifată, apare pe ecran o notificare pop-up atunci când în sistemul de operare este detectată activitate rău intenționată. În notificarea sa, Kaspersky Endpoint Security oferă utilizatorului posibilitatea să efectueze dezinfectarea avansată a computerului. După ce utilizatorul aprobă această procedură, Kaspersky Endpoint Security neutralizează amenințarea. După finalizarea procedurii de dezinfectare avansată, Kaspersky Endpoint Security repornește computerul. Tehnologia de dezinfectare avansată folosește resurse de calcul considerabile, care port încetini alte aplicații.

	Dacă Kaspersky Endpoint Security este instalat pe un computer care rulează Windows Server, Kaspersky Endpoint Security nu va afișa notificarea. Prin urmare, utilizatorul nu poate selecta o activitate pentru a îndepărta o amenințare activă. Pentru a îndepărta o amenințare, este necesar să activați tehnologia Dezinfectare avansată în setările aplicației și să rulați imediat Dezinfectarea avansată din proprietățile activității *Scanare de viruși*. Apoi, este necesar să porniți activitatea *Scanare de viruși*.
Utilizare Kaspersky Security Center ca server proxy pentru activare *(disponibil numai în consola Kaspersky Security Center)*	Dacă această casetă de selectare este bifată, Serverul de administrare Kaspersky Security Center este folosit ca server proxy la activarea aplicației.
Activare Autoprotecție	Când această casetă de selectare este bifată, Kaspersky Endpoint Security previne alterarea sau ștergerea fișierelor aplicației de pe unitatea de hard disk, a proceselor de memorie și a înregistrărilor din registrul de sistem.
Permite gestionarea setărilor Kaspersky Endpoint Security prin aplicații de control de la distanță	Dacă este bifată caseta de selectare, aplicațiile de gestionare la distanță de încredere (cum ar fi TeamViewer, LogMeIn Pro și Remotely Anywhere) pot modifica setările Kaspersky Endpoint Security. Aplicațiilor de administrare la distanță de încredere li se interzice modificarea setărilor Kaspersky Endpoint Security chiar și atunci când este bifată caseta de selectare.
Activare control serviciu extern	Dacă este bifată caseta de selectare, Kaspersky Endpoint Security permite gestionarea serviciilor aplicației de pe un computer la distanță. Atunci când apare o încercare de a gestiona serviciile aplicației de la distanță, 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).
Amână activități planificate la funcționarea cu alimentare de la baterie	Dacă această casetă de selectare este bifată, modul Conservare energie este dezactivat. Kaspersky Endpoint Security amână activitățile planificate. Dacă este necesar, poți porni manual activități de scanare și de actualizare.
Cedare resurse pentru alte aplicații	Atunci când Kaspersky Endpoint Security execută activități planificate, aceasta poate genera o încărcare sporită pentru procesor și pentru subsistemele unității de disc, ceea ce reduce performanțele altor aplicații. Atunci când caseta de selectare este bifată, Kaspersky Endpoint Security suspendă activitățile planificate atunci când detectează o încărcare sporită și eliberează resurse ale sistemului de operare pentru aplicațiile utilizatorului.
Activare scriere	Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security scrie imagini atunci când se blochează.

imagine	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.
Activare protecție fișiere 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 stările *OK*, *Avertizare* și *Critic* .

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\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\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.

Setări pentru rapoarte și zone de stocare

Parametru	Descriere
Stocare	În cazul în care caseta de selectare este bifată, termenul maxim de stocare a raportului este

rapoarte nu mai mult de N zile	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.
Limitare dimensiune fișier raport la N MB	În cazul în care caseta de selectare este bifată, dimensiunea maximă a fișierului 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.
Stocare obiecte nu mai mult de N zile	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.
Limitați dimensiunea Copiei de rezervă la N 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 100 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.
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.

Setări de rețea

Puteți configura serverul proxy utilizat pentru conectarea la Internet și actualizarea bazelor de date antivirus, puteți selecta modul de monitorizare a portului de rețea și configura scanarea conexiunilor securizate.

Opțiuni rețea

Parametru	Descriere
Limitare trafic 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.
Server	Setările serverului proxy utilizat pentru accesul la Internet al utilizatorilor de computere

