ESET NOD32 Antivirus

Ghidul utilizatorului

Faceţi clic aici pentru a afişa versiunea Ajutor a acestui document

Drepturi de autor ©2023 deținute de ESET, spol. s r.o.

Produsul ESET NOD32 Antivirus a fost dezvoltat de ESET, spol. s r.o.

Pentru mai multe informații, vizitați https://www.eset.com.

Toate drepturile rezervate. Nicio parte a acestei documentații nu poate fi reprodusă, stocată într-un sistem de regăsire sau transmisă sub nicio formă și prin niciun mijloc, electronic, mecanic, prin fotocopiere, înregistrare, scanare sau în alt mod, fără permisiunea exprimată în scris a autorului.

ESET, spol. s r.o. își rezervă dreptul de a modifica oricare dintre software-urile de aplicație descrise, fără notificare prealabilă.

Asistență tehnică: https://support.eset.com

REV. 19.03.2023

1 ESET NOD32 Antivirus 1
1.1 Ce este nou? 2
1.2 Ce produs am? 2
1.3 Cerințe de sistem 3
1.3 Versiunea dvs. de Windows 7 este învechită 4
1.3 Microsoft nu mai oferă asistență pentru Windows 7 4
1.3 Windows Vista nu mai este acceptat 5
1.4 Prevenire 5
1.5 Pagini Ajutor 6
2 Instalare 8
2.1 Program de instalare în direct 8
2.2 Instalare offline 9
2.3 Activare produs 11
2.3 Introducerea cheii de licență în cursul activării 12
2.3 Utilizare ESET HOME cont 12
2.3 Activare licență de încercare 13
2.3 Cheie de licență ESET gratuită 14
2.3 Activarea nu a reușit - scenarii comune 15
2.3 Activarea nu a reușit din cauza licenței cu limită de utilizare depășită 15
2.3 Upgrade licență 16
2.3 Upgrade produs 17
2.3 Downgrade licență 17
2.3 Downgrade produs 18
2.4 Depanator de instalare 19
2.5 Prima scanare după instalare 19
2.6 Efectuarea de upgrade la o versiune mai recentă 20
2.6 Upgrade-ul automat pentru un produs moștenit 21
2.7 Recomandați produsul ESET unui prieten 21
2.7 Se va instala ESET NOD32 Antivirus 22
2.7 Treceți la o altă gamă de produse 22
2.7 Înregistrare 22
2.7 Progres activare 22
2.7 Activare reușită 22
3 Ghidul începătorului 23
3.1 Conectați-vă la ESET HOME 23
3.1 Conectați-vă la ESET HOME 24
3.1 Conectarea nu a reușit - erori uzuale 25
3.1 Adăugați un dispozitiv în ESET HOME 26
3.2 Fereastra principală a programului 26
3.3 Actualizări 29
4 Lucrul cu ESET NOD32 Antivirus 30
4.1 Protecție computer 32
4.1 Motor de detecție 33
4.1 Opțiuni avansate pentru motorul de detecție 38
4.1 S-a detectat o infiltrare 38
4.1 Protecție în timp real a sistemului de fișiere 40
4.1 Niveluri de curățare 42
4.1 Când se modifică configurarea protecției în timp real 43
4.1 Verificare protecție în timp real 43
4.1 Ce este de făcut dacă protecția în timp real nu funcționează 43

4.1 Excluderi de procese 44
4.1 Adăugarea sau editarea excluderilor de procese 45
4.1 Protecție bazată pe cloud 45
4.1 Filtru de excluderi pentru protecția bazată pe cloud 48
4.1 Scanare computer 48
4.1 Lansator scanare particularizată 51
4.1 Progres scanare 52
4.1 Log scanare computer 54
4.1 Scanări malware 56
4.1 Scanare stare de inactivitate 56
4.1 Profiluri de scanare 57
4.1 Ținte de scanare 57
4.1 Control dispozitiv 58
4.1 Editor reguli de control dispozitiv 59
4.1 Dispozitive detectate 60
4.1 Grupuri de dispozitive 60
4.1 Adăugarea regulilor de control al dispozitivului 61
4.1 Componenta Sistem de prevenire a intruziunilor la nivel host (HIPS) 64
4.1 Fereastra interactivă HIPS 66
4.1 S-a detectat un posibil comportament de ransomware 68
4.1 Gestionare regulă HIPS 69
4.1 Setări regulă HIPS 70
4.1 Adăugare aplicație/cale registry pentru HIPS 73
4.1 Setare avansată HIPS 73
4.1 Încărcare drivere permisă întotdeauna 74
4.1 Mod Gamer 74
4.1 Scanare la pornire 74
4.1 Verificare automată fișiere la pornire 75
4.1 Protecție documente 76
4.1 Excluderi 76
4.1 Excluderi de performanță 76
4.1 Adăugarea sau editarea excluderilor de performanță 77
4.1 Formatul pentru excluderea unei căi 79
4.1 Excluderi de la detectare 80
4.1 Adăugare sau editare excludere de la detectare 82
4.1 Expertul pentru crearea unei excluderi de la detectare 83
4.1 Excluderi HIPS 84
4.1 Parametri ThreatSense 84
4.1 Listă de fișiere excluse de la scanare 88
4.1 Parametri ThreatSense suplimentari 88
4.2 Protecție internet 89
4.2 Filtrare protocol 90
4.2 Aplicații excluse 91
4.2 Adrese IP excluse 92
4.2 Adăugare adresă IPv4 93
4.2 Adăugare adresă IPv6 93
4.2 SSL/TLS 93
4.2 Certificate 95
4.2 Trafic de rețea criptat 95
4.2 Lista de certificate cunoscute 96
4.2 Listă de aplicații filtrate SSL/TLS 97

4.2 Protecție client email ... 97
4.2 Integrare client email ... 98
4.2 Bara de instrumente Microsoft Outlook ... 98
4.2 Bară de instrumente Outlook Express și Windows Mail ... 99
4.2 Dialog de confirmare ... 99
4.2 Rescanare mesaje ... 99
4.2 Protocoale de email ... 100
4.2 Filtru POP3, POP3S ... 101
4.2 Etichete e-mail ... 102
4.2 Protecție acces Web ... 102
4.2 Setare avansată pentru Protecție acces web ... 105
4.2 Protocoale Web ... 105
4.2 Gestionare adresă URL ... 106
4.2 Listă de adrese URL ... 107
4.2 Crearea unei liste noi de adrese URL ... 108
4.2 Cum se adaugă o mască URL ... 109
4.2 Protecție Anti-Phishing ... 109
4.3 Actualizare program ... 111
4.3 Setare actualizare ... 114
4.3 Derularea înapoi a actualizărilor ... 116
4.3 Interval de timp pentru derulare înapoi ... 118
4.3 Actualizări produs ... 118
4.3 Opțiuni de conectare ... 118
4.3 Cum se creează sarcini de actualizare ... 119
4.3 Fereastră de dialog – Este necesară repornirea ... 120
4.4 Instrumente ... 120
4.4 Instrumente în ESET NOD32 Antivirus ... 120
4.4 Fișiere log ... 121
4.4 Filtrare Log ... 123
4.4 Configurația de scriere în log ... 125
4.4 Procese care se execută ... 126
4.4 Raport de securitate ... 127
4.4 ESET SysInspector ... 129
4.4 Orar ... 130
4.4 Opțiuni pentru Scanare planificată ... 132
4.4 Prezentare sarcină programată ... 133
4.4 Detalii sarcină ... 133
4.4 Program sarcină ... 134
4.4 Program sarcină – O dată ... 134
4.4 Program sarcină – Zilnic ... 134
4.4 Program sarcină – Săptămânal ... 134
4.4 Program sarcină – Declanșat de eveniment ... 134
4.4 Sarcină omisă ... 135
4.4 Detalii activitate – Actualizare ... 135
4.4 Detalii activitate – Rulare aplicație ... 136
4.4 Curățare sistem ... 136
4.4 ESET SysRescue Live ... 137
4.4 Carantină ... 138
4.4 Server proxy ... 140
4.4 Selectare mostră pentru analiză ... 141
4.4 Selectare mostră pentru analiză - Fișier suspect ... 142

4.4 Selectare mostră pentru analiză - Site suspect ... 143
4.4 Selectare mostră pentru analiză - Fișier fals pozitiv ... 143
4.4 Selectare mostră pentru analiză - Site fals pozitiv ... 144
4.4 Selectare mostră pentru analiză - Altele ... 144
4.4 Actualizare Microsoft Windows® ... 144
4.4 Fereastră de dialog – Actualizări de sistem ... 144
4.4 Informații actualizare ... 145
4.5 Interfață utilizator ... 145
4.5 Elemente interfață utilizator ... 145
4.5 Setare acces ... 146
4.5 Parolă pentru Setare avansată ... 147
4.5 Pictograma barei de sistem ... 147
4.5 Asistență pentru cititorul de ecran ... 149
4.5 Ajutor și asistență ... 149
4.5 Despre ESET NOD32 Antivirus ... 150
4.5 Știri ESET ... 150
4.5 Trimiterea datelor de configurare a sistemului ... 151
4.5 Asistență tehnică ... 152
4.6 Notificări ... 152
4.6 Fereastră de dialog - Stări aplicație ... 153
4.6 Notificări desktop ... 153
4.6 Lista Notificări desktop ... 155
4.6 Alerte interactive ... 156
4.6 Mesaje de confirmare ... 158
4.6 Unități media portabile ... 159
4.6 Se redirecționează ... 160
4.7 Setări de confidențialitate ... 162
4.8 Profiluri ... 163
4.9 Scurtături tastatură ... 164
4.10 Diagnostic ... 165
4.10 Asistență tehnică ... 166
4.10 Importarea și exportarea setărilor ... 167
4.10 Restaurează toate setările în secțiunea curentă ... 167
4.10 Revenire la setări implicite ... 168
4.10 Eroare la salvarea configurării ... 168
4.11 Scaner linie de comandă ... 168
4.12 ESET CMD ... 171
4.13 Detectare stare de inactivitate ... 172
5 Întrebări frecvente ... 172
5.1 Cum se actualizează ESET NOD32 Antivirus ... 173
5.2 Cum se elimină un virus din PC ... 174
5.3 Cum se creează o sarcină nouă în Orar ... 174
5.4 Cum se programează o scanare săptămânală a computerului ... 175
5.5 Cum deblocați secțiunea Setări avansate ... 175
5.6 Cum se rezolvă dezactivarea produsului în ESET HOME ... 176
5.6 Produs dezactivat, dispozitiv deconectat ... 176
5.6 Produsul nu a fost activat ... 177
6 Programul de îmbunătățire a experienței clienților ... 177
7 Acord de licență pentru utilizatorul final ... 178
8 Politica de confidenţialitate ... 189

ESET NOD32 Antivirus

ESET NOD32 Antivirus reprezintă o nouă abordare a securității cu adevărat integrate a computerului. Cea mai recentă versiune a motorului de scanare ESET LiveGrid® utilizează viteza și precizia pentru menținerea computerului dvs. în siguranță. Rezultatul este un sistem inteligent aflat mereu în alertă pentru prevenirea atacurilor și a software-ului dăunător care v-ar putea pune computerul în pericol.

ESET NOD32 Antivirus reprezintă o soluție de securitate completă care combină protecția maximă cu efecte minime asupra sistemului. Tehnologiile noastre avansate utilizează inteligența artificială pentru a preveni infiltrarea virușilor, programelor spyware, cailor troieni, viermilor, programelor adware, rootkiturilor și altor amenințări fără a afecta performanța sistemului sau a computerului.

Caracteristici și avantaje

Interfață de utilizator reproiectată	Interfața de utilizator din această versiune a fost reproiectată și simplificată semnificativ pe baza rezultatelor testelor privind gradul de utilizare. Toate textele și notificările din interfața grafică a utilizatorului au fost examinate cu atenție, iar acum interfața acceptă limbi cu scriere/citire de la dreapta la stânga, cum ar fi ebraica și araba. Ajutorul online este acum integrat în ESET NOD32 Antivirus și oferă conținut privind asistența actualizat în mod dinamic.
Antivirus și antispyware	Detectează și curăță în mod proactiv viruși, viermi, troieni și rootkit-uri – atât versiuni cunoscute cât și neclasificate. Tehnologia Euristică avansată semnalizează chiar și programele malware nemaiîntâlnite, protejându-vă împotriva amenințărilor necunoscute și neutralizându-le înainte ca acestea să poată provoca daune. Modulele Protecție acces Web și Protecție Anti-Phishing funcționează prin monitorizarea comunicării dintre browserele Web și serverele la distanță (inclusiv SSL). Modulul Protecție client de email oferă controlul asupra comunicărilor prin email primite prin protocoale POP3(S) și IMAP(S).
Actualizări regulate	Actualizarea regulată a motorului de detecție (cunoscută anterior sub denumirea de „bază de semnături virale”) și a modulelor de program este cel mai bun mod de a asigura nivelul maxim de securitate pe computer.
ESET LiveGrid® (Nivel de reputație cloud-powered)	Puteți verifica reputația proceselor și fișierelor în execuție direct din ESET NOD32 Antivirus.
Control dispozitiv	Scanează automat toate unitățile flash USB, cardurile de memorie și CD-urile/DVD-urile. Blochează unitățile media portabile în funcție de tipul acestora, de producător, de dimensiune și de alte atribute.
Funcționalitate HIPS	Puteți particulariza mai detaliat comportamentul sistemului; specificați reguli pentru registry-ul de sistem, activați procese și programe și efectuați reglajul fin al nivelului de securitate.
Mod Gamer	Amână toate ferestrele pop-up, actualizările sau alte activități care solicită intens sistemul pentru a păstra resursele de sistem pentru jocuri și alte activități pe ecran complet.

Caracteristicile produsului ESET NOD32 Antivirus sunt funcționale dacă se activează licența. Vă recomandăm să reînnoiți licența pentru ESET NOD32 Antivirus cu câteva săptămâni înainte ca aceasta să expire.

Ce este nou?

Ce este nou în ESET NOD32 Antivirus 15

ESET HOME (anterior myESET)

Oferă vizibilitate și control sporite asupra securității dvs. Instalați protecție pentru dispozitive noi, adăugați și partajați licențe și primiți notificări importante prin aplicația mobilă și portalul web. Pentru informații suplimentare, vizitați ghidul de ajutor online ESET HOME.

Sistem de prevenire a intruziunilor la nivel host (HIPS) îmbunătățit

Scanează regiuni de memorie pe care unele tehnici sofisticate de injectare de malware le pot infecta. Îmbunătățirile extind capacitatea tehnologică de detecție a celor mai sofisticate intruziuni malware.

Pentru imagini și informații suplimentare despre noile caracteristici din ESET NOD32 Antivirus, consultați secțiunea Ce este nou în cea mai recentă versiune a produselor ESET destinate persoanelor fizice.

> Pentru a dezactiva notificările de tip **Ce este nou?**, faceți clic pe **Setare avansată** > **Notificări** > **Notificări desktop**. Faceți clic pe **Editare** lângă **Notificări desktop** și debifați caseta de selectare **Afișați notificările de tip Ce este nou**. Pentru informații suplimentare despre notificări, consultați secțiunea Notificări.

Ce produs am?

ESET oferă mai multe niveluri de securitate cu noi produse, de la soluții antivirus puternice și rapide la soluții complete de securitate cu efecte minime asupra sistemului:

- **ESET NOD32 Antivirus**
- **ESET Internet Security**
- **ESET Smart Security Premium**

Pentru a determina produsul care este instalat, deschideți fereastra principală a programului și veți vedea numele produsului în partea de sus a ferestrei (consultați articolul din Baza de cunoștințe).

Tabelul de mai jos descrie caracteristicile disponibile în fiecare produs specific.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Motor de detecție	✔	✔	✔
Învățare programată avansată	✔	✔	✔
Blocare exploit-uri	✔	✔	✔
Protecție împotriva atacurilor bazate pe scripturi	✔	✔	✔
Anti-Phishing	✔	✔	✔
Protecție acces Web	✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
HIPS (inclusiv Ransomware Shield)	✔	✔	✔
Antispam		✔	✔
Protecție firewall		✔	✔
Inspector de rețea		✔	✔
Protecție camere Web		✔	✔
Protecție împotriva atacurilor de rețea		✔	✔
Protecție Botnet		✔	✔
Protecție plăți prin bancă		✔	✔
Control parental		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Este posibil ca unele dintre produsele de mai sus să nu fie disponibile pentru limba/regiunea dvs.

Cerințe de sistem

Sistemul trebuie să respecte următoarele cerințe hardware și software pentru ca ESET NOD32 Antivirus să funcționeze optim:

Procesoare acceptate

Procesor Intel sau AMD pe 32 de biți (x86) cu set de instrucțiuni SSE2 sau pe 64 de biți (x64), la frecvență de 1 GHz sau mai mare
Procesor bazat pe ARM64, 1 GHz sau superior

Sisteme de operare acceptate*

Microsoft® Windows® 11
Microsoft® Windows® 10
Microsoft® Windows® 8.1
Microsoft® Windows® 8
Microsoft® Windows® 7 SP1 cu cele mai recente actualizări Windows
Microsoft® Windows® Home Server 2011 64-bit

Întotdeauna încercați să vă păstrați actualizat sistemul de operare.

Altele

Este necesară o conexiune internet pentru ca activarea și actualizările produsului ESET NOD32 Antivirus să funcționeze corect.

Două programe antivirus care rulează simultan pe un singur dispozitiv provoacă conflicte inevitabile de resurse de sistem, cum ar fi încetinirea sistemului, făcându-l inoperabil.

* ESET nu poate oferi protecție pentru sistemele de operare neacceptate începând cu februarie 2021.

Versiunea dvs. de Windows 7 este învechită

Problemă

Utilizați o versiune învechită a sistemului de operare. Pentru a rămâne protejat, întotdeauna încercați să vă păstrați actualizat sistemul de operare.

Rezolvare

Ați instalat ESET NOD32 Antivirus pe {GET_OSNAME} {GET_BITNESS}.

Verificați că ați instalat Windows 7 Service Pack 1 (SP1) cu cea mai recentă actualizare Windows (cel puțin KB4474419 și KB4490628).

Dacă versiunea dvs. de Windows 7 nu este configurată să se actualizeze în mod automat, faceți clic pe **meniul Start** > **Panou de control** > **Sistem și securitate** > **Windows Update** > **Căutare actualizări**, apoi faceți clic pe **Instalare actualizări**.

Consultați și Microsoft nu mai oferă asistență pentru Windows 7.

Microsoft nu mai oferă asistență pentru Windows 7

Problemă

Asistența Microsoft pentru Windows 7 s-a încheiat pe 14 ianuarie 2020. Ce înseamnă acest lucru?

Dacă veți continua să utilizați Windows 7 după încheierea asistenței, PC-ul va funcționa în continuare, dar poate deveni mai vulnerabil la riscurile de securitate și viruși. PC-ul dvs. nu va mai primi actualizări Windows (inclusiv actualizări de securitate).

Rezolvare

Faceți upgrade de la Windows 7 la Windows 10? Actualizați-vă produsul ESET

Procesul de upgrade este relativ ușor și, în multe cazuri, puteți face acest lucru fără a pierde fișierele. Înainte de a face upgrade la Windows 10:

1. Verificați/actualizați produsul ESET
2. Efectuați copia de rezervă a datelor importante
3. Citiți întrebările frecvente privind upgrade-ul la Windows 10, de la Microsoft, și actualizați sistemul de operare Windows

Obțineți un computer sau un dispozitiv nou? Transferați produsul ESET

Dacă ați achiziționat un computer sau un dispozitiv nou sau dacă urmează să faceți acest lucru - aflați cum să transferați produsul ESET existent pe un dispozitiv nou.

Consultați și Asistența pentru Windows 7 s-a încheiat.

Windows Vista nu mai este acceptat

Problemă

Din cauza limitărilor tehnice de pe Windows Vista, ESET NOD32 Antivirus nu mai poate furniza protecție după **februarie 2021**. Produsul ESET va deveni **nefuncțional**. Acest lucru vă poate face sistemul vulnerabil la infiltrări.

Asistența Microsoft pentru Windows Vista s-a încheiat pe 11 aprilie 2017. Ce înseamnă acest lucru?

Dacă veți continua să utilizați Windows Vista după încheierea asistenței, PC-ul va funcționa în continuare, dar poate deveni mai vulnerabil la riscurile de securitate și viruși. PC-ul dvs. nu va mai primi actualizări Windows (inclusiv actualizări de securitate).

Rezolvare

Faceți upgrade de la Windows Vista la Windows 10? Obțineți un computer sau un dispozitiv nou și transferați produsul ESET

Înainte de a face upgrade la Windows 10:

1. Efectuați copia de rezervă a datelor importante
2. Citiți întrebările frecvente privind upgrade-ul la Windows 10, de la Microsoft, și actualizați sistemul de operare Windows
3. Instalați sau transferați produsul ESET existent pe un dispozitiv nou.

Consultați și Asistența pentru Windows Vista s-a încheiat.

Prevenire

Atunci când lucrați la computer și în special atunci când navigați pe Internet, nu uitați că niciun sistem antivirus din lume nu poate elimina complet riscul prezentat de detectări și atacuri la distanță. Pentru a furniza protecție și convenabilitate maxime, este esențial să folosiți corect soluția antivirus și să respectați câteva reguli utile:

Actualizați cu regularitate

Potrivit statisticilor furnizate de ESET LiveGrid®, mii de infiltrări noi, unice sunt create în fiecare zi pentru a ocoli măsurile de securitate existente și a aduce profit autorilor lor – toate acestea pe seama celorlalți utilizatori. Specialiștii din laboratorul de cercetare de la ESET analizează aceste amenințări zilnic și pregătesc și lansează actualizări pentru a îmbunătăți permanent nivelul de protecție oferit utilizatorilor. Pentru a asigura eficiența maximă a acestor actualizări, este important ca actualizările să fie corect configurate în sistem. Pentru informații suplimentare despre configurarea actualizărilor, consultați capitolul Setare actualizare.

Descărcați corecții de securitate

Autorii de software dăunător exploatează adesea diverse vulnerabilități de sistem pentru a spori eficiența răspândirii de cod dăunător. Ținând cont de acest lucru, companiile de software urmăresc îndeaproape apariția oricăror vulnerabilități în aplicațiile lor și lansează în mod regulat actualizări de securitate pentru a elimina amenințările potențiale. Este important să descărcați aceste actualizări de securitate atunci când sunt lansate. Microsoft Windows și browserele Web cum ar fi Internet Explorer sunt două exemple de programe pentru care actualizările de securitate sunt publicate regulat.

Efectuați copia de rezervă a datelor importante

Celor care scriu programe dăunătoare de obicei nu le pasă de nevoile utilizatorilor, iar activitatea programelor dăunătoare adesea conducea la funcționarea total incorectă a unui sistem de operare și pierderea datelor importante. Este important să efectuați în mod regulat copia de rezervă pentru datele dvs. importante și sensibile pe o sursă externă, cum ar fi un DVD sau un hard disk extern. Astfel este mai ușoară și mai rapidă recuperarea datelor în cazul unei defecțiuni de sistem.

Scanați în mod regulat computerul după viruși

Detectarea mai multor viruși, viermi, troieni și rootkit-uri cunoscute și necunoscute este gestionată de modulul Protecție în timp real sistem de fișiere. Acest lucru înseamnă că de fiecare dată când accesați sau deschideți un fișiere acesta va fi scanat pentru a detecta activitatea dăunătoare. Vă recomandăm să executați o scanare completă a computerului cel puțin o dată pe lună, deoarece semnăturile programelor malware pot varia, iar motorul de detectare se actualizează zilnic.

Respectați regulile elementare de securitate

Aceasta este regula cea mai folositoare și mai eficientă – fiți mereu precaut. În prezent, multe infiltrări necesită intervenția utilizatorului pentru executare și distribuire. Dacă sunteți atent atunci când deschideți fișiere noi, veți economisi timp și efort considerabile, care ar fi altminteri consumate curățând infiltrările. Iată câteva indicații utile:

- Nu vizitați site-uri Web suspecte, cu multiple pop-upuri și reclame strălucitoare.
- Fiți atent atunci când instalați programe freeware, pachete de codecuri etc. Folosiți numai programe sigure și vizitați numai site-uri Web sigure.
- Fiți atent atunci când deschideți atașări de email, în special acelea de la mesaje de corespondență în masă și mesaje de la expeditori necunoscuți.
- Nu folosiți un cont de Administrator pentru lucrul zilnic la computer.

Pagini Ajutor

Bine ați venit la ghidul de utilizare a produsului ESET NOD32 Antivirus. Informațiile furnizate aici vă vor familiariza cu produsul și vă vor ajuta să vă securizați suplimentar computerul.

Introducere

Înainte de a utiliza ESET NOD32 Antivirus, vă recomandăm să vă familiarizați cu diferite tipuri de detectări și atacuri la distanță pe care le puteți întâlni când utilizați computerul.

De asemenea, am compilat o listă de caracteristici noi introduse în ESET NOD32 Antivirus și un ghid pentru a vă ajuta să configurați setările de bază.

Cum se utilizează paginile de ajutor ale produsului ESET NOD32 Antivirus

Subiectele de ajutor sunt împărțite în mai multe capitole și subcapitole. Apăsați pe **F1** pentru a vizualiza informații despre fereastra în care vă aflați în acest moment.

Programul vă permite să căutați un subiect de ajutor în funcție de cuvintele cheie sau să căutați conținutul prin introducerea cuvintelor ori a expresiilor. Diferența dintre cele două metode constă în faptul că un cuvânt cheie poate fi corelat logic cu paginile de ajutor care nu conțin în text cuvântul cheie respectiv. Căutarea după cuvinte și fraze va efectua o căutare în conținutul tuturor paginilor și va afișa numai paginile care conțin cuvântul sau fraza căutat(ă) în textul respectiv.

Pentru consecvență și pentru a elimina confuzia, terminologia utilizată în acest ghid se bazează pe numele de parametri ESET NOD32 Antivirus. De asemenea, utilizăm un set uniform de simboluri pentru a evidenția subiectele de interes sau cu semnificație deosebită.

O notă este doar o scurtă observație. Deși le puteți omite, notele pot furniza informații prețioase, cum ar fi caracteristicile specifice sau un link la anumite subiecte asociate.

Acestea vă necesită atenția și vă încurajăm să nu le omiteți. De obicei, oferă informații care nu sunt critice, dar sunt semnificative.

Acestea reprezintă informații care necesită atenție și precauție suplimentare. Avertismentele sunt plasate special pentru a vă descuraja de la comiterea unor greșeli potențial dăunătoare. Citiți și înțelegeți textul de avertizare introdus în paranteze, deoarece se referă la setări de sistem foarte sensibile sau la o acțiune riscantă.

Acesta este un caz de utilizare sau un exemplu practic care are drept scop să vă ajute să înțelegeți cum poate fi utilizată o anumită funcție sau caracteristică.

Convenție	Semnificație
Tip aldin	Numele elementelor de interfață, cum ar fi casete și butoane de opțiuni.
Tip cursiv	Substituenți pentru informațiile pe care le furnizați. De exemplu, nume fișier sau cale semnifică faptul că tastați calea efectivă sau un nume de fișier.
`Courier New`	Mostre de cod sau comenzi
Hyperlink	Oferă acces rapid și ușor la subiecte cu referințe încrucișate sau la locații Web externe. Hyperlinkurile sunt evidențiate în albastru și pot fi subliniate.
%ProgramFiles%	Directorul sistemului Windows în care sunt stocate programele instalate pe sistemul Windows.

Ajutor online reprezintă sursa principală a conținutului de ajutor. Cea mai recentă versiune Ajutor online va fi afișată automat atunci când aveți o conexiune funcțională la Internet.

Instalare

Există câteva metode pentru a instala ESET NOD32 Antivirus pe computer. Metodele de instalare pot varia în funcție de țară și de mijloacele de distribuire:

- Live Installer – Descărcat de pe site-ul ESET sau CD/DVD. Pachetul de instalare este universal pentru toate limbile (alegeți limba corespunzătoare). Live Installer este un fișier mic; fișierele suplimentare necesare pentru instalarea ESET NOD32 Antivirus sunt descărcate automat.

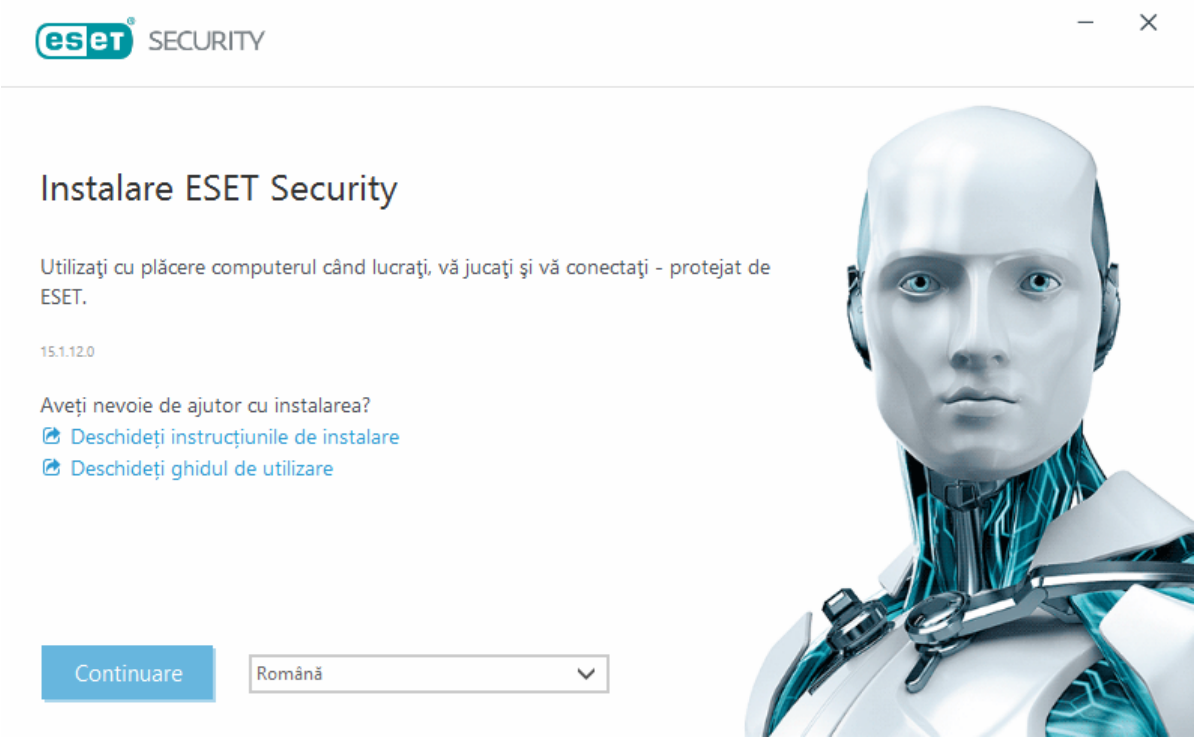
- Instalare offline – Utilizează un fișier .exe mai mare decât Live Installer și nu necesită o conexiune la internet sau fișiere suplimentare pentru a finaliza instalarea.

Înainte de a instala ESET NOD32 Antivirus, asigurați-vă că pe computer nu mai sunt instalate alte programe antivirus. Dacă pe același computer sunt instalate două sau mai multe soluții antivirus, acestea pot intra în conflict. Vă recomandăm să dezinstalați orice alte programe antivirus de pe sistemul dvs. Consultați articolul din Baza de cunoștințe ESET pentru lista instrumentelor de dezinstalare a celor mai cunoscute software-uri antivirus (disponibil în limba engleză și alte câteva limbi).

Program de instalare în direct

După ce ați descărcat pachetul de instalare Live Installer, faceți clic dublu pe fișierul de instalare și urmați instrucțiunile pas cu pas din Expertul de instalare.

Pentru acest tip de instalare trebuie să aveți o conexiune la Internet.



1. Selectați limba dorită în meniul vertical și faceți clic pe **Continuare**.

Dacă instalați o versiune mai recentă decât versiunea anterioară cu setări protejate prin parolă, tastați parola. Puteți configura parola pentru setări în Setare acces.

2. Selectați preferința pentru următoarele funcționalități, citiți Acordul de licență pentru utilizatorul final și Politica de confidențialitate și faceți clic pe **Continuare** sau faceți clic pe **Permiteți toate și continuați** pentru a activa toate funcționalitățile:

- Sistem de feedback ESET LiveGrid®
- Aplicații potențial nedorite
- Programul de îmbunătățire a experienței clienților

> Făcând clic pe **Continuare** sau pe **Permiteți toate și continuați**, acceptați Acordul de licență pentru utilizatorul final și confirmați Politica de confidențialitate.

3. Pentru a activa, a administra și a vizualiza securitatea dispozitivului folosind ESET HOME, conectați dispozitivul la contul ESET HOME. Faceți clic pe **Omitere conectare** pentru a continua fără a vă conecta la ESET HOME. Vă puteți conecta ulterior dispozitivul la contul ESET HOME.

4. Dacă continuați fără a vă conecta la ESET HOME, alegeți o opțiune de activare. Dacă instalați o versiune mai recentă peste una anterioară, cheia de licență va fi introdusă în mod automat.

5. Expertul instalare determină ce produs ESET este instalat pe baza licenței. Versiunea cu cele mai multe caracteristici de securitate este întotdeauna pre-selectată. Faceți clic pe **Schimbați produsul** dacă doriți să instalați o altă versiune a produsului ESET. Faceți clic pe **Continuare** pentru a începe procesul de instalare. Această acțiune poate dura câteva momente.

> Dacă există resturi (fișiere sau foldere) din produsele ESET dezinstalate în trecut, vi se va solicita să permiteți ștergerea acestora. Faceți clic pe **Instalare** pentru a continua.

6. Faceți clic pe **Efectuat pentru** a părăsi Expertul de instalare.

Depanator de instalare.

> După ce produsul este instalat și activat, începe descărcarea modulelor. Protecția este inițializată și este posibil ca anumite caracteristici să nu fie complet funcționale decât după finalizarea descărcării.

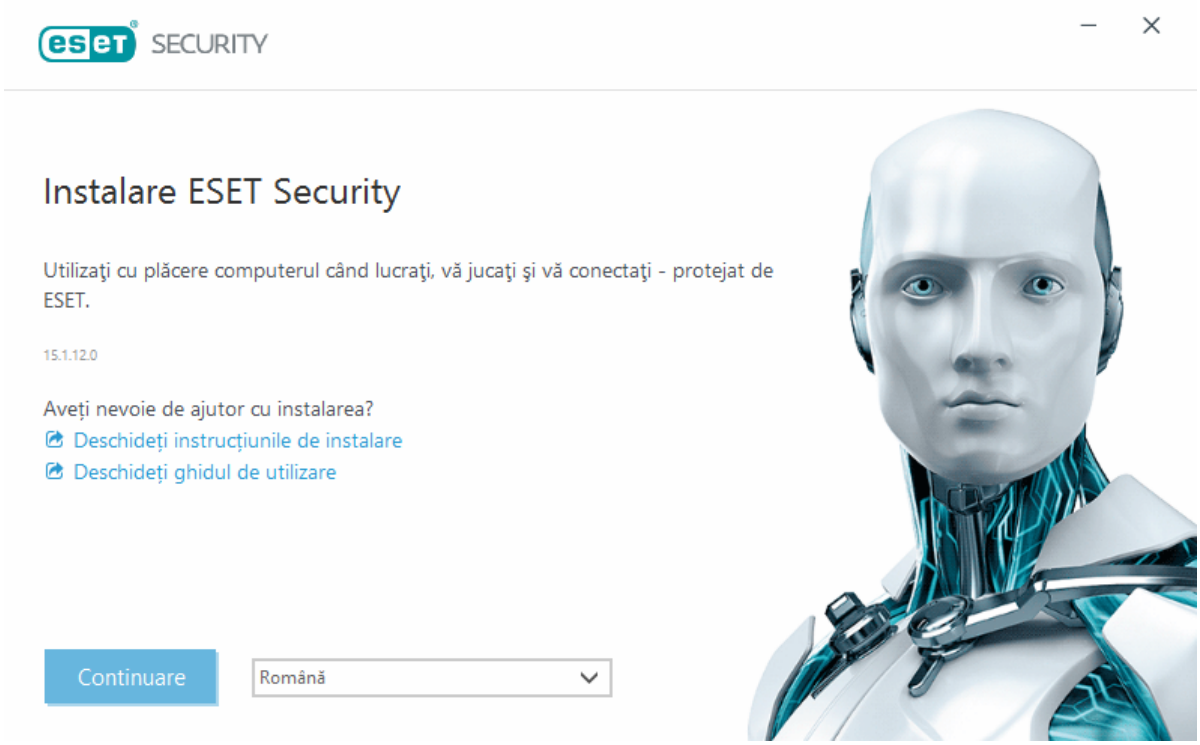
Instalare offline

Descărcați și instalați produsul ESET Windows Home utilizând programul de instalare offline (.exe) de mai jos. Selectați ce versiune de produs ESET HOME să descărcați (pe 32 de biți, pe 64 de biți sau ARM).

ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Descărcare versiune pe 64 de biți Descărcare versiune pe 32 de biți Descărcare ARM	Descărcare versiune pe 64 de biți Descărcare versiune pe 32 de biți Descărcare ARM	Descărcare versiune pe 64 de biți Descărcare versiune pe 32 de biți Descărcare ARM

> Dacă aveți o conexiune la internet activă, instalați produsul ESET utilizând un Live Installer.

Când lansați fișierul de instalare offline (.exe), Expertul de instalare vă ghidează prin procesul de configurare.



1. Selectați limba dorită în meniul vertical și faceți clic pe **Continuare**.

Dacă instalați o versiune mai recentă decât versiunea anterioară cu setări protejate prin parolă, tastați parola. Puteți configura parola pentru setări în Setare acces.

2. Selectați preferința pentru următoarele funcționalități, citiți Acordul de licență pentru utilizatorul final și Politica de confidențialitate și faceți clic pe **Continuare** sau faceți clic pe **Permiteți toate și continuați** pentru a activa toate funcționalitățile:

- Sistem de feedback ESET LiveGrid®
- Aplicații potențial nedorite
- Programul de îmbunătățire a experienței clienților

Făcând clic pe **Continuare** sau pe **Permiteți toate și continuați**, acceptați Acordul de licență pentru utilizatorul final și confirmați Politica de confidențialitate.

3. Faceți clic pe **Omitere conectare**. Când aveți o conexiune la internet, puteți să vă conectați dispozitivul la contul ESET HOME.

4. Faceți clic pe **Omiteți activarea**. ESET NOD32 Antivirus trebuie să fie activat după instalare pentru a fi complet funcțional. Activarea produsului necesită o conexiune activă la internet.

5. Expertul de instalare arată ce produs ESET va fi instalat în funcție de programul de instalare offline descărcat. Faceți clic pe **Continuare** pentru a începe procesul de instalare. Această acțiune poate dura câteva momente.

Dacă există resturi (fișiere sau foldere) din produsele ESET dezinstalate în trecut, vi se va solicita să permiteți ștergerea acestora. Faceți clic pe **Instalare** pentru a continua.

6. Faceți clic pe **Efectuat pentru** a părăsi Expertul de instalare.

Depanator de instalare.

Activare produs

Există mai multe metode disponibile pentru a activa produsul. Disponibilitatea unei anumite situații de activare în fereastra de activare poate depinde de țară și de mijloacele de distribuire (CD/DVD, pagina Web ESET etc.):

- Dacă ați achiziționat o versiune cu amănuntul ambalată în cutie sau ați primit un e-mail cu detaliile licenței, activați produsul făcând clic pe **Folosiți o cheie de licență cumpărată**. Cheia de licență este furnizată, în mod normal, pe spatele ambalajului produsului. Pentru o activare cu succes, cheia de licență trebuie introdusă așa cum a fost furnizată. Cheie de licență – un șir unic în formatul XXXX-XXXX-XXXX-XXXX-XXXX sau XXXX-XXXXXXXX care este utilizat pentru identificarea deținătorului licenței și activarea licenței.

- După ce selectați Utilizare cont ESET HOME, vi se va solicita să vă conectați la contul dvs. ESET HOME.