proxy	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, Kaspersky Endpoint Security utilizează adresa serverului proxy specificată în setările browserului Microsoft Internet Explorer.
Se 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.
Porturi monitorizate	**Monitorizare toate porturile de rețea**. În acest mod de monitorizare a porturilor de rețea, componentele protecției (File Threat Protection, Web Threat Protection, Mail Threat Protection) monitorizează fluxurile de date transmise prin orice porturi de rețea deschise pe computer. **Monitorizare numai porturi 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. **Monitorizare 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. **Monitorizare toate porturile pentru aplicații specificate**. În acest caz este utilizată o listă de aplicații ale căror porturi de rețea sunt monitorizate de Kaspersky Endpoint Security.
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 se scanează conexiunile criptate** Kaspersky Endpoint Security nu va avea acces la conținutul site-urilor web ale căror adrese încep cu `https://`. • **Se scanează conexiunile criptate la cererea componentelor de protecție**. Kaspersky Endpoint Security va scana traficul criptat numai la solicitarea componentelor File Threat Protection, Mail Threat Protection și Control web. • **Se 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.
La vizitarea unui domeniu cu un certificat care nu este de încredere	• **Permitere**. Dacă este selectată această opțiune, atunci când se vizitează un domeniu cu un certificat neautorizat, 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. 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. • **Blocare conexiune**. Dacă este selectată această opțiune, atunci când se vizitează un domeniu cu un certificat neautorizat, Kaspersky Endpoint Security permite 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.
Când apar erori la scanarea conexiunilor criptate	• **Blocare conexiune**. Dacă acest element este selectat, atunci când apare o eroare la scanare în cadrul unei conexiuni criptate, Kaspersky Endpoint Security blochează conexiunea la rețea. • **Adăugare domeniu la excluderi**. Dacă acest element este selectat, atunci când apare o eroare la scanare în cadrul unei conexiuni 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 **Blocare conexiune**.
Blocare conexiuni SSL 2.0	Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security blochează conexiunile la rețea stabilite prin protocolul SSL 2.0. Dacă această casetă de selectare nu este bifată, Kaspersky Endpoint Security nu blochează conexiunile la rețea stabilite prin protocolul SSL 2.0 și nu monitorizează traficul de rețea transmis prin aceste conexiuni.
Decriptarea conexiunilor criptate cu site-urile web care utilizează certificate EV	Certificatele EV (certificate cu validare extinsă) 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, Kaspersky Endpoint Security decriptează și monitorizează conexiunile criptate cu site-uri web care utilizează un certificat EV. În cazul în care caseta de selectare este debifată, Kaspersky Endpoint Security nu are acces la conținutul traficului HTTPS. Din acest motiv, aplicația monitorizează traficul HTTPS doar pe baza adresei site-ului web, de exemplu, `https://facebook.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.
Adrese de încredere	În acest caz este utilizată o listă de adrese web pentru care Kaspersky Endpoint Security nu scanează conexiunile la rețea. Puteți introduce numele unui domeniu sau adresa IP. Kaspersky Endpoint Security acceptă caracterul `*` când introduceți masca unui nume de domeniu. Kaspersky Endpoint Security nu acceptă măști pentru adresele IP. Exemple: • `domain.com` – această intrare include următoarele adrese: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Această intrare include subdomenii (de exemplu, `subdomain.domain.com`). • `subdomain.domain.com` – această intrare include următoarele subdomenii: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Intrarea include domeniul `domain.com`. • `*.domain.com` – această intrare include următoarele adrese: `https://movies.domain.com`, `https://images.domain.com/page123`. Intrarea include domeniul `domain.com`.
Aplicații 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.
Scanează traficul sigur în aplicațiile Mozilla *(disponibil numai în interfața Kaspersky Endpoint Security)*	Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security 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, Kaspersky Endpoint Security nu scanează traficul din browserul Mozilla Firefox și clientul de e-mail Thunderbird. Kaspersky Endpoint Security folosește certificatul rădăcină Kaspersky pentru a decripta și analiza traficul criptat. Puteți selecta depozitul de certificate care va conține certificatul rădăcină Kaspersky. • **Utilizează depozitul de certificate Windows**. Certificatul rădăcină Kaspersky este adăugat la acest depozit în timpul instalării Kaspersky Endpoint Security. • **Utilizează depozitul de certificate Mozilla**. 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.

Setări interfață

Parametru	Descriere
Interacțiune cu utilizatorul *(disponibil numai în consola Kaspersky Security Center)*	**Cu 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, notificări deasupra pictogramei aplicației. **Cu interfață completă**. 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. **Fără interfață**. Pe un computer client, nu sunt afișate semne de funcționare a Kaspersky Endpoint Security. Pictograma din zona de notificare Windows și notificările sunt disponibile.
Setări notificări	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.
Setări notificare e-mail	Setări ale serverului SMTP pentru livrarea notificărilor despre evenimentele înregistrate în timpul funcționării aplicației.
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 stare bază de date antivirus locală	Setările pentru notificări despre baze de date antivirus învechite și utilizate de către aplicație.
Protecția 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 vă solicită să setați o parolă pentru efectuarea operațiunilor.
Resurse Web pentru asistență tehnică *(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 **Asistență** a interfeței locale a aplicației Kaspersky Endpoint Security în locul linkurilor standard.
Mesaj către utilizator	Mesaj care este afișat în fereastra **Asistență** a interfeței locale a Kaspersky Endpoint Security.

(disponibil numai în consola Kaspersky Security Center)	

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 12 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
Import	Extrageți setările aplicației dintr-un fișier în format CFG și le aplicați.
Export	Salvați setările curente ale aplicației într-un fișier în format CFG.
Restaurare	Puteți restaura oricând setările recomandate de Kaspersky for Endpoint Security. Când setările sunt restabilite, nivelul de securitate **Recomandat** este setat pentru toate componentele de protecție.

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*.

Setări pentru Gestionare activități

Parametru	Descriere
Permite utilizarea activităților locale	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 rîmâne 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 de viruși a unui fișier sau director selectând opțiunea **Scanare de viruși** în meniul contextual al fișierului sau directorului respectiv. Activitatea de scanare este pornită cu valorile implicite pentru activitatea de scanare particularizată.
Permite afișarea activităților de grup	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.
Permitere gestionare activități de grup	În cazul în care caseta de selectare este bifată, utilizatorii pot porni și opri activitățile de grup specificate în 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 Kaspersky Security Center.

Scanarea computerului

O scanare de viruși este esențială pentru securitatea computerului. Scanările de viruși executate regulat contribuie la eliminarea posibilității 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:

- Memorie 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 executarea 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 particularizată

Kaspersky Endpoint Security scanează obiectele selectate de utilizator. Poți scana orice obiect din următoarea listă:

- Memorie kernel
- Obiectele încărcate la pornirea sistemului de operare
- Crearea unei copii de rezervă a sistemului de operare
- Cutia poștală Microsoft Outlook
- Unități de hard disk, amovibile și de rețea
- Orice fișier selectat

Scanare în fundal

Scanare în fundal este un mod 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

Kaspersky Endpoint Security verifică modulele aplicației pentru a vedea dacă sunt deteriorate sau modificate.

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, Kaspersky Endpoint Security scanează și fișierele multi-format.