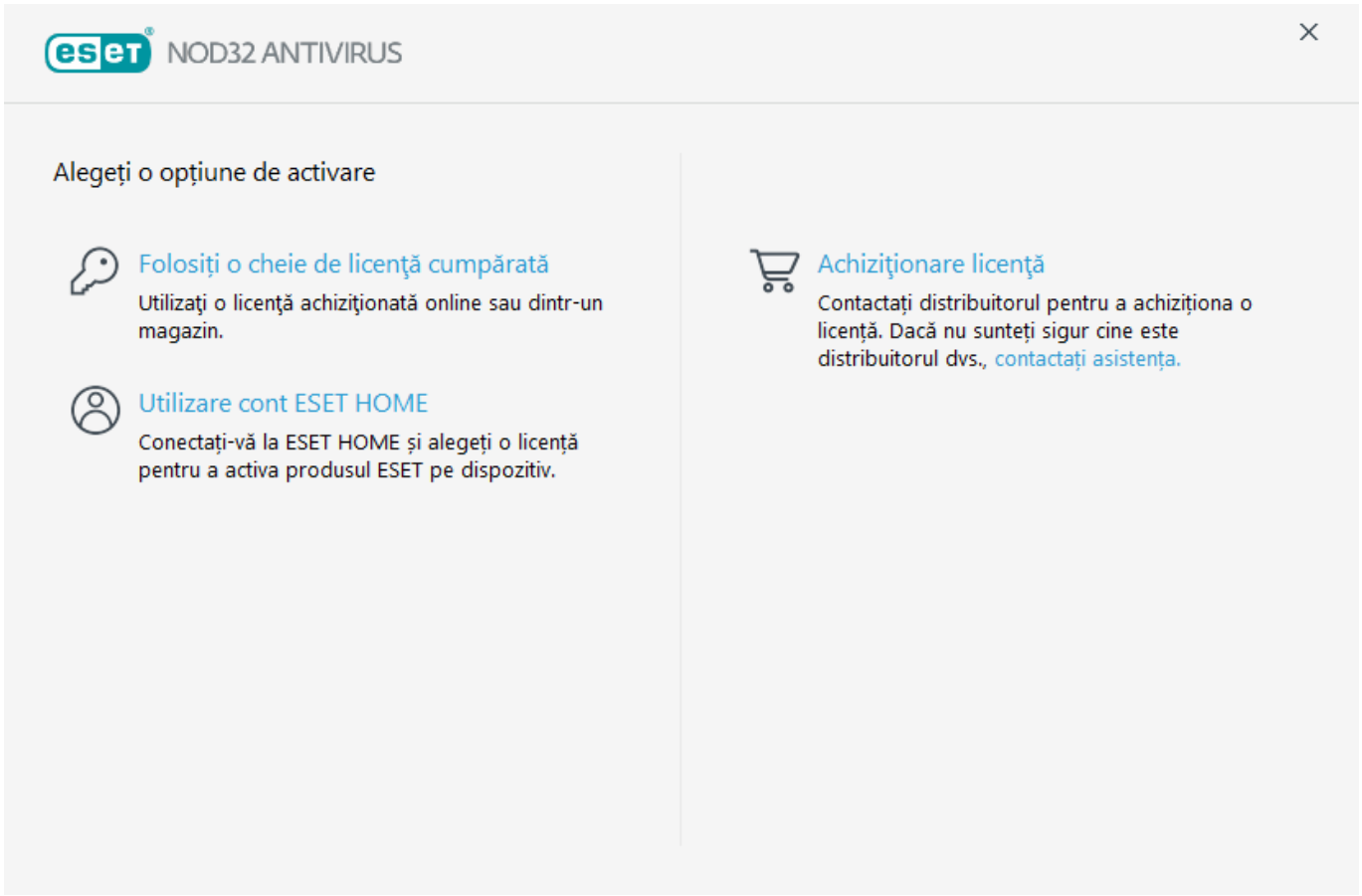
- Dacă doriți să evaluați ESET NOD32 Antivirus înainte de achiziție, selectați Versiune gratuită de încercare. Introduceți adresa de email și țara dvs. pentru a activa ESET NOD32 Antivirus pentru o perioadă limitată. Licența de testare vi se va trimite într-un mesaj de email. Licențele versiunilor de încercare se pot activa o singură dată pentru fiecare client.

- Dacă nu dețineți o licență și doriți să cumpărați una, faceți clic pe **Achiziționare licență**. Astfel veți fi redirecționat la site-ul Web al distribuitorului local ESET. Licențele complete pentru produsele ESET Windows Home nu sunt gratuite.

Puteți schimba oricând licența produsului. Pentru aceasta, faceți clic pe **Ajutor și suport** > **Schimbare licență** în fereastra principală a produsului. Veți vedea ID-ul licenței publice utilizat pentru identificarea licenței dvs. la Asistență ESET.

Dacă aveți un nume de utilizator și o parolă folosite pentru activarea produselor ESET mai vechi și nu știți cum să activați ESET NOD32 Antivirus, faceți conversia acreditărilor moștenite într-o cheie de licență.

Activarea produsului nu a reușit?



Introducerea cheii de licență în cursul activării

Actualizările automate sunt importante pentru securitatea dvs. ESET NOD32 Antivirus va primi actualizări numai după ce este activat.

Atunci când introduceți **cheia de licență**, este important să o tastați exact așa cum este scrisă:

- Cheia de licență este un șir unic în formatul XXXX-XXXX-XXXX-XXXX-XXXX, care este utilizat pentru identificarea deținătorului licenței și activarea licenței.

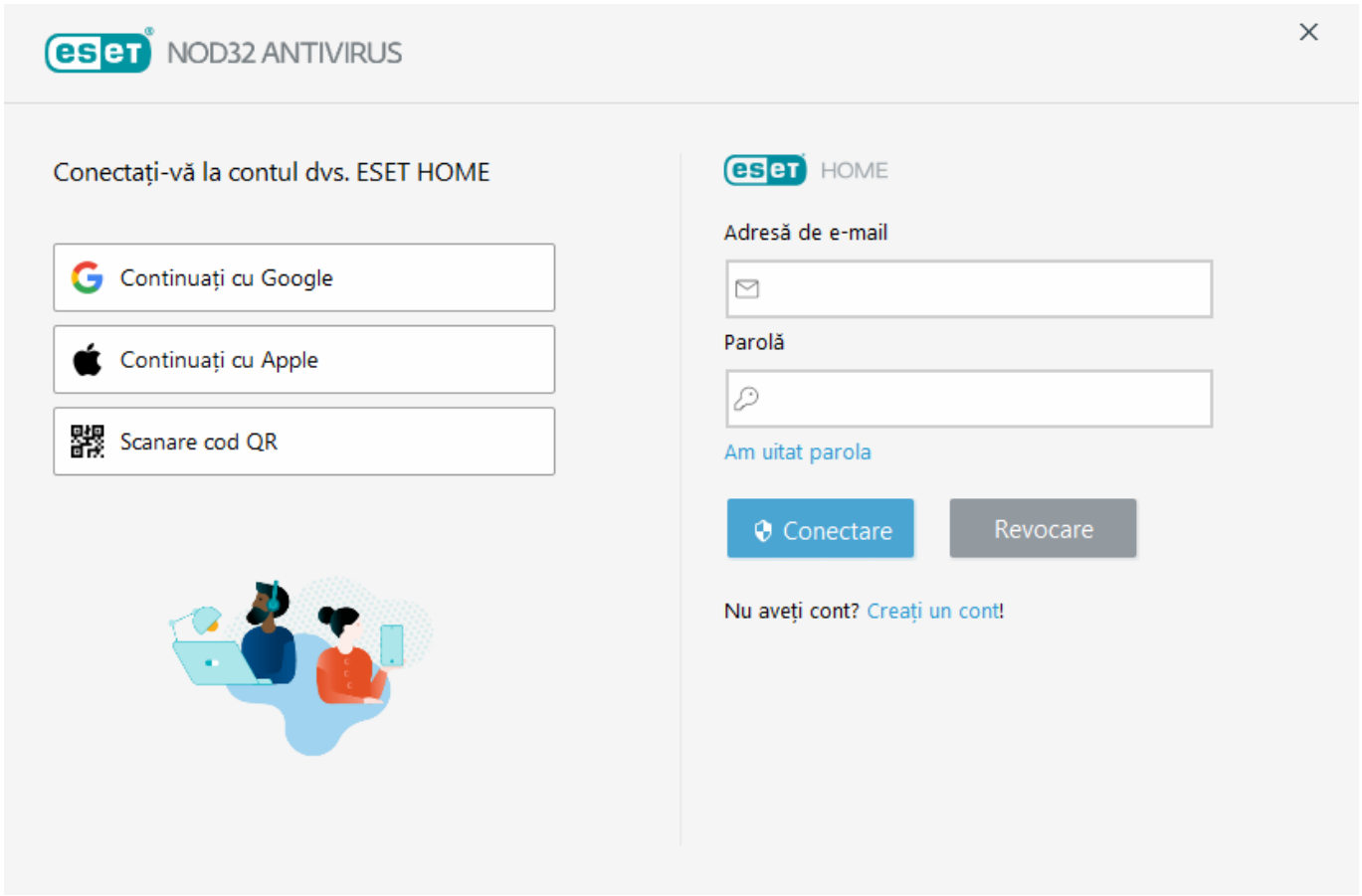
Vă recomandăm să copiați cheia de licență din mesajul de email de înregistrare și să o lipiți pentru a asigura acuratețea.

Dacă nu ați introdus cheia de licență după instalare, produsul nu va fi activat. Puteți activa ESET NOD32 Antivirus în fereastra principală a programului > **Ajutor și suport** > **Activare licență**.

Licențele complete pentru produsele ESET Windows Home nu sunt gratuite.

Utilizare ESET HOME cont

Conectați-vă dispozitivul la ESET HOME pentru a vizualiza și a gestiona toate licențele și dispozitivele ESET activate. Puteți să reînnoiți, să faceți upgrade sau să extindeți licența și să vedeți detalii importante despre licență. În portalul de administrare ESET HOME sau în aplicația mobilă, puteți să adăugați licențe diferite, să descărcați produse pe dispozitive, să verificați starea de securitate a produsului sau să partajați licențe prin e-mail. Pentru mai multe informații, vizitați paginile de Ajutor online ESET HOME.



După ce selectați **Utilizare cont ESET HOME** ca metodă de activare sau când vă conectați la contul ESET HOME în timpul instalării:

1. Conectați-vă la contul dvs. ESET HOME.

> Dacă nu aveți un cont ESET HOME, faceți clic pe **Creare cont** pentru a vă înregistra sau consultați instrucțiunile din secțiunea de ajutor online ESET HOME.
> Dacă v-ați uitat parola, faceți clic pe **Am uitat parola** și urmați pașii de pe ecran sau consultați instrucțiunile din secțiunea de ajutor online ESET HOME.

2. Setați un **nume de dispozitiv** pentru dispozitiv (numele va fi utilizat în toate serviciile ESET HOME) și faceți clic pe **Continuare**.

3. Alegeți o licență pentru activare sau adăugați o licență nouă. Faceți clic pe **Continuare** pentru a activa ESET NOD32 Antivirus.

Activare licență de încercare

Pentru a activa versiunea trial ESET NOD32 Antivirus, introduceți o adresă de email valabilă în câmpurile **Adresă de e-mail** și **Confirmare adresă de e-mail**. După activare, licența ESET se va genera și vă va fi trimisă pe e-mail. Această adresă de e-mail se va mai utiliza pentru notificările privind expirarea produsului și alte comunicări cu ESET. Versiunea trial poate fi activată o singură dată.

Selectați țara în meniul vertical **Țară** pentru a înregistra ESET NOD32 Antivirus la distribuitorul local, care va asigura asistența tehnică.

Cheie de licență ESET gratuită

Licența completă pentru ESET NOD32 Antivirus nu este gratuită.

Cheia de licență ESET este o combinație unică de litere și cifre separate prin liniuță, furnizată de ESET pentru a permite utilizarea legală a ESET NOD32 Antivirus, în conformitate cu Acordul de licență pentru utilizatorul final. Fiecare Utilizator final este dreptul de a folosi Cheia de licență numai în măsura în care are dreptul să utilizeze ESET NOD32 Antivirus, în funcție de numărul de licențe acordate de ESET. Cheia de licență este considerată confidențială și nu poate fi distribuită, dar puteți partaja stațiile din licență folosind ESET HOME.

Este posibil să existe pe internet anumite surse care să vă furnizeze chei de licență „gratuite” pentru produse ESET, dar nu uitați următoarele:

- Când apăsați pe o reclamă „Licență ESET gratuită” vă puteți compromite computerul sau dispozitivul și vă puteți infecta cu malware. Programele malware pot fi ascunse în conținut neoficial de pe web (de exemplu, clipuri video), site-uri web care afișează reclame pentru a câștiga bani în funcție de vizitele dvs. etc. Acestea reprezintă de obicei o capcană.

- ESET poate să dezactiveze licențele piratate și o va face.

- O cheie de licență piratată contravine Acordului de licență pentru utilizatorul final pe care trebuie să-l acceptați pentru a instala ESET NOD32 Antivirus.

- Achiziționați licențe ESET numai folosind canalele oficiale, cum ar fi www.eset.com, distribuitori sau revânzători ESET (nu achiziționați licențe de pe site-uri web terțe neoficiale, cum ar fi eBay, și nu distribuiți licențe de la terți).

- Descărcarea unui produs ESET NOD32 Antivirus este gratuită, dar activarea pe parcursul instalării necesită o cheie de licență ESET validă (puteți descărca și instala produsul, dar acesta nu va funcționa fără activare).

- Nu distribuiți licența dvs. pe internet sau pe canale de socializare media, deoarece s-ar putea răspândi.

Pentru a identifica și a raporta o licență ESET piratată, vizitați articolul din Baza noastră de cunoștințe pentru instrucțiuni.

Dacă nu sunteți convins să achiziționați un produs ESET Security, puteți folosi o versiune trial până când vă decideți:

1. Activați ESET NOD32 Antivirus folosind o licență pentru versiunea gratuită de încercare
2. Participați în in Programul ESET BETA
3. Instalați gratuit ESET Mobile Security, dacă folosiți un dispozitiv mobil Android.

Pentru a obține o reducere sau a vă extinde licența:

- Recomandați ESET NOD32 Antivirus unui prieten
- Reînnoiți produsul ESET (dacă anterior ați avut o licență activă) sau activați-l pentru o perioadă mai lungă

Activarea nu a reușit - scenarii comune

Dacă activarea ESET NOD32 Antivirus nu reușește, cele mai frecvente scenarii sunt:

- Cheia de licență este deja în uz
- Cheie de licență nevalidă. Eroare a formei de activare a produsului
- Informațiile suplimentare necesare activării lipsesc sau nu sunt valide.
- Nu s-a reușit comunicarea cu baza de date a activării. Încercați să activați din nou în 15 minute.
- Lipsă conexiune sau conexiune dezactivată la servere de activare ESET

Verificați dacă ați introdus cheia de licență corespunzătoare și încercați să o activați din nou. Dacă folosiți contul ESET HOME pentru activare, consultați Administrarea licențelor ESET HOME – Ajutor online.

Dacă în continuare nu puteți activa licența, Depanatorul privind activarea ESET vă va însoți printre întrebări, erori și probleme obișnuite legate de activare și licențiere (este disponibil în limba engleză și în alte câteva limbi).

Activarea nu a reușit din cauza licenței cu limită de utilizare depășită

Problemă

- Licența dumneavoastră este posibil să aibă o limită de utilizare depășită sau să fie abuzată
- Activarea nu a reușit din cauza licenței cu limită de utilizare depășită

Rezolvare

Există mai multe dispozitive decât permite licența. Puteți fi victima pirateriei software sau a unui produs contrafăcut. Această licență nu poate fi utilizată pentru a activa alte produse ESET. Puteți rezolva această problemă direct dacă aveți permisiunea de a gestiona licența în contul ESET HOME sau ați achiziționat licența de la o sursă legitimă. Dacă nu aveți încă un cont, creați unul.

Dacă sunteți un proprietar de licență și nu vi s-a solicitat să introduceți adresa de e-mail:

1. Pentru a vă administra licența ESET, deschideți un browser web și navigați la https://home.eset.com. Accesați ESET License Manager pentru a elimina sau a dezactiva stații. Pentru mai multe informații, consultați secțiunea Ce să faceți în cazul unei licențe cu limită de utilizare depășită.

2. Pentru a identifica și a raporta o licență ESET piratată, vizitați articolul nostru Identificarea și raportarea licențelor ESET piratate pentru instrucțiuni.

3. Dacă nu sunteți sigur, faceți clic pe **Înapoi** și trimiteți un e-mail Asistenței tehnice ESET.

Dacă nu sunteți proprietarul licenței, contactați proprietarul licenței și spuneți-i că nu puteți activa produsul ESET din cauza depășirii limitei de utilizare. Proprietarul poate rezolva problema în portalul ESET HOME.

Dacă vi se solicită (în rare cazuri) să vă confirmați adresa de e-mail, introduceți adresa de e-mail folosită inițial pentru achiziția sau activarea produsului ESET NOD32 Antivirus.

Upgrade licență

Această fereastră de notificare apar atunci când licența utilizată pentru activarea produsului ESET s-a modificat. Licența modificată vă permite să activați un produs cu mai multe caracteristici de securitate. Dacă nu s-a efectuat nicio modificare, ESET NOD32 Antivirus va afișa o fereastră de avertizare o singură dată, denumită **Treceți la un produs cu mai multe funcționalități**.

Da (recomandat) – se va instala automat produsul cu mai multe caracteristici de securitate.

Nu, mulțumesc – nu se vor face modificări, iar notificarea va dispărea definitiv.

Pentru a modifica produsul mai târziu, consultați articolul nostru din baza de cunoștințe ESET. Pentru informații suplimentare despre licențele ESET, consultați Întrebări frecvente despre licențiere.

Tabelul de mai jos descrie caracteristicile disponibile în fiecare produs specific.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Motor de detecție	✔	✔	✔
Învățare programată avansată	✔	✔	✔
Blocare exploit-uri	✔	✔	✔
Protecție împotriva atacurilor bazate pe scripturi	✔	✔	✔
Anti-Phishing	✔	✔	✔
Protecție acces Web	✔	✔	✔
HIPS (inclusiv Ransomware Shield)	✔	✔	✔
Antispam		✔	✔
Protecție firewall		✔	✔
Inspector de rețea		✔	✔
Protecție camere Web		✔	✔
Protecție împotriva atacurilor de rețea		✔	✔
Protecție Botnet		✔	✔
Protecție plăți prin bancă		✔	✔
Control parental		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Upgrade produs

Ați descărcat un program de instalare implicit și ați decis să modificați produsul pentru a fi activat sau doriți să modificați produsul instalat într-unul cu mai multe caracteristici de securitate.

Schimbați produsul în timpul instalării.

Tabelul de mai jos descrie caracteristicile disponibile în fiecare produs specific.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Motor de detecție	✔	✔	✔
Învățare programată avansată	✔	✔	✔
Blocare exploit-uri	✔	✔	✔
Protecție împotriva atacurilor bazate pe scripturi	✔	✔	✔
Anti-Phishing	✔	✔	✔
Protecție acces Web	✔	✔	✔
HIPS (inclusiv Ransomware Shield)	✔	✔	✔
Antispam		✔	✔
Protecție firewall		✔	✔
Inspector de rețea		✔	✔
Protecție camere Web		✔	✔
Protecție împotriva atacurilor de rețea		✔	✔
Protecție Botnet		✔	✔
Protecție plăți prin bancă		✔	✔
Control parental		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Downgrade licență

Această fereastră de dialog apare atunci când licența utilizată pentru activarea produsului ESET s-a modificat. Licența dvs. modificată poate fi utilizată numai cu alte produse ESET, cu mai puține funcționalități de securitate. Produsul a fost modificat automat, pentru a preveni pierderea protecției.

Pentru informații suplimentare despre licențele ESET, consultați Întrebări frecvente despre licențiere.

Tabelul de mai jos descrie caracteristicile disponibile în fiecare produs specific.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Motor de detecție	✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Învățare programată avansată	✔	✔	✔
Blocare exploit-uri	✔	✔	✔
Protecție împotriva atacurilor bazate pe scripturi	✔	✔	✔
Anti-Phishing	✔	✔	✔
Protecție acces Web	✔	✔	✔
HIPS (inclusiv Ransomware Shield)	✔	✔	✔
Antispam		✔	✔
Protecție firewall		✔	✔
Inspector de rețea		✔	✔
Protecție camere Web		✔	✔
Protecție împotriva atacurilor de rețea		✔	✔
Protecție Botnet		✔	✔
Protecție plăți prin bancă		✔	✔
Control parental		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Downgrade produs

Produsul pe care-l aveți instalat în prezent are mai multe caracteristici de securitate decât cel pe care sunteți pe cale să-l activați.

Tabelul de mai jos descrie caracteristicile disponibile în fiecare produs specific.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Motor de detecție	✔	✔	✔
Învățare programată avansată	✔	✔	✔
Blocare exploit-uri	✔	✔	✔
Protecție împotriva atacurilor bazate pe scripturi	✔	✔	✔
Anti-Phishing	✔	✔	✔
Protecție acces Web	✔	✔	✔
HIPS (inclusiv Ransomware Shield)	✔	✔	✔
Antispam		✔	✔
Protecție firewall		✔	✔
Inspector de rețea		✔	✔
Protecție camere Web		✔	✔
Protecție împotriva atacurilor de rețea		✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Protecție Botnet		✔	✔
Protecție plăți prin bancă		✔	✔
Control parental		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Depanator de instalare

Dacă apar probleme în timpul instalării, Expertul de instalare vă pune la dispoziție un depanator care rezolvă problema, dacă este posibil.