	• **Recomandat**. Kaspersky Endpoint Security scanează numai formatele de fișiere specificate de pe toate unitățile de hard disk, de pe toate unitățile de rețea și de pe toate suporturile de stocare amovibile ale computerului, dar și de pe obiecte OLE încorporate. Kaspersky Endpoint Security nu scanează arhivele și pachetele de instalare. • **Redus**. Kaspersky Endpoint Security scanează numai fișierele noi sau modificate, cu extensii specificate de pe toate unitățile de hard disk, unitățile amovibile și unitățile de rețea ale computerului. Kaspersky Endpoint Security nu scanează fișierele compuse.
Acțiune la detectarea amenințării	**Dezinfectare; șterge dacă dezinfectarea nu reușește**. Dacă selectați această opțiune, Kaspersky Endpoint Security încearcă automat să dezinfecteze toate fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, Kaspersky Endpoint Security șterge fișierele. **Dezinfectare. Blochează dacă dezinfectarea nu reușește**. Dacă selectați această opțiune, Kaspersky Endpoint Security încearcă automat să dezinfecteze toate fișierele infectate care sunt detectate. Dacă nu este posibilă dezinfectarea, Kaspersky Endpoint Security adaugă informațiile despre fișierele infectate detectate în lista de amenințări active. **Informare**. 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, Kaspersky Endpoint Security creează o copie de rezervă a fișierului în cazul în care trebuie să restaurați fișierul sau dacă acesta poate fi dezinfectat în viitor.
Domeniu de protecție	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, bazele de date de e-mail, hard diskul, unitatea amovibilă sau unitatea, directorul sau fișierul de rețea.
Planificare scanare	**Manual**. Modul de executare în care puteți porni scanarea manuală la un moment în care vă este convenabil. **Programată**. În acest mod de executare a activității de scanare, Kaspersky Endpoint Security 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.
Executare activități omise *(disponibil numai în consola Kaspersky Security Center)*	Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security pornește activitatea de scanare omisă imediat ce acest lucru devine posibil. Activitatea de scanare poate fi omisă, de exemplu, dacă computerul a fost oprit la ora programată a activității de scanare. Dacă această casetă de selectare este nebifată, Kaspersky Endpoint Security nu execută activitățile de scanare omise. În schimb, aplicația execută următoarea activitate de scanare în conformitate cu planificarea curentă.
Execută doar atunci când computerul este inactiv	Amânarea începerii activității de scanare atunci când resursele computerului sunt ocupate. Kaspersky Endpoint Security pornește activitatea de scanare dacă computerul este blocat sau dacă economizorul de ecran este pornit.
Executare scanare 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 Kaspersky Endpoint Security și puteți rula activitatea de scanare în contul acestui utilizator.
Tipuri de fișiere	Kaspersky Endpoint Security consideră fișierele fără extensie ca fiind fișiere executabile. Kaspersky Endpoint Security 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, Kaspersky Endpoint Security 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, Kaspersky Endpoint Security scanează numai fișierele infectabile. Formatul fișierului se determină în funcție de extensia sa.
Scanare 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.
Omitere fișiere scanate mai mult de N secunde	Limitează durata scanării unui singur obiect. După scurgerea duratei specificate, Kaspersky Endpoint Security oprește scanarea fișierului. Acest lucru reduce durata unei scanări.
Scanare arhive	Scanează arhivele în următoarele formate: RAR, ARJ, ZIP, CAB, LHA, JAR, și ICE.
Scanare pachete de distribuție	Această casetă de selectare activează/dezactivează scanarea pachetelor de distribuție terțe.
Scanare fișiere în formate Microsoft Office	Scanează fișierele Microsoft Office (DOC, DOCX, XLS, PPT și alte extensii Microsoft). Fișierele în format Office includ și obiecte OLE.
Scanare formate de e-mail	Această casetă activează/dezactivează în Kaspersky Endpoint Security opțiunea de scanare a fișierelor în formate de e-mail și a bazelor de date de e-mail. Aplicația scanează complet numai formatele de fișiere e-mail Microsoft Outlook, Windows Mail/Microsoft Outlook Express și EML și numai dacă computerul are clientul de e-mail Microsoft Outlook x86. 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.
Scanare arhive	Dacă este bifată caseta de selectare, Kaspersky Endpoint Security scanează arhivele protejate prin parolă. Pentru ca fișierele dintr-o arhivă să fie scanate, ți se solicită să introduci parola.

protejate prin parolă	În cazul în care caseta de selectare este debifată, Kaspersky Endpoint Security omite scanarea arhivelor protejate prin parolă.
Nu dezarhiva fișiere 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 mari extrase din arhive, indiferent dacă această casetă de selectare este bifată sau nu.
Tehnologia Machine 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.
Tehnologie iSwift	Această tehnologie permite creșterea vitezei de scanare excluzând de la scanare anumite fișiere. Fișierele sunt excluse de la scanare 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.
Tehnologie 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).

Scanare în fundal

Scanare în fundal este un mod 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. 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.

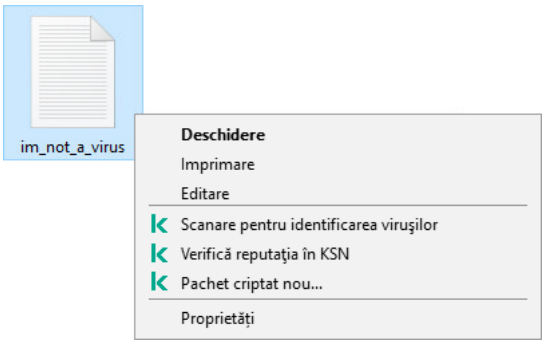
- Computerul (laptopul) a trecut la modul baterie.

Când se execută scanarea în fundal, Kaspersky Endpoint Security nu scanează fișiere al căror conținut este localizat în spațiul de stocare în cloud OneDrive.

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

Setările activității Scanare din Meniu contextual

Parametru	Descriere
Acțiune la detectarea amenințării	**Dezinfectare; șterge dacă dezinfectarea nu reușește**. Dacă selectați această opțiune, Kaspersky Endpoint Security încearcă automat să dezinfecteze toate fișierele infectate care sunt detectate. Dacă dezinfectarea nu reușește, Kaspersky Endpoint Security șterge fișierele. **Dezinfectare. Blochează dacă dezinfectarea nu reușește**. Dacă selectați această opțiune, Kaspersky Endpoint Security încearcă automat să dezinfecteze toate fișierele infectate care sunt detectate. Dacă nu este posibilă dezinfectarea, Kaspersky Endpoint Security adaugă informațiile despre fișierele infectate detectate în lista de amenințări active. **Informare**. Dacă este selectată această opțiune, Kaspersky Endpoint Security adaugă informațiile despre fișierele infectate în lista de amenințări active la detectarea acestor fișiere.
Scanare numai fișiere	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.