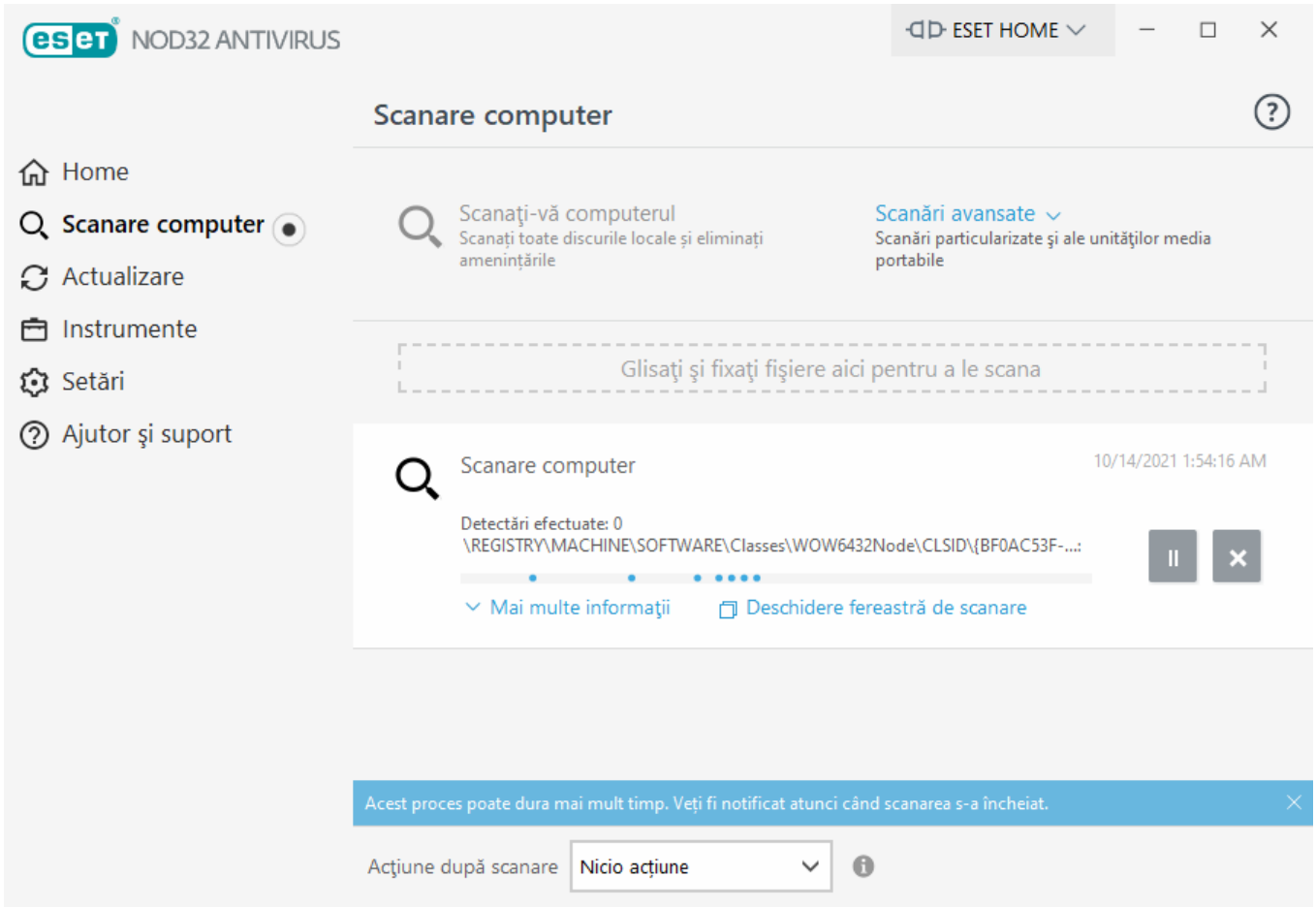
Faceți clic pe **Executați depanatorul** pentru a lansa depanatorul. Când depanatorul încheie procesul, urmați soluția recomandată.

Dacă problema persistă, consultați lista de erori de instalare uzuale și rezolvări.

Prima scanare după instalare

După instalarea produsului ESET NOD32 Antivirus, o scanare a computerului va porni automat după prima actualizare reușită pentru a verifica existența codurilor dăunătoare.

De asemenea, puteți porni manual o scanare a computerului din fereastra principală a programului făcând clic pe **Scanare computer** > **Scanați computerul**. Pentru informații suplimentare despre scanările computerului, consultați secțiunea Scanare computer.



Efectuarea de upgrade la o versiune mai recentă

Versiunile noi ale produsului ESET NOD32 Antivirus sunt publicate pentru a implementa îmbunătățiri sau pentru a rezolva probleme care nu pot fi rezolvate prin actualizări automate ale modulelor de program. Upgrade-ul la o versiune mai recentă se poate realiza în mai multe moduri:

1. Automat, prin intermediul unei actualizări a programului.
Deoarece upgrade-ul programului se distribuie tuturor utilizatorilor și pot afecta anumite configurații de sistem, acesta este publicat după o perioadă lungă de testare pentru a asigura funcționarea cu toate configurațiile de sistem posibile. Dacă doriți să efectuați upgrade la o versiune mai nouă imediat după publicarea acesteia, utilizați una dintre metodele de mai jos.
Asigurați-vă că ați activat opțiunea **Actualizări ale funcționalităților aplicației** în **Setare avansată** (F5) > **Actualizare** > **Profiluri** > **Actualizări**.

2. Manual, în fereastra principală a programului, făcând clic pe **Căutare actualizări** în secțiunea **Actualizare**.

3. Manual, prin descărcarea și instalarea unei versiuni mai recente peste cea anterioară.

Pentru informații suplimentare și instrucțiuni ilustrate, consultați:

- Actualizarea produselor ESET: verificați cele mai recente module de produs
- Care sunt diferitele tipuri de actualizări și lansări de produse ESET?

Upgrade-ul automat pentru un produs moștenit

Versiunea produsului ESET pe care o aveți nu mai este acceptată și am făcut upgrade la cea mai recentă versiune produsului dvs.

Probleme frecvente la instalare

Fiecare nouă versiune de produse ESET include multe remedieri de erori și îmbunătățiri. Clienții existenți cu o licență validă pentru un produs ESET pot face în mod gratuit upgrade la cea mai recentă versiune a aceluiași produs.

Pentru a finaliza instalarea:

1. Faceți clic pe **Acceptați și continuați** pentru a accepta Acordul de licență pentru utilizatorul final și a confirma Politica de confidențialitate. Dacă nu sunteți de acord cu Acordul de licență pentru utilizatorul final, faceți clic pe **Dezinstalare**. Nu este posibilă revenirea la versiunea anterioară.

2. Faceți clic pe **Permiteți toate și continuați** pentru a permite atât sistemul de feedback ESET LiveGrid®, cât și Programul de îmbunătățire a experienței clienților sau faceți clic pe **Continuare** dacă nu doriți să participați.

3. După activarea noului produs ESET cu cheia de licență, va fi afișată pagina Home. Dacă informațiile despre licență nu sunt găsite, veți continua cu o nouă licență trial. Dacă licența utilizată în produsul anterior nu este validă, activați produsul ESET.

4. Pentru finalizarea instalării este necesară o repornire a dispozitivului.

Recomandați produsul ESET unui prieten

În prezent, această versiune a ESET NOD32 Antivirus oferă bonusuri pentru recomandări, pentru a putea împărtăși experiența dumneavoastră cu produsele ESET cu familia sau prietenii dumneavoastră. Puteți trimite recomandări și dintr-un produs activat cu o licență de încercare. Dacă sunteți utilizator al unei versiuni de încercare, pentru fiecare recomandare care va genera o activare de produs, atât dumneavoastră, cât și prietenul respectiv veți primi timp suplimentar pentru licența de încercare.

Puteți transmite o recomandare folosind ESET NOD32 Antivirus instalat de dumneavoastră. Produsul pe care îl puteți recomanda depinde de produsul pe care l-ați instalat, conform tabelului de mai jos.

Produsul instalat de dumneavoastră	Produsul pe care îl puteți recomanda
ESET NOD32 Antivirus	ESET Internet Security
ESET Internet Security	ESET Internet Security
ESET Smart Security Premium	ESET Smart Security Premium

Recomandarea unui produs

Pentru a transmite un link de recomandare, faceți clic pe **Recomandați un prieten** din meniul principal al ESET NOD32 Antivirus. Faceți clic pe **Trimiteți link de partajare**. Produsul va genera un link de recomandare care va fi afișat într-o fereastră nouă. Copiați linkul și trimiteți-l familiei și prietenilor. Puteți partaja linkul de recomandare direct din produsul ESET, folosind opțiunile **Partajare pe Facebook**, **Recomandați contactelor dumneavoastră**

Gmail și **Partajare pe Twitter**.

Atunci când un prieten face clic pe linkul de recomandare trimis, va fi redirecționat spre o pagină web de unde va putea descărca produsul și îl va putea folosi pentru o lună de protecție GRATUITĂ. Ca utilizator al unei versiuni de încercare, pentru fiecare link de recomandare activat cu succes veți primi o notificare, iar licența vă va fi extinsă automat pentru încă o lună de protecție GRATUITĂ. Astfel vă puteți prelungi protecția GRATUITĂ cu până la 5 luni. Puteți verifica numărul de linkuri de recomandare activate cu succes în fereastra **Recomandați un prieten** a produsului ESET.

Caracteristica Referință este posibil să nu fie disponibilă pentru limba/regiunea dvs.

Se va instala ESET NOD32 Antivirus

Această fereastră de dialog poate fi afișată:

- În timpul procesului de instalare – Faceți clic pe **Continuare** pentru a instala ESET NOD32 Antivirus.
- Când schimbați o licență în ESET NOD32 Antivirus – Faceți clic pe **Activare** pentru a modifica licența și a activa ESET NOD32 Antivirus.

Opțiunea **Modificare produs** vă permite să comutați între diferitele produse ESET Windows Home, în conformitate cu licența dvs. Consultați Ce produs am? pentru informații suplimentare.

Treceți la o altă gamă de produse

ESET, puteți să comutați între diferite produse ESET Windows Home. Consultați Ce produs am? pentru informații suplimentare.

Înregistrare

Înregistrați-vă licența completând câmpurile din formularul de înregistrare și făcând clic pe Activare. Câmpurile marcate ca necesare în paranteze sunt obligatorii. Aceste informații vor fi utilizate numai pentru aspecte legate de licența dvs. Aceste informații vor fi utilizate numai pentru aspecte legate de licența dvs. ESET.

Progres activare

Așteptați câteva secunde finalizarea procesului de activare (timpul necesar poate varia în funcție de viteza conexiunii la internet sau de computer).

Activare reușită

S-a terminat procesul de activare.

O actualizare de modul va începe în câteva secunde. Actualizările periodice pentru ESET NOD32 Antivirus vor începe imediat.

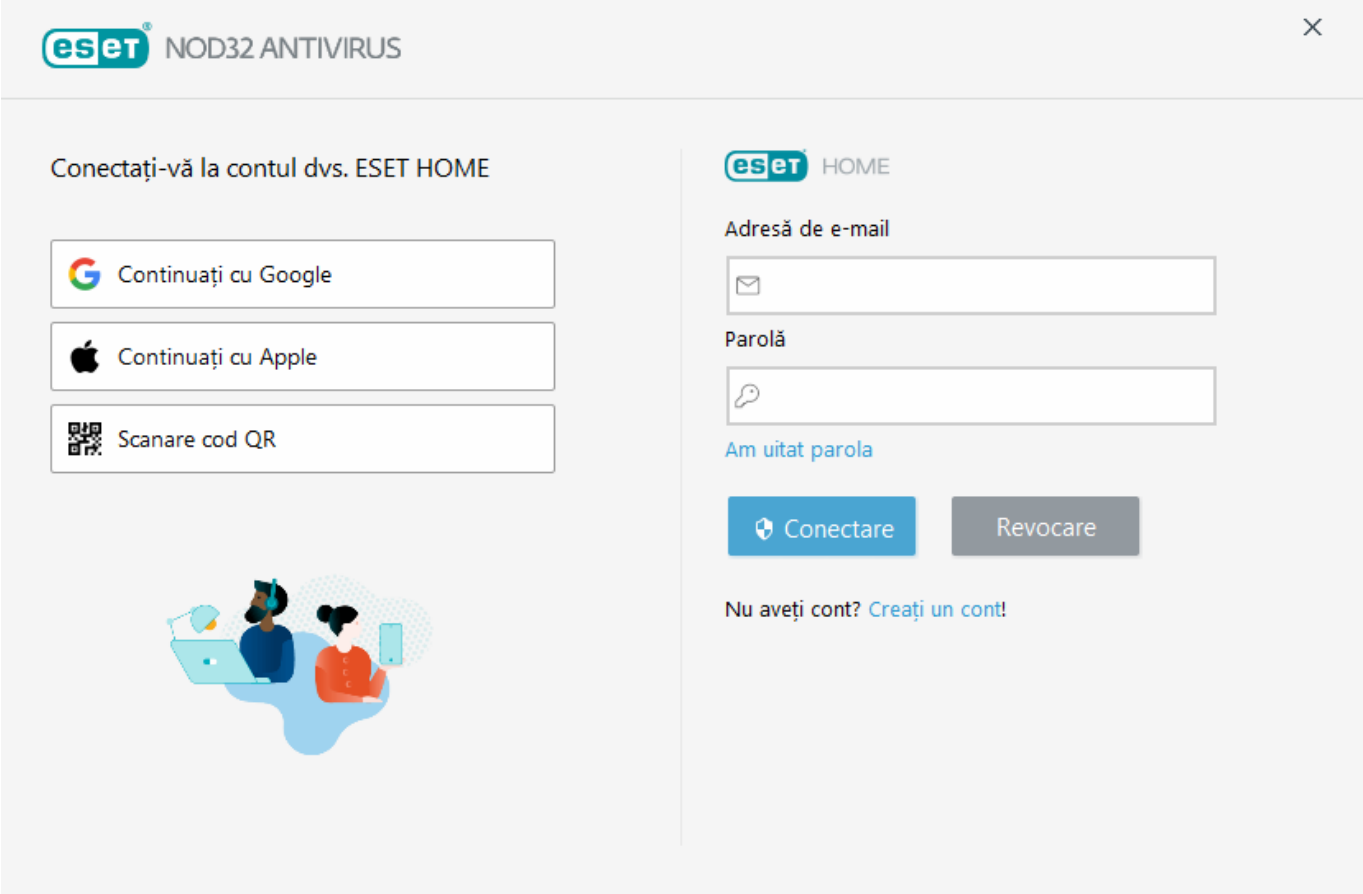
O scanare inițială va începe automat în 20 de minute de la actualizarea de modul.

Ghidul începătorului

Acest capitol oferă o prezentare generală inițială pentru ESET NOD32 Antivirus și pentru setările sale de bază.

Conectați-vă la ESET HOME

Conectați-vă dispozitivul la ESET HOME pentru a vizualiza și a gestiona toate licențele și dispozitivele ESET activate. Puteți să reînnoiți, să faceți upgrade sau să extindeți licența și să vedeți detalii importante despre licență. În portalul de administrare ESET HOME sau în aplicația mobilă, puteți să adăugați licențe diferite, să descărcați produse pe dispozitive, să verificați starea de securitate a produsului sau să partajați licențe prin e-mail. Pentru mai multe informații, vizitați paginile de Ajutor online ESET HOME.



Pentru a conecta dispozitivul la ESET HOME:

Dacă vă conectați la ESET HOME în timpul instalării sau când selectați opțiunea **Utilizați contul ESET HOME** ca metodă de activare, urmați instrucțiunile din subiectul Utilizați contul ESET HOME.
Dacă ați instalat și activat deja ESET NOD32 Antivirus cu o licență adăugată în contul ESET HOME, vă puteți conecta dispozitivul la ESET HOME folosind portalul ESET HOME. Urmați instrucțiunile din ESET HOME Ghidul de ajutor online și permiteți conexiunea în ESET NOD32 Antivirus.

1. În fereastra principală a programului, faceți clic pe **ESET HOME** > **Conectare la ESET HOME** sau faceți clic pe **Conectare la ESET HOME** în notificarea **Conectați acest dispozitiv la un cont ESET HOME**.

2. Conectați-vă la contul dvs. ESET HOME.

Dacă nu aveți un cont ESET HOME, faceți clic pe **Creare cont** pentru a vă înregistra sau consultați instrucțiunile din secțiunea de ajutor online ESET HOME.
Dacă v-ați uitat parola, faceți clic pe **Am uitat parola** și urmați pașii de pe ecran sau consultați instrucțiunile din secțiunea de ajutor online ESET HOME.

3. Stabiliți un **nume de dispozitiv** și faceți clic pe **Continuare**.

4. După o conexiune reușită, se afișează o fereastră de detalii. Faceți clic pe **Terminat**.

Conectați-vă la ESET HOME

Există mai multe metode disponibile pentru a vă conecta la contul dvs. ESET HOME:

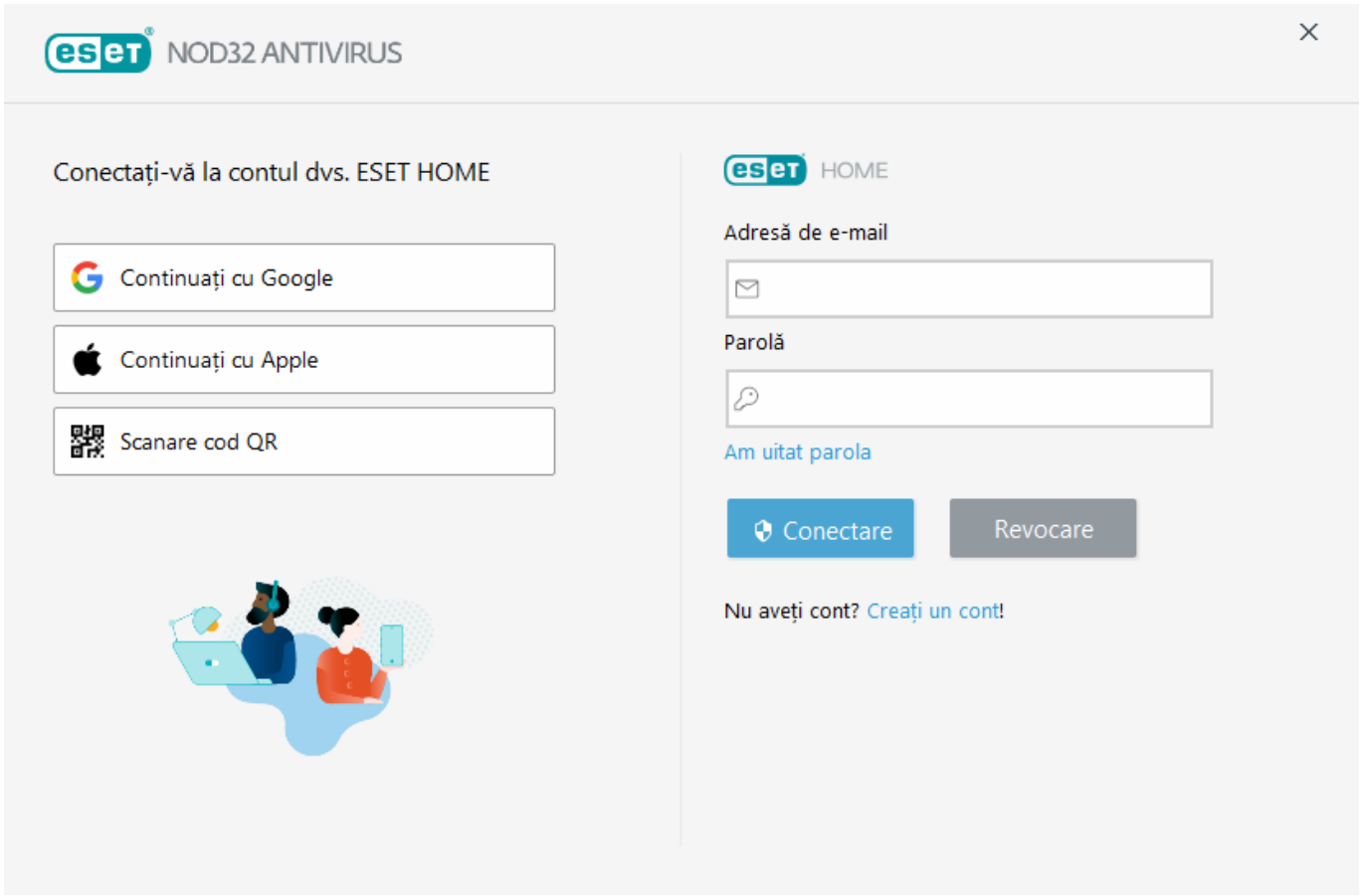
- **Utilizați adresa de e-mail și parola pentru ESET HOME** – Tastați **adresa de e-mail** și **parola** pe care le-ați folosit pentru a crea contul ESET HOME și faceți clic pe **Conectare**.

- **Folosiți contul Google/AppleID** – Faceți clic pe **Continuați cu Google** sau **Continuați cu Apple** și conectați-vă cu contul corespunzător. După conectarea cu succes, veți fi redirecționat către pagina web de confirmare ESET HOME. Pentru a continua, comutați înapoi la fereastra produsului ESET. Pentru mai multe informații despre conectarea cu contul Google/AppleID, consultați instrucțiunile din ESET HOME secțiunea de ajutor online.

- **Scanați codul QR** – Faceți clic pe **Scanare cod QR** pentru a afișa codul QR. Deschideți aplicația mobilă ESET HOME și scanați codul QR sau îndreptați camera dispozitivului spre codul QR. Pentru mai multe informații, consultați instrucțiunile din ESET HOME secțiunea de ajutor online.

Dacă nu aveți un cont ESET HOME, faceți clic pe **Creare cont** pentru a vă înregistra sau consultați instrucțiunile din secțiunea de ajutor online ESET HOME.
Dacă v-ați uitat parola, faceți clic pe **Am uitat parola** și urmați pașii de pe ecran sau consultați instrucțiunile din secțiunea de ajutor online ESET HOME.

Conectarea nu a reușit - erori uzuale.



Conectarea nu a reușit - erori uzuale

Nu am putut găsi un cont care să se potrivească cu adresa de e-mail introdusă

Adresa de e-mail pe care ați introdus-o nu corespunde cu niciun cont ESET HOME. Faceți clic pe **Înapoi** și tastați adresa de e-mail și parola corecte.

Pentru a vă conecta, trebuie să creați un cont ESET HOME. Dacă nu aveți un cont ESET HOME, faceți clic pe **Înapoi** > **Creați un cont** sau consultați secțiunea Crearea unui cont ESET HOME nou.

Numele de utilizator și parola nu se potrivesc

Parola introdusă nu se potrivește cu adresa de e-mail introdusă. Faceți clic pe **Înapoi**, tastați parola corectă și asigurați-vă că adresa de e-mail introdusă este corectă. Dacă tot nu vă puteți conecta, faceți clic pe **Înapoi** > **Am uitat parola** pentru a reseta parola și urmați pașii de pe ecran sau consultați secțiunea Am uitat parola ESET HOME.

Opțiunea de conectare selectată nu se potrivește contului.

Contul dvs. este asociat cu contul dvs. de socializare. Pentru a vă conecta la ESET HOME, faceți clic pe **Continuați cu Google** sau pe **Continuați cu Apple** și conectați-vă la contul corespunzător. După conectarea cu succes, veți fi redirecționat către pagina web de confirmare ESET HOME. Puteți deconecta contul de socializare de la contul ESET HOME pe portalul ESET HOME.

Parolă incorectă

Această eroare poate apărea dacă ESET NOD32 Antivirus este deja conectat la ESET HOME și efectuați modificări care necesită să vă conectați (de exemplu, dezactivarea caracteristicii Anti-Theft) și parola pe care ați introdus-o nu corespunde cu contul dvs. Faceți clic pe **Înapoi** și tastați parola corectă. Dacă tot nu vă puteți conecta, faceți clic pe **Înapoi** > **Am uitat parola** pentru a reseta parola și urmați pașii de pe ecran sau consultați secțiunea Am uitat parola ESET HOME.

Adăugați un dispozitiv în ESET HOME

Dacă ați instalat și activat deja ESET NOD32 Antivirus cu o licență adăugată în contul ESET HOME, vă puteți conecta dispozitivul la ESET HOME folosind portalul ESET HOME:

1. Trimiteți o solicitare de conexiune către dispozitiv.

2. ESET NOD32 Antivirus afișează fereastra de dialog **Conectați acest dispozitiv la un cont ESET HOME**, cu un nume de cont ESET HOME. Faceți clic pe **Permitere** pentru a conecta dispozitivul la contul ESET HOME menționat.

Dacă nu există nicio interacțiune, solicitarea de conectare va fi revocată automat după aproximativ 30 de minute.

Fereastra principală a programului

Fereastra principală a programului ESET NOD32 Antivirus se împarte în două secțiuni de bază. Fereastra principală din dreapta afișează informații care corespund opțiunii selectate în meniul principal din dreapta.

Instrucțiuni ilustrate
Consultați secțiunea Deschiderea ferestrei principale a programului produselor ESET Windows pentru instrucțiuni ilustrate disponibile în limba engleză și în alte câteva limbi.

ESET HOME – Conectați-vă dispozitivul la ESET HOME. Folosiți ESET HOME pentru a vizualiza și a gestiona licențele și dispozitivele ESET activate.

În continuare vă oferim o descriere a opțiunilor din meniul principal:

Acasă – furnizează informații despre starea protecției produsului ESET NOD32 Antivirus.

Scanare computer – configurați și lansați o scanare a computerului sau creați o scanare particularizată.

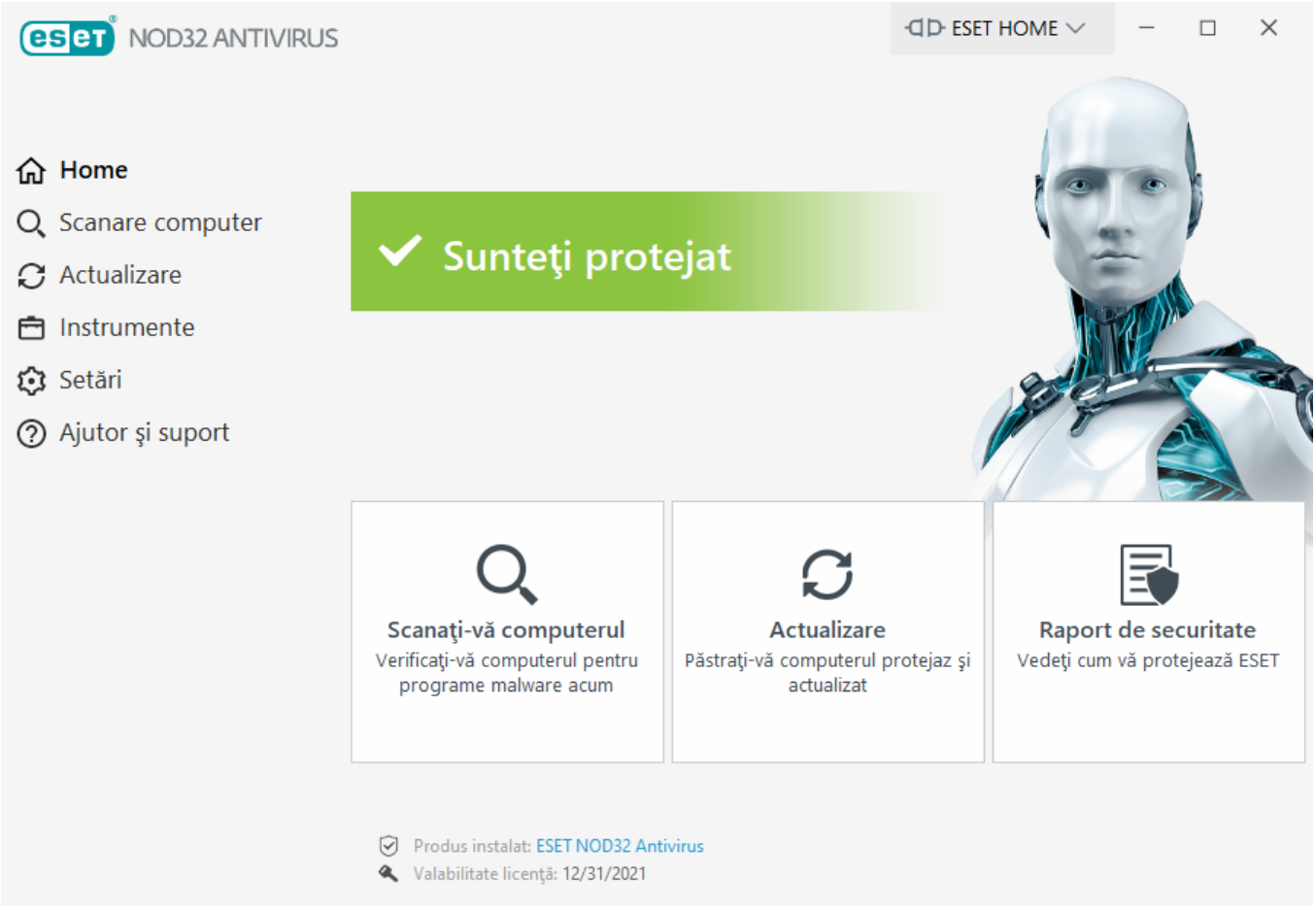
Actualizare – afișează informații despre actualizările motorului de detecție.

Instrumente – Oferă acces la module care ajută la simplificarea administrării programului și oferă opțiuni suplimentare pentru utilizatorii avansați. Pentru mai multe informații, consultați Instrumente în ESET NOD32 Antivirus.

Setare – selectați această opțiune pentru a regla nivelul de securitate pentru Computer, Internet.

Ajutor și suport – asigură acces la fișiere de ajutor, la Baza de cunoștințe ESET, la site-ul Web ESET și legături

pentru trimiterea de solicitări de suport.

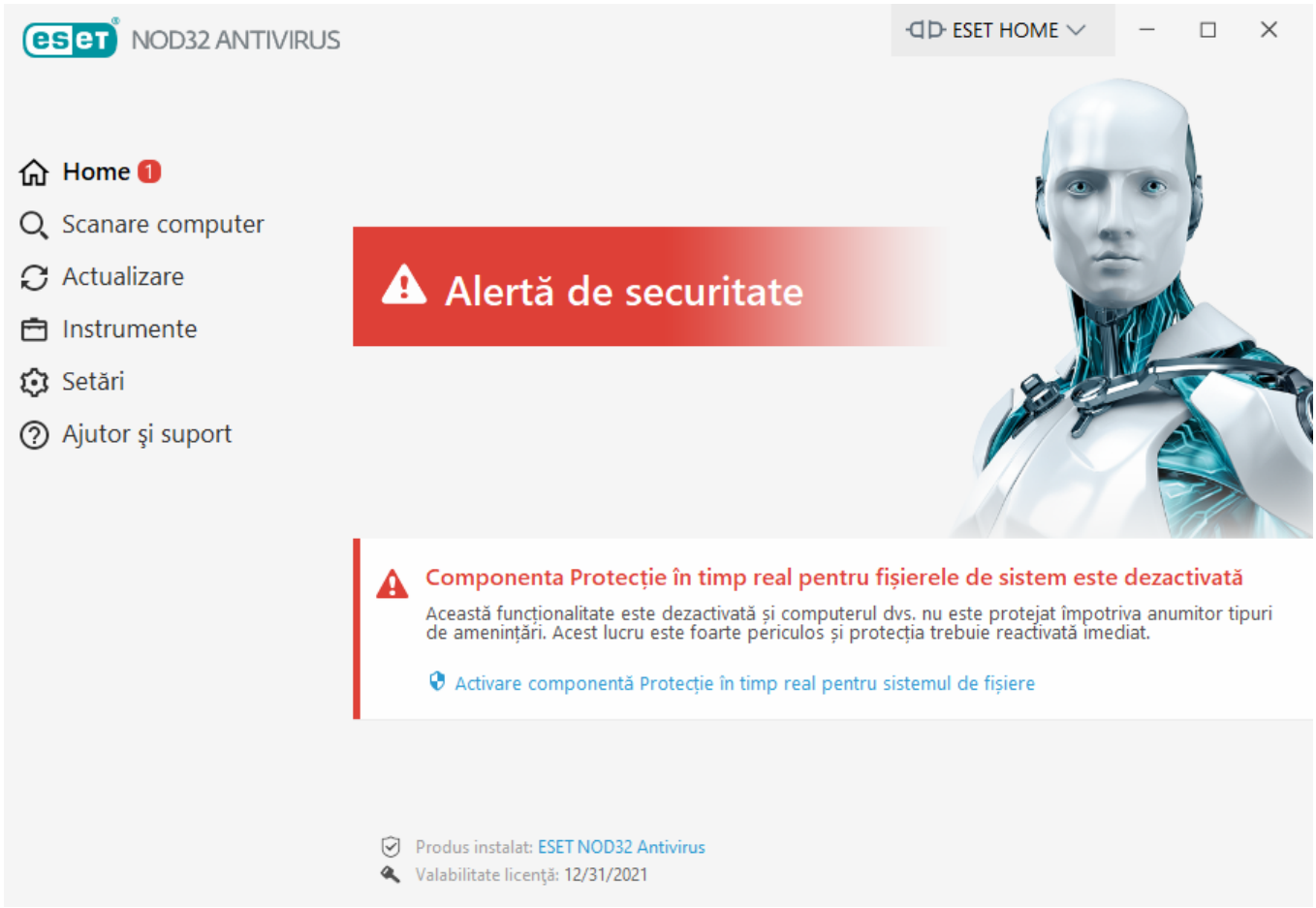


Ecranul de pornire conține informații importante despre nivelul de protecție curent al computerului. Fereastra de stare afișează caracteristicile utilizate frecvent în ESET NOD32 Antivirus. Aici găsiți și informații despre produsul instalat și data de expirare a licenței. Faceți clic pe **ESET NOD32 Antivirus** dacă doriți să instalați o altă versiune a produsului ESET. Informații suplimentare despre caracteristicile din fiecare produs în parte.

Pictograma verde și mesajul de stare **Sunteți protejat**, scris cu culoarea verde, indică faptul că este asigurată protecția maximă.

Ce este de făcut dacă programul nu funcționează corect?

Dacă un modul de protecție activ lucrează normal, pictograma stării sale de protecție va fi verde. Un semn de exclamare roșu sau o pictogramă de notificare portocalie indică faptul că nu s-a asigurat protecția maximă. În panoul **Acasă** se vor afișa informații suplimentare despre starea de protecție a fiecărui modul, precum și soluțiile sugerate pentru restaurarea protecției complete. Pentru a schimba starea fiecărui modul în parte, faceți clic pe **Setare** și selectați modulul dorit.



Pictograma roșie și starea roșie **Alertă de securitate** indică probleme critice.
Iată câteva dintre motivele pentru afișarea acestei stări:

- **Produsul nu a fost activat** sau **Licența a expirat** – Acest lucru este indicat printr-o pictogramă roșie a stării protecției. Programul nu va mai putea face actualizarea după expirarea licenței. Urmați instrucțiunile din fereastra de alertă pentru a reînnoi licența.
- **Motorul de detectare nu este actualizat**– această eroare apare după mai multe încercări nereușite de actualizare a motorului de detectare. Vă recomandăm să verificați setările de actualizare. Cel mai întâlnit motiv al acestei erori este introducerea incorectă a datelor de autentificare sau configurarea incorectă a setărilor conexiunii.
- **Componenta Protecție în timp real pentru sistemul de fișiere este dezactivată** – protecția în timp real pentru sistemul de fișiere a fost dezactivată de către utilizator. Computerul dvs. nu este protejat împotriva amenințărilor. Faceți clic pe **Activare componenta Protecție în timp real pentru sistemul de fișiere** pentru a reactiva această funcționalitate.
- **Protecție antivirus și antispyware dezactivată** – puteți să reactivați protecția antivirus și antispyware făcând clic pe **Activare protecție antivirus și antispyware**.

Pictograma portocalie indică faptul că protecția este limitată. De exemplu, ar putea exista o problemă la actualizarea programului sau este posibil ca licența să se apropie de data expirării.
Iată câteva dintre motivele pentru afișarea acestei stări:

- **Mod Gamer activ** – activarea modului Gamer reprezintă un potențial risc de securitate. Activarea acestei caracteristici dezactivează toate ferestrele pop-up și oprește orice sarcină planificată.
- **Licența va expira în curând** – această problemă este semnalată afișarea unui semn de exclamare pe

pictograma de stare a protecției, lângă ceasul sistemului. După expirarea licenței, programul nu va putea face actualizarea, iar pictograma Stare protecție va deveni roșie.

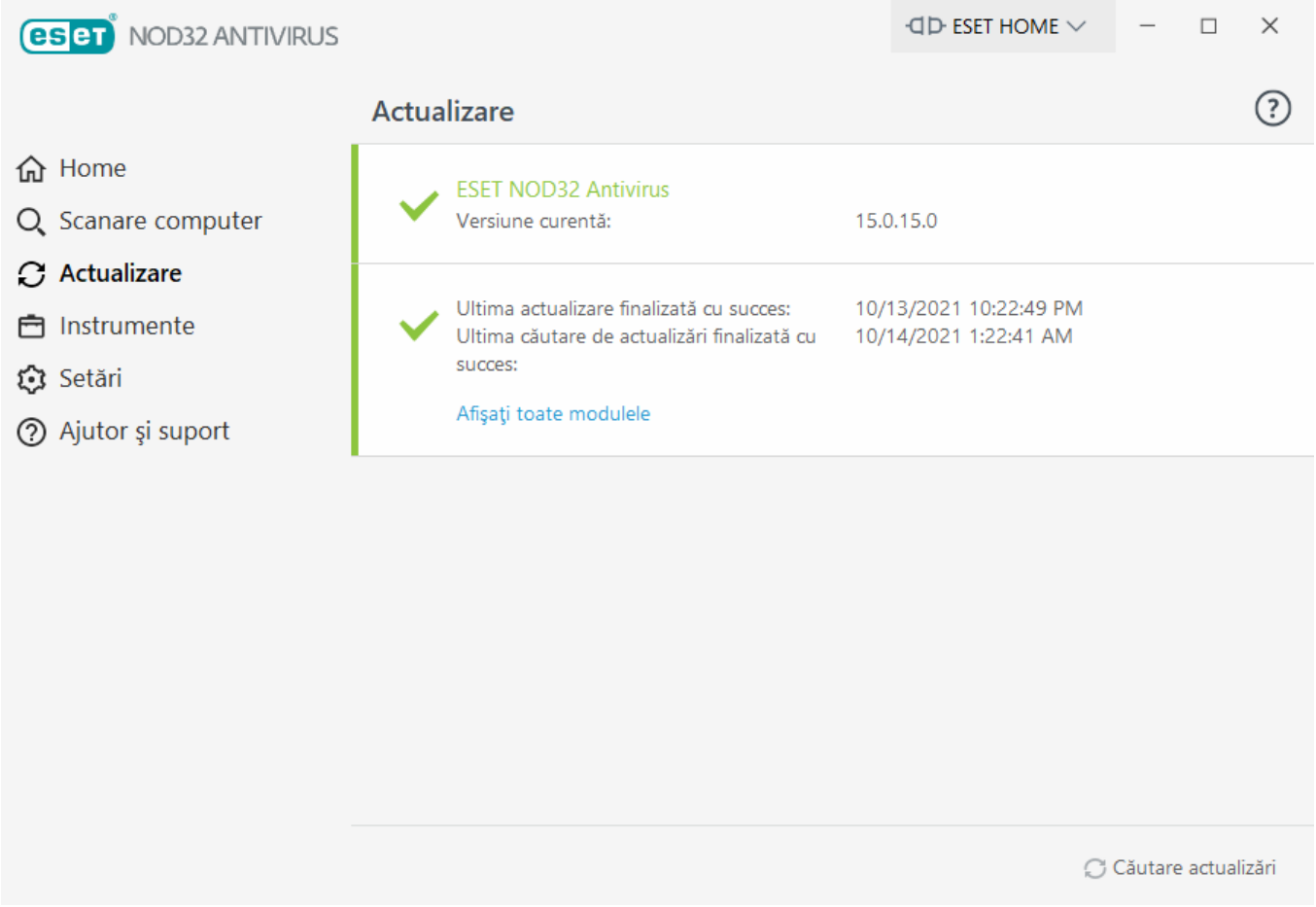
Dacă nu reușiți să rezolvați o problemă utilizând soluțiile sugerate, faceți clic pe **Ajutor și suport** pentru a accesa fișierele de ajutor sau pentru a căuta în baza de cunoștințe ESET. Dacă în continuare aveți nevoie de asistență, puteți trimite o solicitare de asistență. Serviciul de asistență tehnică ESET va răspunde rapid întrebărilor dvs. și vă va ajuta la găsirea unei soluții.