noi și modificate	
Omite fișierele scanate mai mult de N s	Limitează durata scanării unui singur obiect. După scurgerea duratei specificate, Kaspersky Endpoint Security oprește scanarea fișierului. Acest lucru reduce durata unei scanări.
Scanare arhive	Scanează arhivele în următoarele formate: RAR, ARJ, ZIP, CAB, LHA, JAR, și ICE.
Scanare pachete de distribuție	Această casetă de selectare activează/dezactivează scanarea pachetelor de distribuție.
Scanare fișiere în formate Microsoft Office	Scanează fișierele Microsoft Office (DOC, DOCX, XLS, PPT și alte extensii Microsoft). Fișierele în format Office includ și obiecte OLE.
Nu dezarhiva fișiere compuse mari	Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security nu scanează fișierele compuse a căror dimensiune depășește valoarea specificată.
Tehnologia Machine 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.
Tehnologie iSwift	Această tehnologie permite creșterea vitezei de scanare excluzând de la scanare anumite fișiere. Fișierele sunt excluse de la scanare 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.
Tehnologie 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).

Scanare unități amovibile

Kaspersky Endpoint Security permite scanarea unităților amovibile conectate al computer pentru detectarea virușilor și a altor programe malware.

Setări pentru activitatea Scanare unități amovibile

Parametru	Descriere
Acțiune la conectarea unei unități amovibile	• **Nu scana**. • **Scanare detaliată** Dacă această opțiune este selectată, atunci când o unitate amovibilă este conectată, Kaspersky Endpoint Security va scana toate fișierele aflate pe unitatea amovibilă, inclusiv fișierele din obiectele compuse. • **Scanare rapidă** Dacă această opțiune este selectată, atunci când o unitate amovibilă este conectată, Kaspersky Endpoint Security va scana numai fișierele cu anumite formate care sunt cele mai vulnerabile să fie infectate și nu va dezarhiva obiectele compuse.
Dimensiune maximă unitate amovibilă	Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security execută acțiunea selectată în lista verticală **Acțiune la conectarea unei unități amovibile** pentru unitățile amovibile cu o dimensiune mai mică decât dimensiunea maximă specificată a unității. Dacă nu este bifată caseta de selectare, Kaspersky Endpoint Security execută acțiunea selectată în lista verticală **Acțiune la conectarea unei unități amovibile** pentru toate unitățile, indiferent de dimensiune.
Afișare progres scanare	Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security afișează progresul scanării unităților amovibile într-o fereastră separată și în fereastra **Activități**. Dacă această casetă de selectare este debifată, Kaspersky Endpoint Security începe în fundal scanarea unităților amovibile.
Blochează oprirea activității de scanare	Dacă este bifată caseta de selectare, butonul **Oprire** din fereastra **Activități** și butonul **Oprire** din fereastra **Scanare de viruși** sunt indisponibile în interfața locală Kaspersky Endpoint Security.

Verificare integritate

Kaspersky Endpoint Security verifică fișierele aplicației din directorul de instalare a 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* este destinată scanării fișierelor aplicațiilor. Executați activitatea *Verificare integritate* dacă Kaspersky Endpoint Security a detectat un obiect rău intenționat, dar nu l-a neutralizat.

Puteți crea activitatea *Verificare integritate* atât în Kaspersky Security Center 12 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.

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. **Programată**. În acest mod de executare a activității de scanare, Kaspersky Endpoint Security 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.
Executare activități omise	Dacă această casetă de selectare este bifată, Kaspersky Endpoint Security pornește activitatea de scanare omisă imediat ce acest lucru devine posibil. Activitatea de scanare poate fi omisă, de exemplu, dacă computerul a fost oprit la ora programată a activității de scanare. Dacă această casetă de selectare este nebifată, Kaspersky Endpoint Security nu execută activitățile de scanare omise. În schimb, aplicația execută următoarea activitate de scanare în conformitate cu planificarea curentă.
Execută doar atunci când computerul este inactiv	Amânarea începerii activității de scanare atunci când resursele computerului sunt ocupate. Kaspersky Endpoint Security pornește activitatea de scanare dacă computerul este blocat sau dacă economizorul de ecran este pornit.
Executare ca *(disponibil numai în consola Kaspersky Security Center)*	În mod implicit, activitatea de scanare este executată în numele utilizatorului cu drepturile căruia sunteți înregistrat în sistemul de operare. Pot fi necesare permisiuni speciale pentru accesarea directorului de instalare a aplicației. Puteți specifica un utilizator care are drepturile solicitate în setările Kaspersky Endpoint Security și puteți rula activitatea de scanare în contul acestui utilizator.

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.

Actualizările regulate necesită o licență activă. Dacă nu există nicio licență curentă, vei avea posibilitatea să efectuezi doar o singură actualizare.

Sursa principală de actualizare a aplicației Kaspersky Endpoint Security o reprezintă serverele de actualizare Kaspersky.

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.

Fișierele de ajutor contextual pentru aplicație pot fi actualizate odată cu actualizările modulelor aplicației.

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 secțiunea **Actualizare** din fereastra **Activități**.

Informațiile despre rezultatele actualizărilor și despre toate evenimentele care apar în timpul funcționării activității de actualizare sunt înregistrate în Raportul Kaspersky Endpoint Security.

Modulul aplicației și setările de actualizare a bazei de date

Parametru	Descriere
Mod executare	**Automat**. În acest mod, Kaspersky Endpoint Security 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. **Manual**. Acest mod de executare a activității de actualizare vă permite să porniți manual activitatea de actualizare. **Programată**. 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.
Executare activități omise	Dacă este bifată caseta de selectare, Kaspersky Endpoint Security pornește activitatea de actualizare omisă de îndată ce acest lucru devine posibil. Activitatea de actualizare poate fi omisă, de exemplu, dacă computerul a fost oprit la ora de începere a activității de actualizare.

	În cazul în care caseta de selectare este nebifată, Kaspersky Endpoint Security nu începe activități de actualizare omise. În schimb, rulează următoarea activitate de actualizare în conformitate cu programul curent.
Sursă 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. Lista implicită de surse de actualizare include Kaspersky Security Center și servere de actualizare ale Kaspersky. Poți adăuga la listă alte surse de actualizare. Poți 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.
Executare activitate 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 Kaspersky Endpoint Security, poți specifica un utilizator care are astfel de drepturi și poți porni activitatea de actualizare a aplicației Kaspersky Endpoint Security din contul utilizatorului respectiv.
Descărcare actualizări ale modulelor aplicației	Această casetă de selectare activează/dezactivează descărcările de actualizări ale modulelor aplicației împreună cu actualizările bazei de date antivirus. 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: • **Instalare actualizări 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. • **Instalare numai actualizări 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.
Copiere actualizări în folder	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. În mod implicit este specificat următorul director: `C:\ProgramData\Kaspersky Lab\KES\Update distribution\`.
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 (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.
Se 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 aplicațiile 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 aplicațiile 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 aplicațiile 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 aplicațiile în grupul Nu este de încredere.

  Pentru aceste 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

eml – mesaj de e-mail Microsoft Outlook Express

nws – mesaj de e-mail nou Microsoft Outlook Express

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

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

eml – mesaj de e-mail Microsoft Outlook Express

nws – mesaj de e-mail nou Microsoft Outlook Express

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 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

`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 a modulelor aplicațiilor

`downloads.upd.kaspersky.com` Protocolul: `HTTPS` Port: `443`	• Actualizarea bazelor de date și a modulelor aplicațiilor • Se verifică dacă serverele Kaspersky se pot accesa. 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 despre refuzarea accesului la o resursă web în browser (Web Threat Protection și Control Web)

`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`
	Actualizarea bazelor de date și a modulelor aplicațiilor

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	
ds.kaspersky.com Protocolul: HTTPS Port: 443	Despre 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: Any Port: 443, 1443	Despre Kaspersky Security Network
click.kaspersky.com redirect.kaspersky.com Protocolul: HTTPS	Urmați linkurile din interfață
crl.kaspersky.com ocsp.kaspersky.com Protocolul: HTTP Port: 80	Infrastructură cu cheie publică (PKI)

Anexa 6. Evenimentele aplicației în Jurnalul de evenimente Windows

Informațiile despre funcționarea fiecărei componente Kaspersky Endpoint Security, evenimentele de criptare a datelor, performanța fiecărei activități de scanare, activitatea de actualizare și activitatea de verificare a integrității, precum și funcționarea generală a aplicației sunt înregistrate în Jurnalul de evenimente Windows.

Auditare sistem

Codurile evenimentelor

ID eveniment	Descriere	Activat în mod implicit
201	Acordul de licență pentru utilizatorul final a fost încălcat	✓
203	Licența aproape a expirat	–
204	Licența expiră în curând	–
206	Bazele de date lipsesc sau sunt deteriorate	–
207	Bazele de date sunt extrem de învechite	–
208	Bazele de date nu mai sunt actuale	–
209	Executarea automată a aplicației este dezactivată	–
210	Actualizările automate sunt dezactivate	–
211	Autoprotecția este dezactivată	–
212	Activitatea nu se poate executa	–
213	Operația cu resursele aplicației este blocată de componenta Autoprotecție	–
214	Componentele de protecție sunt dezactivate	–
215	Computerul funcționează în modul de siguranță	–
216	Există fișiere neprocesate	–
217	Raport golit	✓
218	Setări aplicație modificate	✓
219	Politică de grup aplicată	✓
220	Politică de grup dezactivată	–
221	Ac	–
222	Activitate oprită	–
223	Activitate finalizată	–
224	Repornește aplicația pentru a finaliza actualizarea	–
225	Este necesară repornirea computerului	✓
226	Licența permite utilizarea componentelor care nu au fost instalate	–
227	Compnentele instalate corespund cu licența	–
229	Eroare de activare	✓
230	Cod de activare de rezervă incorect	–
231	Amenințare activă detectată Dezinfectarea avansată trebuie pornită	–
232	Dezinfectare avansată pornită	–
233	Dezinfectare avansată finalizată	–
235	Aplicație pornită	✓
236	Aplicație oprită	✓

237	Aplicația a căzut în timpul sesiunii anterioare	✓
240	Licența expiră în curând	✓
238	S-au schimbat setările abonamentului	✓
239	S-a reînnoit abonamentul	✓
335	Obiect restaurat din Copie de rezervă	✓
336	Imposibil de restaurat obiectul din Copie de rezervă	✓
245	Procesarea anumitor funcții ale SO este dezactivată	✓
250	Conexiunea criptată a fost terminată	✓
708	Setări activitate aplicate cu succes	–
335	Obiect restaurat din Copie de rezervă	✓
2000	Introduceți un nume de utilizator și parola	–
2001	S-a detectat activitate suspectă în rețea	–
2020	Participarea la KSN este activată	–
2021	Participarea la KSN este dezactivată	–
2022	Servere KSN disponibile	–
2023	Servere KSN indisponibile	–
2024	Aplicația funcționează și prelucrează datele conform legislației relevante, utilizând infrastructura corespunzătoare	✓
227	Toate componentele aplicației definite de licență au fost instalate și se execută în modul normal	–

Behavior Detection

Codurile evenimentelor

ID eveniment	Descriere	Activat în mod implicit
303	S-a detectat un software legal care poate fi utilizat de intruși pentru a vă deteriora computerul sau datele cu caracter personal	–
307	Obiect șters	–
308	A fost creată o copie de rezervă a obiectului	–
311	Nu se poate crea o copie de rezervă	–
313	Nu se poate șterge	–
323	Obiectul va fi șters la repornire	–
329	Obiect redenumit	–
331	Blocat	–
452	Proces terminat	–
453	Procesul nu poate fi oprit	–
455	Derulare înapoi finalizată	–
458	Valoare de registry restaurată	–
459	Valoare de registry ștearsă	–
453	Execuția fișierului/codului este blocată	–

Exploit Prevention

Codurile evenimentelor

ID eveniment	Descriere	Activat în mod implicit
302	S-a detectat un obiect periculos	–
331	Blocat	–
455	Derulare înapoi finalizată	–
323	Obiectul va fi șters la repornire	–
307	Obiect șters	–
329	Obiect redenumit	–
457	Fișier restaurat	–
458	Valoare de registry restaurată	–
459	Valoare de registry ștearsă	–