Actualizări

Actualizarea regulată a produsului ESET NOD32 Antivirus este cea mai bună metodă de a asigura nivelul maxim de securitate pe computerul dvs. Modulul Actualizare asigură că atât modulele de program, cât și componentele sistemului sunt întotdeauna actualizate.

Cu clic pe **Actualizare** în fereastra principală a meniului, puteți vizualiza starea curentă a actualizării, inclusiv data și ora ultimei actualizări reușite și dacă este necesară o actualizare.

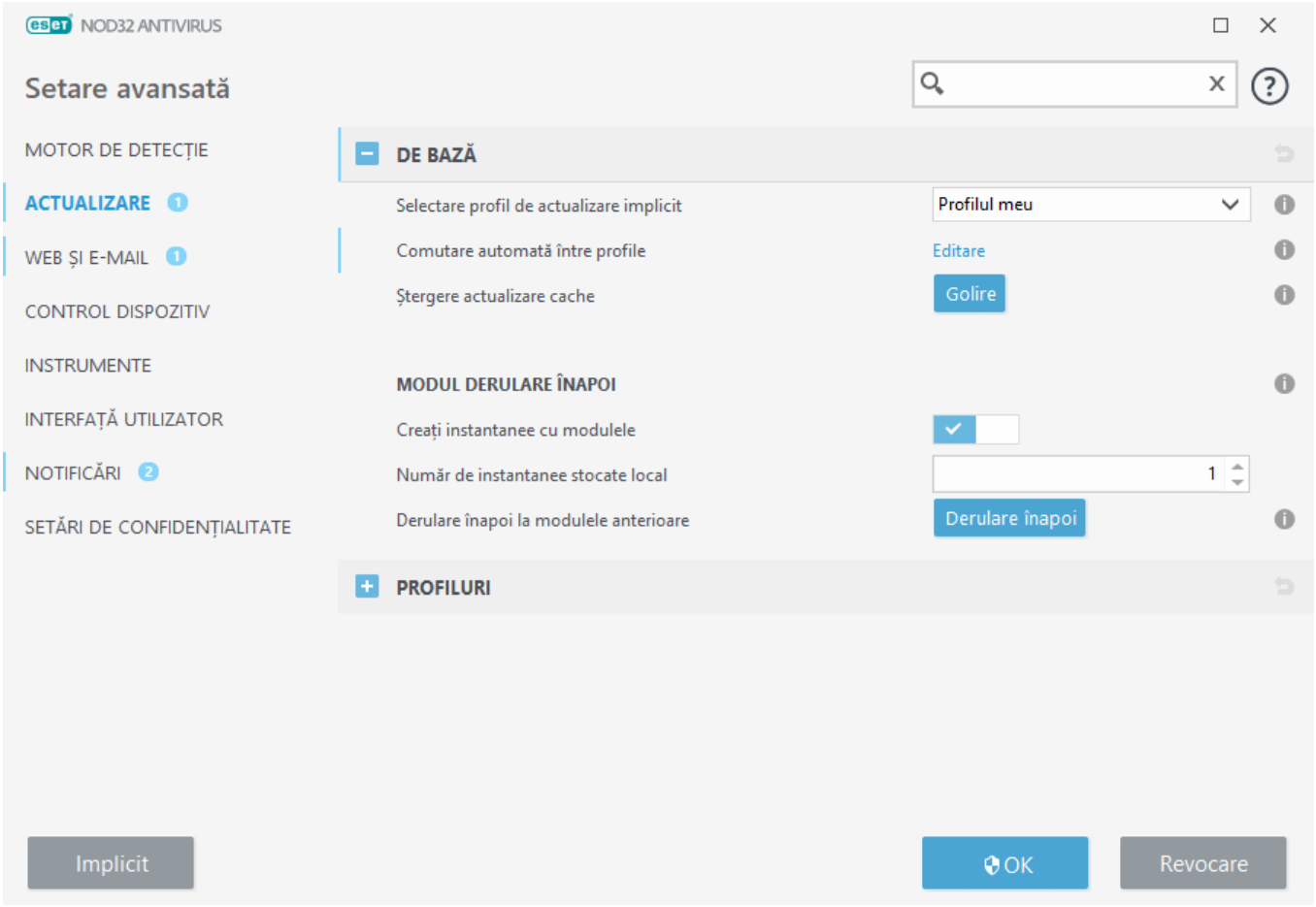
Pe lângă actualizările automate, puteți face clic pe **Căutare actualizări** pentru a declanșa o actualizare manuală.



Fereastra Setare avansată (faceți clic pe **Setare** în meniul principal, apoi faceți clic pe **Setări avansate** sau apăsați pe tasta **F5** a tastaturii) conține opțiuni suplimentare de actualizare. Pentru a configura opțiuni avansate de actualizare, cum ar fi modul de actualizare, accesul la serverul proxy și conexiunile LAN, faceți clic pe **Actualizare** în arborele Setare avansată.

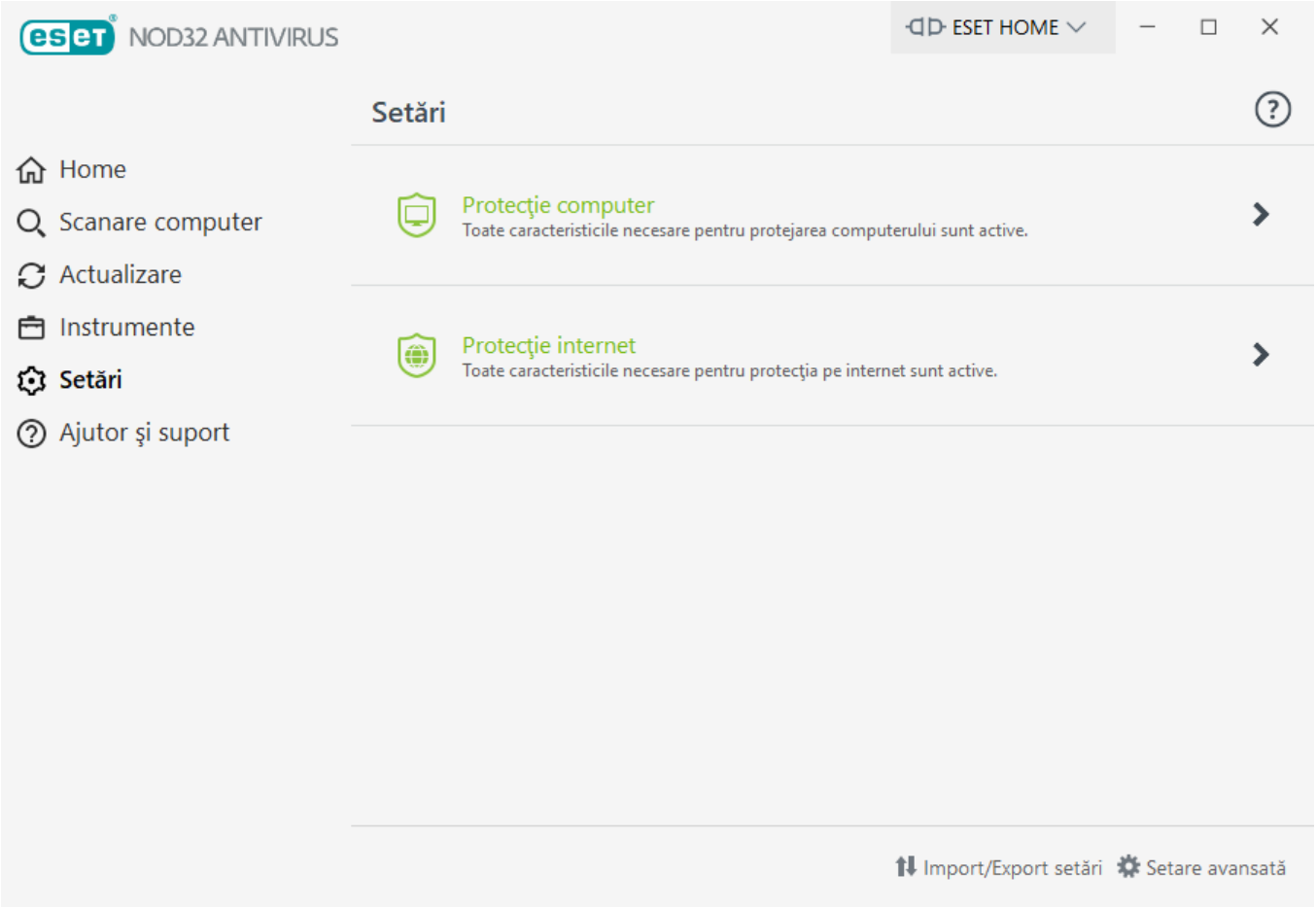
Dacă aveți probleme cu o actualizare, faceți clic pe **Golire** pentru a goli memoria cache de actualizări. Dacă în continuare nu puteți actualiza modulele de program, consultați secțiunea Depanarea mesajului „Nu s-a reușit

actualizarea modulelor”.



Lucrul cu ESET NOD32 Antivirus

Opțiunile de setare ale produsului ESET NOD32 Antivirus vă permit să ajustați nivelurile de protecție pentru computer.



Meniul **Setare** este împărțit în secțiunile următoare:

Protecție computer

Protecție internet

Faceți clic pe o componentă pentru a regla setările avansate ale modulului de protecție corespunzător.

Setarea **Protecție computer** vă permite să activați sau să dezactivați componentele următoare:

- **Protecție în timp real pentru sistemul de fișiere** – toate fișierele sunt scanate pentru a depista cod rău intenționat în momentul în care sunt deschise, create sau executate.
- **Control dispozitiv** – acest modul vă permite să scanați, să blocați sau să reglați filtrele/permisiunile extinse și să selectați modul în care utilizatorul poate accesa și utiliza un anumit dispozitiv (CD/DVD/USB...).
- **HIPS** – sistemul HIPS monitorizează evenimentele din sistemul de operare și reacționează la acestea conform unui set de reguli particularizat.
- **Mod Gamer** – activează sau dezactivează mod gamer. Veți primi un mesaj de avertizare (risc potențial de securitate) și fereastra principală va deveni portocalie după activarea mod pentru jocuri.

Setarea **Protecție internet** vă permite să activați sau să dezactivați componentele următoare:

- **Protecție acces Web** – Dacă se activează, se scanează de cod dăunător tot traficul prin HTTP sau HTTPS.

- **Protecție client e-mail** – monitorizează comunicările prin email primite prin protocoalele POP3(S) și IMAP(S).

- **Protecție Anti-Phishing** – filtrează site-urile Web suspectate de distribuirea unui conținut cu intenția de a convinge utilizatorii să trimită informații confidențiale.

Pentru a reactiva o componentă de securitate dezactivată, faceți clic pe cursorul , astfel încât să afișeze un marcaj de selectare verde .

Când dezactivați protecția utilizând această metodă, toate modulele de protecție dezactivate se vor activa după repornirea computerului.

Opțiunile suplimentare sunt disponibile în partea de jos a ferestrei de setare. Utilizați legătura **Setări avansate** pentru a seta parametri mai detaliați pentru fiecare modul. Utilizați **Importare/exportare setări** pentru a încărca parametrii de setare utilizând un fișier de configurare .xml sau pentru a salva parametrii de setare actuali într-un fișier de configurare.

Protecție computer

Faceți clic pe **Protecție computer** în fereastra **Configurare** pentru a vedea o prezentare generală a tuturor modulelor de protecție:

- Protecție în timp real a sistemului de fișiere
- Control dispozitiv
- Componenta Sistem de prevenire a intruziunilor la nivel host (HIPS)
- Mod Gamer

Pentru a pune în pauză sau a dezactiva module de protecție individuale, faceți clic pe pictograma barei cu glisor .

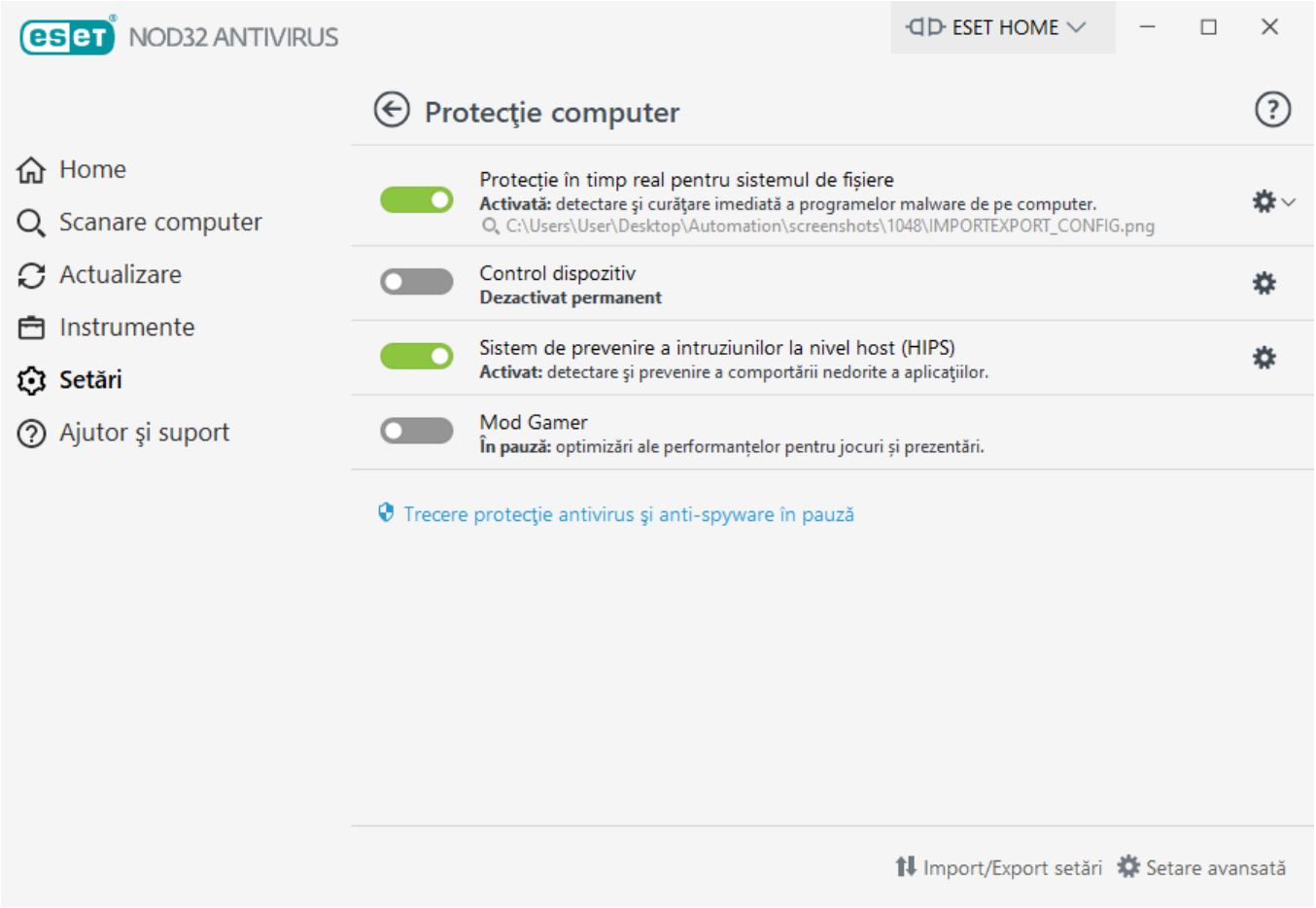
Dezactivarea modulelor de protecție poate scădea nivelul de protecție pentru computerul dvs.

Faceți clic pe pictograma rotiță Lângă un modul de protecție pentru a accesa setările avansate ale modulului respectiv.

Pentru componenta **Protecție în timp real pentru sistemul de fișiere**, faceți clic pe pictograma rotiță și alegeți dintre următoarele opțiuni:

- **Configurare** – Deschide Setare avansată pentru Protecție în timp real pentru sistemul de fișiere.

- **Editare excluderi** – Deschide fereastra de configurare a excluderilor, unde să puteți exclude fișiere și foldere de la scanare.



Pauză protecție antivirus și antispyware – Dezactivează toate modulele de protecție antivirus și anti-spyware. Atunci când dezactivați protecția, se va deschide o fereastră în care puteți stabili cât timp este dezactivată protecția utilizând meniul vertical **Interval de timp**. Utilizați această opțiune doar dacă sunteți un utilizator experimentat sau dacă primiți instrucțiuni de la Asistența tehnică ESET.

Motor de detecție

Motorul de detecție vă protejează împotriva atacurilor rău intenționate asupra sistemului, controlând fișiere, mesaje de e-mail și comunicări internet. De exemplu, dacă se detectează un obiect clasificat ca malware, va începe remedierea. Motorul de detecție o poate elimina blocând-o mai întâi, apoi curățând-o, ștergând-o sau mutând-o în carantină.

Pentru a configura în detaliu setările motorului de detecție, faceți clic pe **Setare avansată** sau apăsați pe tasta **F5**.

Modificările setărilor motorului de detecție trebuie efectuate numai de către un utilizator experimentat. Configurarea incorectă a setărilor poate avea drept rezultat un nivel scăzut de protecție.

În această secțiune:

- Categorii pentru protecția în timp real și învățarea programată
- Scanări malware
- Configurarea rapoartelor
- Configurarea protecției

Categorii pentru protecția în timp real și învățarea programată

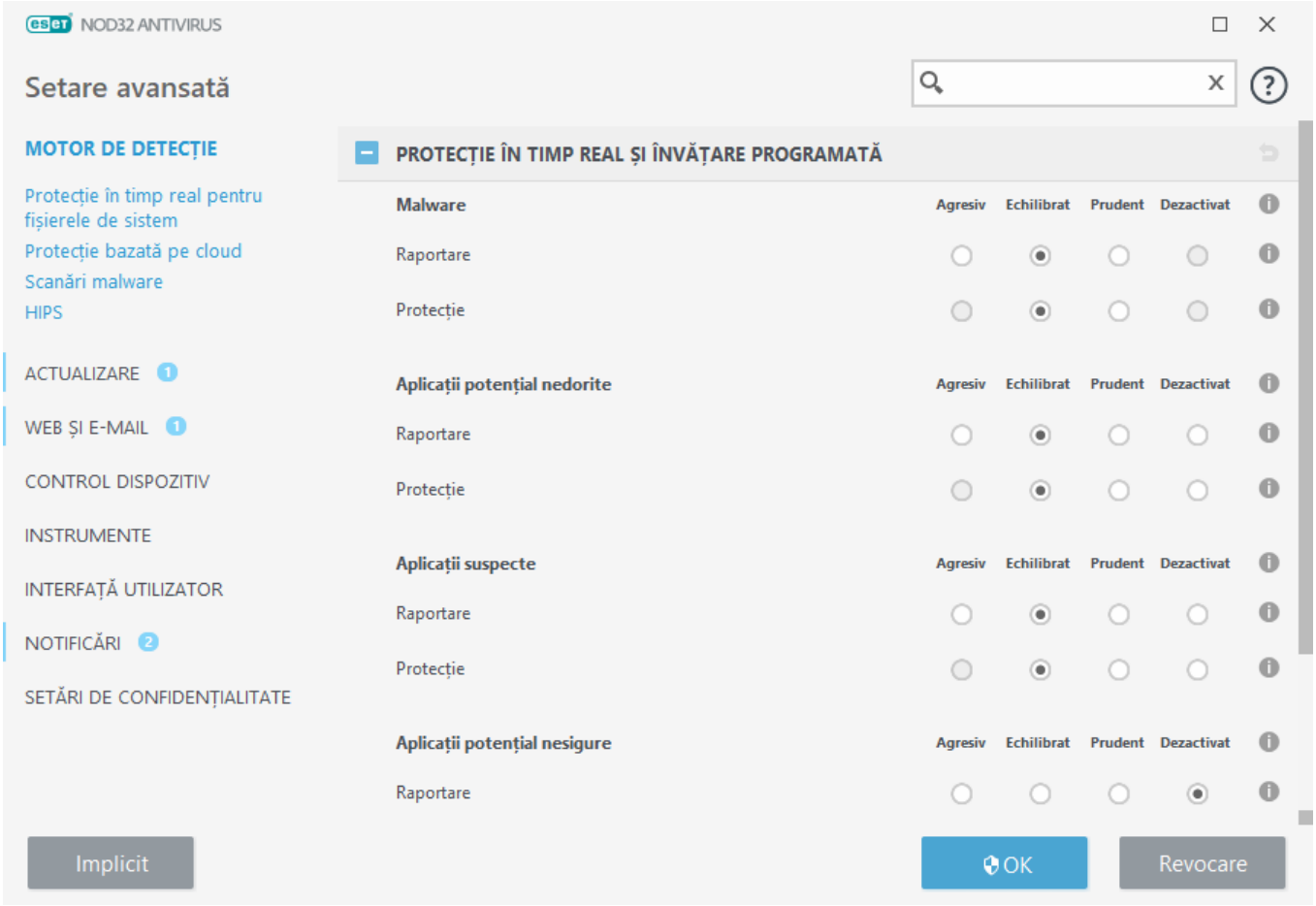
Componenta **Protecție în timp real și învățare programată** pentru toate modulele de protecție (de exemplu, Protecție în timp real pentru sistemul de fișiere, Protecție acces web etc.) vă permite să configurați nivelurile de raportare și protecție folosind următoarele categorii:

- **Malware** – Un virus de computer este o bucată de cod rău intenționat care este adăugată sau anexată la fișiere existente de pe computer. Însă termenul „virus” este adesea utilizat în mod incorect. „Malware” (software rău intenționat) este un termen mai precis. Detectarea programelor malware este efectuată de către modulul motorului de detecție, în combinație cu componenta Învățare programată. Citiți mai multe detalii despre aceste tipuri de aplicații în Glosar.