Host Intrusion Prevention

Codurile evenimentelor

ID eveniment	Descriere	Activat în mod implicit
301	Obiect procesat	–
302	S-a detectat un obiect periculos	–
303	S-a detectat un software legal care poate fi utilizat de intruși pentru a vă deteriora computerul sau datele cu caracter personal	–
306	Obiect dezinfectat	–
307	Obiect șters	–
308	A fost creată o copie de rezervă a obiectului	–
310	Nu se poate crea o copie de rezervă	–
312	Dezinfectare imposibilă	–
313	Nu se poate șterge	–
314	Obiect neprocesat	–
315	Obiect omis	–
317	Eroare de procesare	✓
318	Arhivă detectată	–
319	Obiect arhivat detectat	–
320	Obiect criptat	–
321	Obiect deteriorat	–
322	Arhivă protejată prin parolă detectată	–
323	Obiectul va fi șters la repornire	–
324	Obiectul va fi dezinfectat la repornire	–
327	Suprascris cu o copie dezinfectată anterior	–
332	Informații despre obiectul detectat	–
335	Obiect restaurat din Copie de rezervă	–
336	Imposibil de restaurat obiectul din Copie de rezervă	✓
340	Obiectul este în lista Private KSN permise	✓
401	Aplicație plasată în grupul De încredere	–
402	Aplicație plasată în grupul restricționat	–
403	A fost declanșată componenta Host Intrusion Prevention	–
452	Proces terminat	–
453	Procesul nu poate fi oprit	–

File Threat Protection

Codurile evenimentelor

ID eveniment	Descriere	Activat în mod implicit
302	S-a detectat un obiect periculos	✓
317	Eroare de procesare	✓
336	Imposibil de restaurat obiectul din Copie de rezervă	✓
340	Obiectul este în lista Private KSN permise	✓
301	Obiect procesat	–
306	Obiect dezinfectat	–
307	Obiect șters	–
308	A fost creată o copie de rezervă a obiectului	–
310	Nu se poate crea o copie de rezervă	–
312	Dezinfectare imposibilă	–
313	Nu se poate șterge	–
314	Obiect neprocesat	–
315	Obiect omis	–
318	Arhivă detectată	–
319	Obiect arhivat detectat	–
320	Obiect criptat	–
321	Obiect deteriorat	–
322	Arhivă protejată prin parolă detectată	–
323	Obiectul va fi șters la repornire	–
324	Obiectul va fi dezinfectat la repornire	–
325	Suprascris cu o copie dezinfectată anterior	–
303	S-a detectat un software legal care poate fi utilizat de intruși pentru a vă deteriora computerul sau datele cu caracter personal	–
329	Obiect redenumit	–
335	Obiect restaurat din Copie de rezervă	–
452	Proces terminat	–
453	Procesul nu poate fi oprit	–
332	Informații despre obiectul detectat	–

Web Threat Protection

Codurile evenimentelor

ID eveniment	Descriere	Activat în mod implicit
301	Obiect procesat	–
302	S-a detectat un obiect periculos	✓
303	S-a detectat un software legal care poate fi utilizat de intruși pentru a vă deteriora computerul sau datele cu caracter personal	–
317	Eroare de procesare	✓
318	Arhivă detectată	–
319	Obiect arhivat detectat	–
321	Obiect deteriorat	–
322	Arhivă protejată prin parolă detectată	–
329	Obiect redenumit	–
362	Link periculos blocat	✓
1201	S-a detectat un link periculos deschis anterior	✓
1211	S-a detectat un link rău intenționat deschis anterior	✓
363	Link periculos deschis	✓
341	S-a blocat descărcarea obiectului	–
370	Linkul este	✓
370	Obiectul este în lista Private KSN permise	✓
332	Informații despre obiectul detectat	–

Mail Threat Protection

Codurile evenimentelor

ID eveniment	Descriere	Activat în mod implicit
301	Obiect procesat	–
306	Obiect dezinfectat	–
302	S-a detectat un obiect periculos	✓
317	Eroare de procesare	✓
340	Obiectul este în lista Private KSN permise	✓
307	Obiect șters	–
308	A fost creată o copie de rezervă a obiectului	–
312	Dezinfectare imposibilă	–
314	Obiect neprocesat	–
318	Arhivă detectată	–
319	Obiect arhivat detectat	–
321	Obiect deteriorat	–
322	Arhivă protejată prin parolă detectată	–
329	Obiect redenumit	–
303	S-a detectat un software legal care poate fi utilizat de intruși pentru a vă deteriora computerul	–
332	Informații despre obiectul detectat	–

Firewall

Codurile evenimentelor

ID eveniment	Descriere	Activat în mod implicit
601	Activitate de rețea permisă	–
602	Activitate de rețea blocată	–

Network Threat Protection

Codurile evenimentelor

ID eveniment	Descriere	Activat în mod implicit
651	Atac de rețea detectat	–

BadUSB Attack Prevention

Codurile evenimentelor

ID eveniment	Descriere	Activat în mod implicit
2050	Tastatură autorizată	–
2051	Tastatură neautorizată	✓
2052	Eroare autorizare tastatură	✓

Protecție AMSI

Codurile evenimentelor

ID eveniment	Descriere	Activat în mod implicit
301	Obiect procesat	–
302	S-a detectat un obiect periculos	✓
303	S-a detectat un software legal care poate fi utilizat de intruși pentru a vă deteriora computerul sau datele cu caracter personal	–
314	Obiect neprocesat	–
315	Obiect omis	–
317	Eroare de procesare	✓
318	Arhivă detectată	–
319	Obiect arhivat detectat	–
320	Obiect criptat	–
321	Obiect deteriorat	–
322	Arhivă protejată prin parolă detectată	–
1512	Rezultatul scanării obiectului a fost trimis unei aplicații terțe	–
329	Obiect redenumit	–
332	Informații despre obiectul detectat	–
340	Obiectul este în lista Private KSN permise	✓
2200	Solicitarea AMSI a fost blocată	✓