- **Aplicații potențial nedorite**– Aplicațiile grayware sau aplicațiile potențial nedorite (PUA) reprezintă o categorie extinsă de programe software al căror scop nu este în mod clar rău intenționat, ca în cazul altor tipuri de programe malware, cum ar fi viruși sau cai troieni. Cu toate acestea, ele ar putea instala programe software suplimentare nedorite, pot schimba comportamentul dispozitivului digital sau pot efectua activități care nu sunt aprobate sau așteptate de către utilizator. Citiți mai multe detalii despre aceste tipuri de aplicații în Glosar.

- **Aplicații suspecte** includ programe comprimate în pachete sau protecții. Aceste tipuri de protecții sunt adesea exploatate de autorii programelor rău intenționate pentru a evita detectarea.

- **Aplicații potențial periculoase** – Se referă la software comercial legal care poate fi utilizat în scopuri rău intenționate. Exemple de aplicații potențial periculoase (PUA): instrumente de acces la distanță, aplicații pentru spargerea parolelor și pentru înregistrarea tastelor (programe ce înregistrează fiecare tastă apăsată de un utilizator). Citiți mai multe detalii despre aceste tipuri de aplicații în Glosar.



Protecție îmbunătățită

Învățarea programată avansată face acum parte din motorul de detecție și reprezintă un strat avansat de protecție care îmbunătățește detectarea bazată pe învățarea programată. Citiți mai multe despre acest tip de protecție în glosar.

Scanări malware

Setările scanerului pot fi configurate separat pentru scanerul în timp real și pentru scanerul la cerere. În mod implicit, opțiunea **Utilizarea setărilor de protecție în timp real** este activată. Atunci când această opțiune este activată, setările pentru scanarea la cerere sunt moștenite din secțiunea **Protecție în timp real și învățare programată**. Pentru mai multe informații, consultați Scanări malware.

Configurarea rapoartelor

Atunci când apare o detectare (de exemplu, se găsește o amenințare și este clasificată drept malware), informațiile sunt înregistrate în jurnalul Detectări și se trimit Notificări desktop, dacă această opțiune este configurată în ESET NOD32 Antivirus.

Pragul pentru raportare este configura pentru fiecare categorie în parte (desemnată mai departe drept „CATEGORIE”):

1. Malware

2.Aplicații potențial nedorite

3.Potențial nesigure

4.Aplicații suspecte

Raportare efectuată cu motorul de detecție, inclusiv componenta de învățare programată. Este posibilă setarea unui prag de raportare mai ridicat decât pragul de protecție curent. Aceste setări de raportare nu influențează blocarea, curățarea sau ștergerea obiectelor.

Citiți următoarele informații înainte de a modifica un prag (sau nivel) pentru raportarea pentru CATEGORIE:

Prag	Explicație
Agresiv	Raportarea programelor CATEGORIE este configurată la Sensibilitate maximă. Vor fi raportate mai multe detectări. Setarea **Agresiv** poate identifica în mod fals unele obiecte ca CATEGORIE.
Echilibrat	Raportarea programelor CATEGORIE este configurată la Echilibrat. Această setare este optimizată pentru a oferi un echilibru între performanțele și precizia ratelor de detectare, pe de o parte, și numărul de obiecte raportate în mod fals, pe de altă parte.
Prudent	Raportarea programelor CATEGORIE este configurată pentru a reduce numărul obiectelor identificate în mod fals, păstrând în același timp un nivel suficient de protecție. Obiectele sunt raportate numai atunci când probabilitatea este evidentă și se potrivește comportamentului programelor CATEGORIE.
Dezactivat	Raportarea programelor CATEGORIE nu este activă, iar detectările de acest tip nu sunt găsite, raportate sau curățate. Prin urmare, această setare dezactivează protecția pentru acest tip de detectare. Opțiunea Dezactivat nu este disponibilă pentru raportarea programelor malware și este valoarea implicită pentru aplicațiile potențial periculoase.

Disponibilitatea modulelor de protecție din ESET NOD32 Antivirus

Disponibilitatea (activat sau dezactivat) unui modul de protecție pentru un prag de CATEGORIE selectat este următoarea:

	Agresiv	Echilibrat	Prudent	Dezactivat**
Modul Învățare programată avansată*	✔ (mod agresiv)	✔ (mod conservator)	X	X
Modul Motor de detecție	✔	✔	✔	X
Alte module de protecție	✔	✔	✔	X

* Disponibil în ESET NOD32 Antivirus versiunea 13.1 și în versiunile ulterioare.
**Nerecomandat

Stabilirea versiunii produsului, a versiunilor modulului programului și a datelor versiunilor

1. Faceți clic pe **Ajutor și suport** > **Despre ESET NOD32 Antivirus**.

2. În ecranul **Despre**, primul rând de text afișează numărul versiunii produsului dvs. ESET.

3. Faceți clic pe **Instalare componente** pentru a accesa informații despre module specifice.

Aspecte importante

Câteva aspecte importante când setați un prag adecvat pentru mediul dvs.:

- Pragul **Echilibrat** este recomandat pentru cele mai multe configurări.
- Pragul **Prudent** corespunde nivelului de protecție din versiuni anterioare ale ESET NOD32 Antivirus (versiunea 13.0 și versiuni anterioare). Este recomandat pentru medii în care accentul se pune pe minimizarea obiectelor identificate în mod fals de programele software de securitate.
- Cu cât nivelul de raportare este mai ridicat, cu atât rata de detectare va fi mai mare, dar în același timp există o șansă mai mare de a identifica în mod fals anumite obiecte.
- În lumea reală, nu există niciun scenariu care să garanteze o rată de detectare de 100% și 0% clasificări incorecte (pentru obiecte curate identificate ca malware).
- Păstrați actualizate ESET NOD32 Antivirus și modulele sale, pentru un echilibru între performanțe și precizia ratelor de detectare și numărul de obiecte raportate în mod fals.

Configurarea protecției

Dacă se raportează un obiect clasificat drept CATEGORIE, programul blochează obiectul și apoi îl curăță, îl șterge sau îl mută în Carantină.

Citiți următoarele informații înainte de a modifica un prag (sau nivel) pentru protecția pentru CATEGORIE:

Prag	Explicație
Agresiv	Detecțiile raportate care au nivelul Agresiv sau un nivel inferior sunt blocate și pornește remedierea automată (de exemplu, curățarea). Această setare este recomandată atunci când toate dispozitivele endpoint au fost scanate cu setări agresive și obiecte raportate în mod fals au fost adăugate la excluderi de la detectare.
Echilibrat	Detectările raportate care au nivelul Echilibrat sau un nivel inferior sunt blocate și se pornește remedierea automată (de exemplu, curățarea).
Prudent	Detecțiile raportate care au nivelul Prudent sunt blocate și se pornește remedierea automată (de exemplu, curățarea).
Dezactivat	Opțiunea este utilă pentru a identifica și a exclude obiectele raportate în mod eronat. Opțiunea Dezactivat nu este disponibilă pentru protecția programelor malware și este valoarea implicită pentru aplicațiile potențial periculoase.

Tabel de conversie pentru ESET NOD32 Antivirus versiunea 13.0 și versiuni anterioare

Atunci când faceți upgrade de la versiunea 13.0 și versiuni anterioare la versiunea 13.1 și versiuni ulterioare, noua stare pentru prag va fi următoarea:

Comutator categorie înainte de upgrade		
Prag nou CATEGORIE după upgrade	Echilibrat	Dezactivat

Opțiuni avansate pentru motorul de detecție

Tehnologia Anti-Stealth este un sistem sofisticat ce permite detectarea programelor periculoase, cum ar fi rootkiturile, care sunt capabile de disimulare față de sistemul de operare. Acest lucru înseamnă că nu pot fi detectate utilizând tehnici obișnuite de testare.

Activare scanare avansată prin AMSI – instrumentul Microsoft Antimalware Scan Interface asigură dezvoltatorilor de aplicații noi mijloace de apărare împotriva programelor malware (doar pentru Windows 10).

S-a detectat o infiltrare

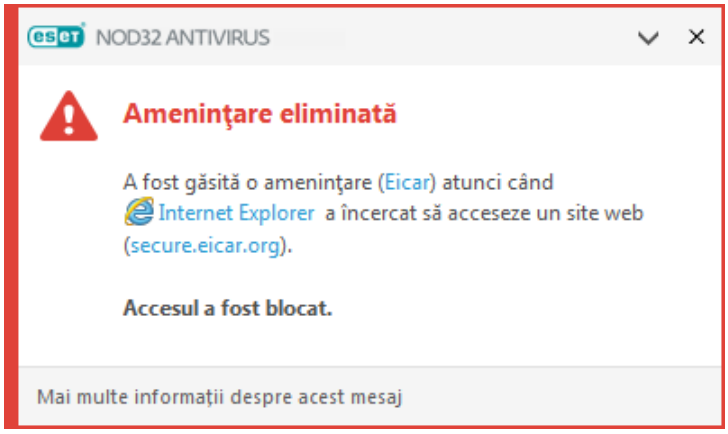
Infiltrările pot ajunge în sistem prin diverse puncte de intrare: pagini Web, directoare partajate, prin email sau de la dispozitivele amovibile (USB, discuri externe, CD-uri, DVD-uri, dischete etc.).

Comportament standard

Ca exemplu general despre cum tratează ESET NOD32 Antivirus infiltrările, acestea pot fi detectate utilizând următoarele componente:

- Protecție în timp real a sistemului de fișiere
- Protecție acces Web
- Protecție client email
- Scanare computer la cerere

Fiecare utilizează nivelul de curățare standard și va încerca să curețe fișierul și să îl mute în Carantină sau să închidă conexiunea. În zona de notificare, în partea din dreapta jos a ecranului, se afișează o fereastră de notificare. Pentru informații detaliate despre obiectele detectate/curățate, consultați Fișiere log. Pentru informații suplimentare despre nivelurile de curățare și comportament, consultați Nivel de curățare.



Scanarea computerului pentru fișiere infectate

În cazul în care computerul prezintă semne de infecție malware, de exemplu este încetinit, îngheață des etc., vă recomandăm următoarele:

1. Deschideți ESET NOD32 Antivirus și faceți clic pe **Scanare computer**.

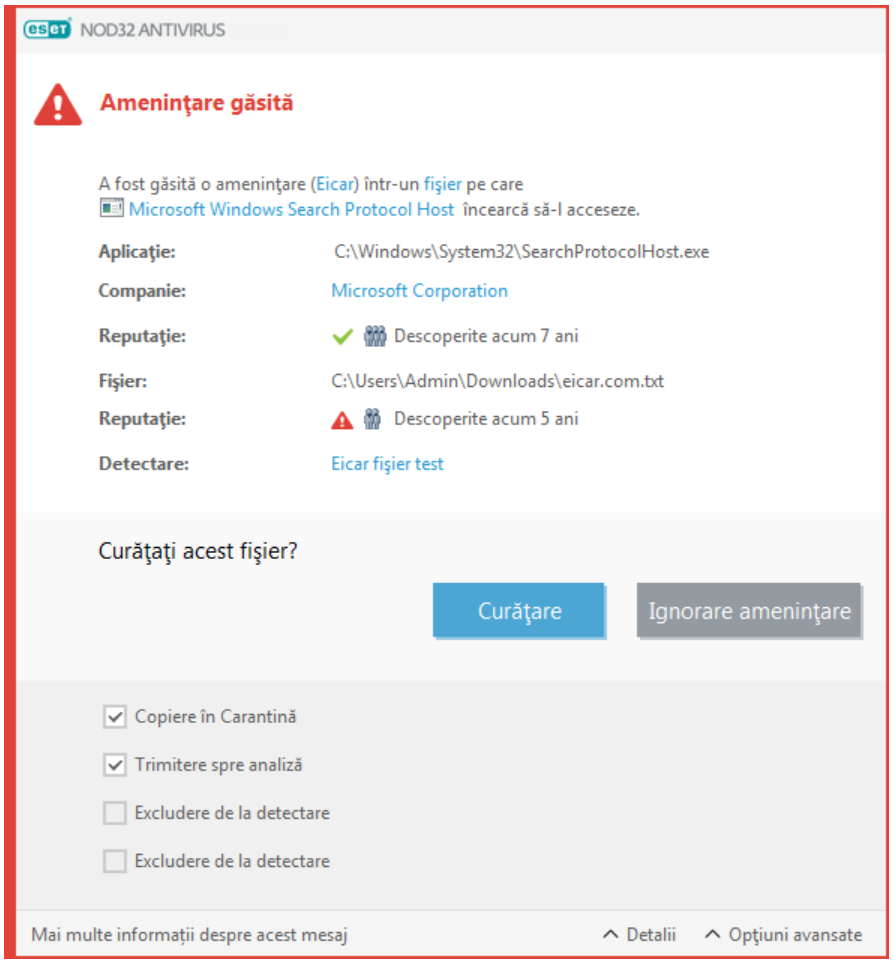
2.Faceți clic pe **Scanați computerul** (pentru informații suplimentare, consultați Scanare computer).

3.După terminarea scanării, consultați logul pentru a vedea numărul de fișiere scanate, infectate și curățate.

Dacă doriți să scanați numai o parte a discului, faceți clic pe **Scanare personalizată** și selectați țintele ce trebuie scanate pentru viruși.

Curățare și ștergere

Dacă nu există o acțiune predefinită de urmat pentru protecția sistemului de fișiere în timp real, vi se va solicita să selectați o opțiune în fereastra de alertă. În general, sunt disponibile opțiunile **Curățare**, **Ștergere** și **Păstrare**. Nu vă recomandăm să selectați **Păstrare**, deoarece fișierele infectate vor rămâne necurățate. Singura excepție este atunci când sunteți sigur că un fișier este inofensiv și a fost detectat din greșeală.



Aplicați curățarea dacă un fișier a fost atacat de un virus care a atașat cod dăunător fișierului. În acest caz, încercați mai întâi să curățați fișierul infectat pentru a-l readuce la starea inițială. Fișierul va fi șters dacă este format exclusiv din cod dăunător.

Dacă un fișier infectat este „blocat” sau este utilizat de un proces de sistem, de obicei va fi șters numai după ce este eliberat (de obicei, după o repornire a sistemului).

Restaurare din Carantină

Puteți accesa Carantina din fereastra principală a programului ESET NOD32 Antivirus, făcând clic pe **Instrumente** > **Carantină**.

Fișierele aflate în carantină pot fi și restaurate în locația lor inițială:

- Utilizați în acest scop caracteristica **Restaurare**, disponibilă în meniul contextual atunci când faceți dreapta pe un anumit fișier din Carantină.

- Dacă un fișier este marcat ca o aplicație potențial nedorită, opțiunea **Restaurare și excludere de la scanare** este activată. Consultați și Excluderi.

- Meniul contextual oferă și o opțiune **Restaurare la**, care vă permite să restaurați un fișier într-o altă locație decât cea din care a fost șters.

- Funcționalitatea de restaurare nu este disponibilă în unele cazuri, de exemplu, pentru fișierele amplasate pe o partiție de rețea doar în citire.

Amenințări multiple

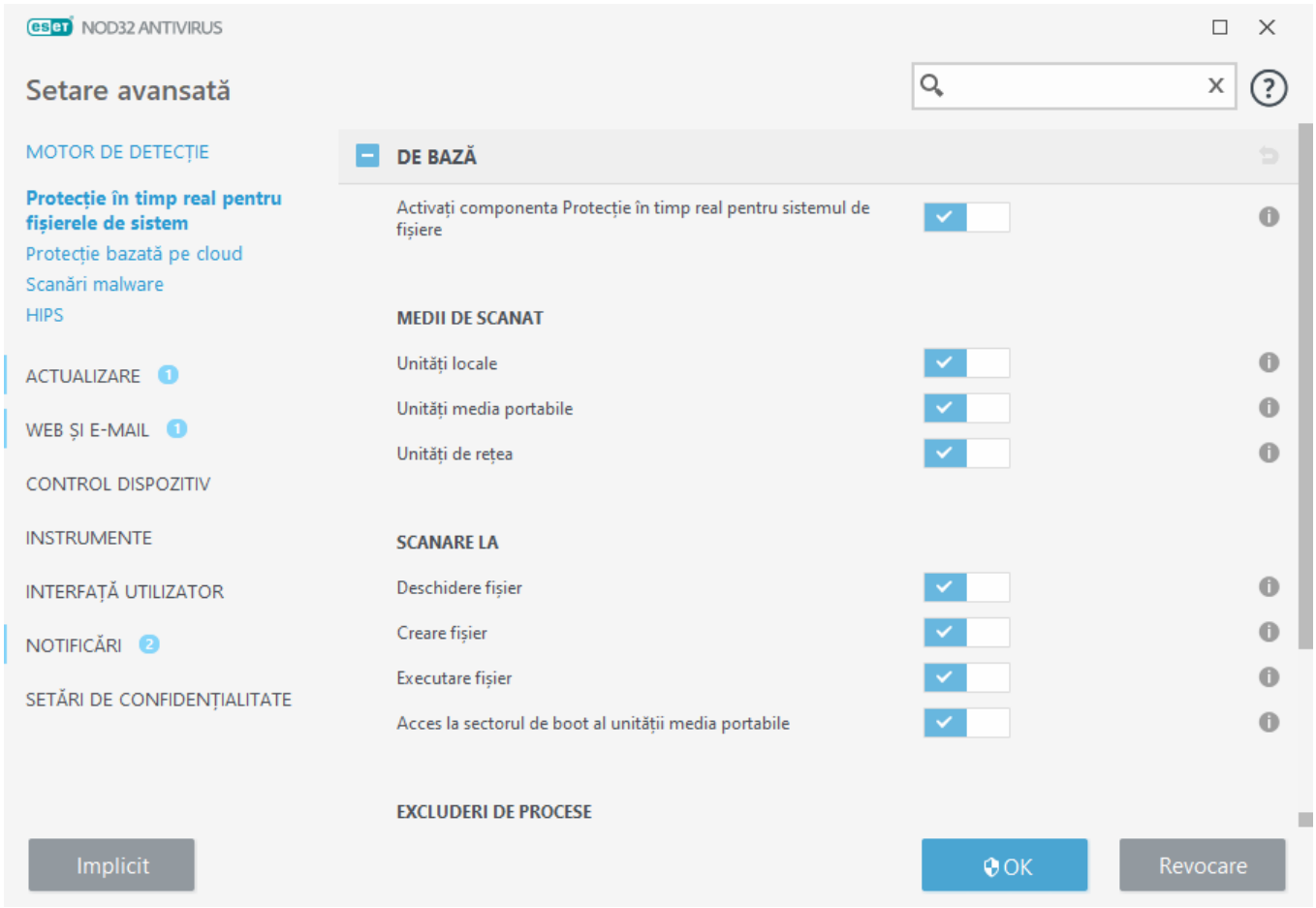
Dacă în timpul unei scanări a computerului au rămas fișiere infectate necurățate (sau nivelul de curățare s-a setat la **Fără curățare**), se va afișa o fereastră de alertă care vă va solicita selectarea unor acțiuni pentru fișierele respective. Selectați acțiuni pentru fișiere (acțiunile sunt setate individual pentru fiecare fișier din listă), apoi faceți clic pe **Terminare**.