Application Control

Codurile evenimentelor

ID eveniment	Descriere	Activat în mod implicit
701	Pornire aplicație permisă	–
702	Pornire aplicație interzisă	–
703	Pornire aplicație interzisă în modul testare	–
704	Pornire aplicație permisă în modul testare	–
707	Eroare în setările activității. Setările activității nu sunt aplicate	–
710	Procesul interzis a fost pornit înainte de pornirea componentei Kaspersky Endpoint Security fpr Windows	–
708	Setări activitate aplicate cu succes	–

Control dispozitive

Codurile evenimentelor

ID eveniment	Descriere	Activat în mod implicit
801	Operație cu dispozitivul permisă	–
802	Operație cu dispozitivul interzisă	–
803	Accesul temporar la dispozitiv a fost activat	✓
808	S-a efectuat o operațiune cu fișiere	–
809	Conectarea la rețea a fost blocată	–

Control Web

Codurile evenimentelor

ID eveniment	Descriere	Activat în mod implicit
751	Acces permis	–
752	Acces blocat	–
753	Avertizare despre conținut nedorit	–
754	S-a accesat conținut nedorit după o avertizare	–
751	Pagina permisă a fost deschisă	–

Control anomalie adaptivă

Codurile evenimentelor

ID eveniment	Descriere	Activat în mod implicit
501	Reclamație privind activitatea blocată a aplicației	–
2201	Acțiune proces omisă	–
2200	Acțiune proces blocată	✓

Data Encryption

Codurile evenimentelor

ID eveniment	Descriere	Activat în mod implicit
904	Eroare la aplicarea regulilor de criptare/decriptare a fișierelor	✓
912	Eroare criptare/decriptare fișiere	✓
1305	Eroare la criptarea/decriptarea dispozitivului	✓
931	Eroare la crearea pachetului criptat	✓
951	Eroare la activarea modului portabil	✓
953	Eroare la dezactivarea modului portabil	✓
1311	Încărcarea modului criptat a eșuat	✓
1340	Activitatea pentru gestionarea conturilor Agent de autentificare s-a terminat cu o eroare	✓
1312	Politica nu poate fi aplicată	✓
1342	Efectuare upgrade FDE nereușită	✓
1343	Derulare înapoi a upgrade-ului FDE reușită	✓
1345	Instalarea sau efectuarea upgrade-ului pentru driverele Kaspersky Disk Encryption în imaginea WinRE a eșuat	✓
1346	Dezinstalarea driverelor Kaspersky Disk Encryption din imaginea WinRE a eșuat	✓
1370	Cheia de recuperare BitLocker a fost modificată	✓
901	S-a început aplicarea regulilor de criptare/decriptare a fișierelor	–
902	Aplicarea regulilor de criptare/decriptare a fișierelor s-a terminat	–
903	S-a întrerupt aplicarea regulilor de criptare/decriptare a fișierelor	–
905	Aplicarea regulilor de criptare/decriptare a fișierelor s-a reluat	–
910	Criptare/decriptare fișiere pornită	–
911	Criptare/decriptare fișiere finalizată	–
913	Fișierul nu a fost criptat deoarece este o excludere	–
914	Criptare/decriptare fișiere întreruptă	–
1301	S-a început criptarea/decriptarea dispozitivului	–
1302	Criptarea/decriptarea dispozitivului s-a finalizat	–
1307	Dispozitivul nu este criptat	–
1303	S-a întrerupt criptarea/decriptarea dispozitivului	–
1304	Criptarea/decriptarea dispozitivului s-a reluat	–
1309	Procesul de criptare/decriptare a unității a fost comutat la modul pasiv	–
1308	Procesul de criptare/decriptare a dispozitivului a fost comutat la modul activ	–
1306	Utilizatorul a renunțat la politica de criptare	–
940	Acces la fișier blocat	✓

950	Mod portabil activat	–
952	Mod portabil dezactivat	–
1330	Cont nou Agent de autentificare creat	–
1337	Contul nu a fost adăugat. Acest cont există deja	–
1338	Contul nu a fost modificat. Acest cont nu există	–
1339	Contul nu a fost șters. Acest cont nu există	–
1331	Cont Agent de autentificare șters	–
1332	Parolă cont Agent de autentificare schimbată	–
1334	Încercarea de conectare la Agent de autentificare nu a reușit	–
1333	Conectare cu succes în Agentul de autentificare	–
1335	Unitate de hard disk accesată utilizându-se procedura de solicitare a accesului la dispozitive criptate	–
1336	Încercare de accesare a unității de hard disk utilizând procedura de solicitare a accesului la dispozitive criptate nu a reușit	–
1310	Modul de criptare încărcat	–
1344	Derularea înapoi a upgrade-ului pentru Full Disk Encryption s-a finalizat cu o eroare	✓
1341	Upgrade FDE reușit	✓
1332	Parolă cont Agent de autentificare schimbată	–

Senzor Endpoint

Codurile evenimentelor

ID eveniment	Descriere	Activat în mod implicit
2100	Server Kaspersky Anti Targeted Attack Platform indisponibil	–
2105	Pornirea aplicației a fost blocată	✓
2106	Deschiderea documentului a fost blocată	✓
2104	Procesarea activităților de la serverul Kaspersky Anti Targeted Attack Platform este activă	–
2103	Procesarea activităților de la serverul Kaspersky Anti Targeted Attack Platform este inactivă	–
2101	Componenta Senzor Endpoint este conectată la server	–
2102	S-a restaurat conexiunea la Kaspersky Anti Targeted Attack Platform	–
2112	Toate procesele pornite de la un fișier imagine sau flux au fost terminate	✓
2113	Aplicație pornită	✓
2111	Fișierul sau fluxul a fost șters de administratorul serverului Kaspersky Anti Targeted Attack Platform	✓
2110	Fișierul a fost restaurat din carantină pe serverul Kaspersky Anti Targeted Attack Platform de către administrator	✓
2109	Fișierul a fost mutat pe serverul Kaspersky Anti Targeted Attack Platform de către administrator	✓
2107	Activitatea în rețea a tuturor aplicațiilor terțe este blocată	✓
2108	Activitatea în rețea a tuturor aplicațiilor terțe este deblocată	✓

Scanarea computerului

Codurile evenimentelor

ID eveniment	Descriere	Activat în mod implicit
302	S-a detectat un obiect periculos	✓
335	Obiect restaurat din Copie de rezervă	✓
336	Imposibil de restaurat obiectul din Copie de rezervă	✓
340	Obiectul este în lista Private KSN permise	✓
301	Obiect procesat	–
329	Obiect redenumit	–
306	Obiect dezinfectat	–
307	Obiect șters	–
308	A fost creată o copie de rezervă a obiectului	–
310	Nu se poate crea o copie de rezervă	–
312	Dezinfectare imposibilă	–
313	Nu se poate șterge	–
314	Obiect neprocesat	–
315	Obiect omis	–
317	Eroare de procesare	–
318	Arhivă detectată	–
319	Obiect arhivat detectat	–
320	Obiect criptat	–
321	Obiect deteriorat	–
322	Arhivă protejată prin parolă detectată	–
323	Obiectul va fi șters la repornire	–
324	Obiectul va fi dezinfectat la repornire	–
327	Suprascris cu o copie dezinfectată anterior	–
303	S-a detectat un software legal care poate fi utilizat de intruși pentru a vă deteriora computerul sau datele cu caracter personal	–

Verificare integritate

Codurile evenimentelor

ID eveniment	Descriere	Activat în mod implicit
2002	Verificarea semnăturii modulului de sistem nu a reușit	–

Actualizare bază de date

Codurile evenimentelor

ID eveniment	Descriere	Activat în mod implicit
101	A apărut o eroare internă	✓
1001	Sursă actualizare selectată	–
1002	Server proxy selectat	–
1003	Descărcare fișier	–
1004	Fișier descărcat	–
1005	Fișier instalat	–
1006	Fișier actualizat	–
1007	Fișier derulat înapoi din cauza unei erori de actualizare	–
1008	Se actualizează fișierele	–
1009	Se distribuie actualizările	–
1010	Se derulează înapoi fișierele	–
1011	Eroare la actualizarea componentei	–
1012	Eroare la distribuirea actualizărilor componentei	–
1013	Se creează lista de fișiere de descărcat	–
1014	Eroare actualizare locală	–
1016	Operațiune revocată de utilizator	–
1017	Imposibil de pornit simultan două activități	–
1018	Eroare la verificarea bazelor de date și a modulelor aplicației	–
1019	Eroare la interacțiunea cu Kaspersky Security Center	–
1020	Nicio actualizare disponibilă	–
1021	Nu s-au actualizat toate componentele	–
1022	Distribuirea actualizării s-a finalizat cu succes	–
1023	Actualizarea s-a finalizat cu succes, distribuirea actualizării nu a reușit	–
2153	Nu s-a reușit instalarea corecției	–
2156	Nu s-a reușit derularea înapoi a corecției	–
2150	Se descarcă corecțiile	–
2151	Se instalează corecțiile	–
2152	Corecție instalată	–
2154	Se derulează înapoi corecția	–
2155	Corecție derulată înapoi	–

Ștergere date

Codurile evenimentelor

ID eveniment	Descriere	Activat în mod implicit
223	Activitate finalizată	–
221	Ac	–
222	Activitate oprită	–
2252	Obiectul nu se poate șterge	–
2253	Statistici activitate de ștergere	–
2251	Obiect șters	–

Informații despre codurile de la terți

Informațiile despre codurile de la terți sunt conținute în fișierul legal_notices.txt din directorul de instalare al aplicației.

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 Systems Incorporated în Statele Unite ale Americii și/sau în alte țări.

Apple, FireWire, iTunes și Safari sunt mărci comerciale ale Apple Inc. înregistrate în Statele Unite ale Americii și 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.

Android și Google Chrome sunt mărci comerciale ale Google, Inc.

Citrix și Citrix Provisioning Services și XenDesktop sunt mărci comerciale ale Citrix Systems, Inc. Și/sau a uneia dintre companiile sale afiliate și pot fi înregistrate la Oficiul pentru Brevete și Mărci Comerciale din Statele Unite ale Americii și din alte țări.

Dell este o marcă comercială a Dell, Inc. sau a filialelor sale.

dBase este o marcă comercială a dataBased Intelligence, Inc.

EMC este o marcă comercială sau o marcă comercială înregistrată a EMC Corporation în Statele Unite ale Americii și/sau în alte țări.

Radmin este o marcă comercială înregistrată a Famatech.

IBM este o marcă comercială a International Business Machines Corporation, înregistrată în multe jurisdicții din lume.

ICQ este o marcă comercială și/sau marcă de serviciu a ICQ LLC.

Intel este o marcă comercială a Intel Corporation în S.U.A. și/sau în alte țări.

IOS este o marcă comercială înregistrată a Cisco Systems, Inc. și/sau a companiilor sale afiliate din Statele Unite ale Americii și alte țări.

Lenovo și 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 înregistrată a Mail.Ru, LLC.

McAfee este o marcă comercială sau o marcă comercială înregistrată a McAfee, Inc. în Statele Unite ale Americii și în alte țări.

Microsoft, Access, Active Directory, ActiveSync, BitLocker, Excel, Internet Explorer, LifeCam Cinema, MSDN, MultiPoint, Outlook, PowerPoint, PowerShell, Visual Basic, Visual FoxPro, Windows, Windows PowerShell, Windows Server, Windows Store, MS-DOS, Surface și Hyper-V sunt mărci comerciale ale Microsoft Corporation în Statele Unite ale Americii și în alte țări.

Mozilla, Firefox și Thunderbird sunt mărci comerciale ale Mozilla Foundation.

Java și JavaScript sunt mărci comerciale înregistrate ale Oracle și/sau ale companiilor sale afiliate.

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 și VMware ESXi sunt mărci comerciale înregistrate sau mărci comerciale ale VMware, Inc. în Statele Unite ale Americii și/sau în alte jurisdicții.

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.

SAMSUNG este o marcă comercială a SAMSUNG în Statele Unite ale Americii și în alte țări.