Ștergere fișiere în arhive

În modul de curățare implicit, va fi șterasă arhiva în totalitate numai dacă aceasta conține fișiere infectate și niciun fișier curat. Cu alte cuvinte, arhivele nu sunt șterse dacă ele conțin și fișiere curate inofensive. Aveți grijă atunci când efectuați o scanare de curățare strictă; dacă este activată curățarea strictă, o arhivă va fi ștearsă dacă aceasta conține cel puțin un fișier infectat, indiferent de starea celorlalte fișiere din arhivă.

Protecție în timp real a sistemului de fișiere

Protecția în timp real pentru sistemul de fișiere controlează toate fișierele din sistem pentru cod rău intenționat, atunci când fișierele sunt deschise, create sau rulate.



În mod implicit, componenta Protecție în timp real pentru fișierele de sistem se lansează la pornirea sistemului și asigură scanare neîntreruptă. Nu recomandăm dezactivarea opțiunii **Activare Protecție în timp real pentru sistemul de fișiere** în secțiunea **Setări avansate**, sub **Motor de detecție** > **Protecție în timp real pentru sistemul de fișiere** > **De bază**.

Medii de scanat

În mod implicit, toate tipurile de medii sunt controlate pentru amenințări potențiale:

- **Unități locale** – Scanează toate unitățile de hard disk ale sistemului și pe cele fixe (de exemplu: *C:*\, *D:*\).
- **Unități media portabile** – Scanează CD-uri/DVD-uri, memorii USB, carduri de memorie etc.
- **Unități de rețea** – Scanează toate unitățile de rețea mapate (de exemplu: *H:*\ mapat ca *store04*) sau unitățile de rețea cu acces direct (de exemplu: *store08*).

Vă recomandăm să utilizați setările implicite sau să modificați aceste setări numai în cazuri specifice, cum ar fi atunci când scanarea anumitor medii încetinește semnificativ transferurile de date.

Scanare la

În mod implicit, toate fișierele sunt scanate la deschidere, creare sau executare. Vă recomandăm să păstrați aceste setări implicite, deoarece acestea asigură nivelul maxim de protecție în timp real pentru computer:

- **Deschidere fișier** – Scanează fișierul atunci când acesta este deschis.

- **Creare fișier** – Scanează un fișier când acesta a fost creat sau modificat.
- **Executare fișier** – Scanează un fișier când acesta este executat sau rulat.
- **Acces la sectorul de boot al unității media portabile** – Atunci când în dispozitiv sunt inserate unități media portabile care conțin un sector de boot, sectorul de boot este scanat imediat. Această opțiune nu activează scanarea fișierelor de pe unități media portabile. Scanarea fișierelor de pe unități media portabile se găsește în **Medii de scanat** > **Unități media portabile**. Pentru ca opțiunea **Acces la sectorul de boot al unității media portabile** să funcționeze corect, păstrați opțiunea **Sectoare de boot/UEFI** activată în parametrii ThreatSense.

Protecție în timp real pentru fișierele de sistem verifică toate tipurile de medii și este declanșată de diverse evenimente din sistem, cum ar fi accesarea unui fișier. Dacă se utilizează metode de detecție ale tehnologiei ThreatSense (așa cum sunt descrise în secțiunea Setare parametri motor ThreatSense), Protecție în timp real pentru fișierele de sistem poate fi configurată pentru a trata fișierele create recent în mod diferit față de fișierele existente. De exemplu, puteți configura Protecție în timp real pentru fișierele de sistem astfel încât să monitorizați mai îndeaproape fișierele create recent.

Pentru efecte minime asupra sistemului la utilizarea protecției în timp real, fișierele deja scanate nu se scanează în mod repetat (cu excepția cazului în care aceste fișiere au fost modificate). Fișierele sunt scanate imediat după fiecare actualizare a motorului de detecție. Acest comportament este controlat prin utilizarea caracteristicii **Optimizare Smart**. Atunci când caracteristica **Optimizare Smart** este dezactivată, toate fișierele sunt scanate la fiecare accesare. Pentru a modifica această setare, apăsați pe **F5** pentru a deschide fereastra **Setări avansate** și extindeți **Motor de detecție** > **Protecție în timp real pentru sistemul de fișiere**. Faceți clic pe **Parametri ThreatSense** > **Altele** și bifați sau debifați opțiunea **Activare optimizare Smart**.

Niveluri de curățare

Pentru a accesa setările pentru nivelul de curățare pentru modulul de protecție dorit, extindeți secțiunea **Parametri ThreatSense** (de exemplu, **Protecție în timp real pentru sistemul de fișiere**), apoi găsiți opțiunea **Curățare > Nivel de curățare**.

Parametrii ThreatSense au următoarele niveluri de remediere (adică curățare).

Remedierea în ESET NOD32 Antivirus

Nivel de curățare	Descriere
Remediați întotdeauna detectarea	Se încearcă remedierea detectării curățând obiectele fără intervenția utilizatorului final. În unele cazuri rare (de exemplu, fișiere de sistem), dacă detectarea nu poate fi remediată, obiectul raportat este lăsat în locația sa originală.
Se remediază detectarea dacă este sigur, altminteri se păstrează	Se încearcă remedierea detectării curățând obiectele fără intervenția utilizatorului final. În unele cazuri (de exemplu, fișiere de sistem sau arhive care conțin atât fișiere curate, cât și infectate), dacă o detectare nu poate fi remediată, obiectul raportat este lăsat în locația sa originală.
Se remediază detectarea dacă este sigur, altminteri se întreabă	Se încearcă remedierea detectării curățând obiectele. În unele cazuri, dacă nu se poate efectua nicio acțiune, utilizatorul final primește o alertă interactivă și trebuie să selecteze o acțiune de remediere (de exemplu, Ștergere sau Ignorare). Această setare este recomandată în majoritatea cazurilor.

Nivel de curățare	Descriere
Întrebați întotdeauna utilizatorul final	Se afișează o fereastră interactivă utilizatorului final atunci când se curăță obiecte, în care acesta trebuie să selecteze o acțiune de remediere (de exemplu, Ștergere sau Ignorare). Acest nivel este destinat utilizatorilor mai avansați, care știu ce pași să urmeze în eventualitatea unei detectări.

Când se modifică configurarea protecției în timp real

Protecția în timp real este cea mai importantă componentă pentru menținerea unui sistem securizat. Fiți atent atunci când modificați parametrii acesteia. Vă recomandăm să modificați parametrii acesteia numai în anumite cazuri.

După instalarea ESET NOD32 Antivirus, toate setările sunt optimizate pentru a oferi pentru utilizatori nivelul maxim de securitate de sistem. Pentru a restaura setările implicite, faceți clic pe ↩ lângă fiecare filă din fereastră (**Setări avansate** > **Motor de detecție** > **Protecție în timp real pentru sistem fișiere**).

Verificare protecție în timp real

Pentru a verifica dacă protecția în timp real funcționează și detectează viruși, utilizați un fișier test de la *www.eicar.com*. Acest fișier test este un fișier inofensiv, detectabil de către toate programele antivirus. Fișierul a fost creat de compania EICAR (European Institute for Computer Antivirus Research) pentru a testa funcționalitatea programelor antivirus.

Fișierul este disponibil pentru descărcare la adresa http://www.eicar.org/download/eicar.com
După ce introduceți acest URL în browser, ar trebui să vedeți un mesaj care vă spune că amenințarea a fost eliminată.

Ce este de făcut dacă protecția în timp real nu funcționează

În acest capitol sunt descrise problemele care pot să apară la utilizarea protecției în timp real, precum și modul de depanare a acestora.

Protecția în timp real este dezactivată

Dacă un utilizator dezactivează din greșeală protecția în timp real, trebuie să reactivați caracteristica. Pentru a reactiva protecția în timp real, accesați **Setare** în fereastra principală a programului și faceți clic pe **Protecție computer** > **Protecție în timp real pentru sistemul de fișiere**.

Dacă protecția în timp real nu s-a inițiat la pornirea sistemului, acest lucru se datorează, de obicei, dezactivării opțiunii **Pornire automată a protecției în timp real a sistemului de fișiere**. Pentru a vă asigura că această opțiune este activată, navigați la **Setări avansate** (**F5**) și faceți clic pe **Motor de detecție** > **Protecție în timp real a sistemului de fișiere**.

Dacă protecția în timp real nu detectează și nu curăță infiltrările

Asigurați-vă că pe computer nu mai sunt instalate alte programe antivirus. Dacă aveți instalate simultan două programe antivirus, acestea pot intra în conflict unul cu celălalt. Vă recomandăm să dezinstalați orice alte programe antivirus de pe sistemul dvs. înainte de a instala ESET.

Protecția în timp real nu pornește

Dacă protecția în timp real nu s-a inițiat la pornirea sistemului (iar opțiunea **Activați componenta Protecție în timp real pentru sistemul de fișiere** este activată), cauza ar putea fi conflictele cu alte programe. Dacă a rezolva această problemă, creați un jurnal SysInspector și trimiteți-l Asistenței tehnice ESET pentru analiză.

Excluderi de procese

Caracteristica Excluderi de procese vă permite să excludeți procese de aplicații de la Protecția în timp real pentru fișierele de sistem. Pentru a îmbunătăți viteza pentru copiile de rezervă, integritatea proceselor și disponibilitatea serviciului, în timpul copierii de rezervă sunt utilizate unele tehnici despre care se știe că intră în conflict cu protecția malware la nivel de fișier. Singurul mod eficient pentru a evita ambele situații este dezactivarea software-ului anti-malware. Prin excluderea procesului specific (de exemplu, cel al soluției de copiere de rezervă), toate operațiunile cu fișiere atribuite acestui proces exclus sunt ignorate și sunt considerate sigure, reducând astfel la minimum interferența cu procesul de copiere de rezervă. Vă recomandăm să aveți grijă atunci când creați excluderi: un instrument de copiere de rezervă care a fost exclus poate accesa fișiere infectate fără a declanșa o alertă, de aceea permisiunile extinse sunt permise numai în modulul Protecție în timp real.

Nu confundați cu Extensiile de fișiere excluse, Excluderile HIPS, Excluderile de la detectare sau Excluderile de performanță.

Excluderile de procese ajută la reducerea la minimum a riscului de conflicte potențiale și îmbunătățesc performanțele aplicațiilor excluse, ceea ce are un efect pozitiv asupra performanței generale și a stabilității sistemului de operare. Excluderea unui proces sau a unei aplicații reprezintă o excludere a fișierului său executabil (*.exe*).

Puteți adăuga fișiere executabile în lista de procese excluse în **Setare avansată** (F5) > **Motor de detecție** > **Protecție în timp real pentru sistemul de fișiere** > **Excluderi de procese**.

Această caracteristică a fost concepută pentru a exclude instrumentele de copiere de rezervă. Excluderea procesului instrumentului de copiere de rezervă nu numai că asigură stabilitatea sistemului, dar nu afectează nici performanța copierii de rezervă, deoarece aceasta nu este încetinită atunci când rulează.

Faceți clic pe **Editare** pentru a deschide fereastra de administrare **Excluderi de procese**, în care puteți selecta opțiunile Adăugare pentru a adăuga excluderi și puteți răsfoi până la fișierul executabil (de exemplu, *Backup-tool.exe*), care va fi exclus de la scanare.
Imediat ce fișierul *.exe* este adăugat la excluderi, activitatea acestui proces nu va mai fi monitorizată de ESET NOD32 Antivirus și nicio scanare nu va fi efectuată pentru operațiunile cu fișiere efectuate de acest proces.

Dacă nu folosiți funcția de răsfoire atunci când selectați fișierul executabil al procesului, trebuie să introduceți manual o cale completă către fișierul executabil. În caz contrar, excluderea nu av funcționa corect și HIPS este posibil să raporteze erori.

Puteți selecta și **Editare** pentru procese existente sau **Ștergere** pentru a le șterge din excludere.

Protecție acces web nu ia în calcul această excludere, astfel că, dacă excludeți fișierul executabil al browserului web, fișierele descărcate vor fi în continuare scanate. Astfel o infiltrare poate fi detectată în continuare. Acest scenariu este doar un exemplu și nu recomandăm crearea unor excluderi pentru browserele web.

Adăugarea sau editarea excluderilor de procese

Această fereastră de dialog vă permite să **adăugați** procese excluse de la motorul de detecție. Excluderile de procese ajută la reducerea la minimum a riscului de conflicte potențiale și îmbunătățesc performanțele aplicațiilor excluse, ceea ce are un efect pozitiv asupra performanței generale și a stabilității sistemului de operare. Excluderea unui proces sau a unei aplicații reprezintă o excludere a fișierului său executabil (*.exe*).

Selectați calea fișierului pentru o aplicație exceptată făcând clic pe ... (de exemplu, *C:\Program Files\Firefox\Firefox.exe*). NU introduceți numele aplicației.
Imediat ce fișierul *.exe* este adăugat la excluderi, activitatea acestui proces nu va mai fi monitorizată de ESET NOD32 Antivirus și nicio scanare nu va fi efectuată pentru operațiunile cu fișiere efectuate de acest proces.

Dacă nu folosiți funcția de răsfoire atunci când selectați fișierul executabil al procesului, trebuie să introduceți manual o cale completă către fișierul executabil. În caz contrar, excluderea nu av funcționa corect și HIPS este posibil să raporteze erori.

Puteți selecta și **Editare** pentru procese existente sau **Ștergere** pentru a le șterge din excludere.

Protecție bazată pe cloud

ESET LiveGrid® (bazat pe sistemul avansat de avertizare timpurie ESET ThreatSense.Net) utilizează date pe care utilizatorii ESET din întreaga lume le-au trimis la laboratorul de cercetare de la ESET. Furnizând mostre suspecte și metadate, ESET LiveGrid® ne permite să reacționăm imediat la nevoile clienților noștri și să menținem nivelul de răspuns al produsului ESET împotriva celor mai recente amenințări.

Sunt disponibile următoarele opțiuni:

Activați sistemul bazat pe reputație ESET LiveGrid®

Sistemul bazat pe reputație ESET LiveGrid® furnizează o încadrare bazată pe cloud într-o lista albă și o listă neagră.

Puteți verifica reputația Proceselor care se execută și a fișierelor direct din interfața programului sau din meniul contextual cu informații suplimentare disponibile din ESET LiveGrid®.

Activați sistemul de feedback ESET LiveGrid®

În plus față de sistemul bazat pe reputație ESET LiveGrid®, sistemul de feedback ESET LiveGrid® va colecta informații despre computer, corelate cu amenințările nou detectate. Este posibil ca aceste informații să includă:

- o mostră sau o copie a fișierului în care a apărut amenințarea,
- calea către fișierul respectiv,

- numele fișierului,
- data și ora,
- procesul cu ajutorul căruia amenințarea a apărut pe computer,
- informații despre sistemul de operare al computerului.

În mod implicit, ESET NOD32 Antivirus este configurat să trimită fișierele suspecte la laboratorul de viruși de la ESET pentru analizare detaliată. Fișierele cu extensii specifice, de exemplu *.doc* sau *.xls*, sunt întotdeauna excluse. De asemenea, puteți adăuga alte extensii, în cazul în care există fișiere specifice pe care dvs. sau organizația dvs. dorește să evite să le trimită.

Citiți mai multe despre trimiterea datelor relevante în Politica de confidențialitate.

Puteți opta să nu activați ESET LiveGrid®

Nu veți pierde nici o funcționalitate în software, dar în unele cazuri, ESET NOD32 Antivirus poate reacționa mai rapid la noile amenințări când este activată caracteristica ESET LiveGrid®. Dacă ați utilizat ESET LiveGrid® anterior și l-ați dezactivat, este posibil să mai fie pachete de date de trimis. Chiar și după dezactivare, astfel de pachete vor fi trimise către ESET. După trimiterea tuturor informațiilor curente, nu vor mai fi create alte pachete.

Citiți detalii despre ESET LiveGrid® în Glosar.
Consultați instrucțiunile noastre ilustrate disponibile în limba engleză și în alte câteva limbi referitoare la activarea sau dezactivarea ESET LiveGrid® în ESET NOD32 Antivirus.

Configurarea protecției bazate pe cloud în Setare avansată

Pentru a accesa setările pentru ESET LiveGrid®, deschideți **Setare avansată** (F5) > **Motor de detecție** > **Protecție bazată pe cloud**.

- **Activare sistem bazat pe reputație ESET LiveGrid® (recomandat)** – sistemul bazat pe reputație ESET LiveGrid® îmbunătățește eficiența soluțiilor antimalware de la ESET comparând fișierele scanate cu baza de date de elemente din lista albă și lista neagră din cloud.

- **Activare sistem de feedback ESET LiveGrid®** – Trimite datele relevante (descrise în secțiunea **Trimiterea mostrelor** de mai jos), împreună cu rapoarte privind opririle neașteptate și statistici, către laboratorul de cercetare ESET, pentru analize suplimentare.

- **Trimiteți rapoartele privind opririle neașteptate și datele de diagnosticare** – Trimiteți date de diagnosticare aferente ESET LiveGrid®, cum ar fi rapoarte privind opririle neașteptate și imagini de memorie pentru module. Vă recomandăm să păstrați activată această opțiune, pentru a ajuta ESET să diagnosticheze problemele, să îmbunătățească produsele și să asigure o protecție mai bună pentru utilizatorii finali.

- **Trimitere statistici anonime** – permiteți ESET să colecteze informații despre amenințările noi detectate, cum ar fi numele amenințării, data și ora detectării, metoda de detectare și metadatele asociate și versiunea și configurația produsului, inclusiv informații despre sistemul dvs.

- **Email de contact (opțional)** – Email-ul dvs. de contact se poate include împreună cu fișierele suspecte și

poate fi folosit pentru a vă contacta dacă sunt necesare informații suplimentare pentru analiză. Veți primi un răspuns de la ESET numai dacă sunt necesare informații suplimentare.

Trimiterea mostrelor

Trimitere manuală a mostrelor – Vă permite să trimiteți manual mostre către ESET din meniul contextual, din Carantină sau folosind opțiunea Instrumente.

Trimiterea automată a mostrelor detectate

Selectați ce fel de mostre vor fi trimise la ESET pentru analiză și pentru a îmbunătăți detectări viitoare (în mod implicit, mostra trebuie să aibă maximum 64 MB). Sunt disponibile următoarele opțiuni:

- **Toate mostrele detectate** – Toate obiectele detectate de motorul de detecție (inclusiv aplicații potențial nedorite, dacă această opțiune este activată în setările scanerului).
- **Toate mostrele, cu excepția documentelor** – Toate obiectele detectate, cu excepția **Documentelor** (vedeți mai jos).
- **Nu se trimit** – Obiectele detectate nu vor fi trimise către ESET.

Trimiterea automată a mostrelor suspecte

Aceste mostre vor fi trimise către ESET și în cazul în care motorul de detecție nu le-a detectat. De exemplu, atunci când mostrele au ratat de puțin detectarea sau atunci când modulele de protecție ESET NOD32 Antivirus consideră mostrele respective ca fiind suspecte sau comportându-se într-un mod neclar (în mod implicit, mostra trebuie să aibă maximum 64 MB).

- **Executabile** – Include fișiere executabile, cum ar fi .exe, .dll, .sys.
- **Arhive** – Include tipuri de fișiere de tip arhivă, cum ar fi .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.
- **Scripturi** – Include tipuri de fișiere de tip script, cum ar fi .bat, .cmd, .hta, .js, .vbs, .ps1.
- **Altele** – Include tipuri de fișiere cum ar fi .jar, .reg, .msi, .sfw, .lnk.
- **Eventuale mesaje de e-mail considerate spam** – Permite trimiterea unor părți ale unor eventuale mesaje de e-mail considerate ca fiind spam sau a mesajelor întregi cu atașări către ESET pentru a fi analizate. Activarea acestei opțiuni îmbunătățește detectarea globală a mesajelor spam, incluzând îmbunătățiri ale detectării mesajelor spam în viitor.
- **Documente** – Include documente Microsoft Office sau PDF, cu sau fără conținut activ.

Expandați pentru a vedea o listă cu toate tipurile de fișiere document incluse

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

Excluderi

Filtrul Excluderi vă permite să excludeți fișiere/directoare din trimitere (de exemplu, această opțiune poate fi utilă pentru a exclude fișiere care pot conține informații confidențiale, cum ar fi documente sau foi de calcul). Fișierele listate nu vor fi trimise niciodată spre analiză către laboratoarele ESET, chiar dacă acestea conțin cod suspect. Tipurile de fișiere cele mai obișnuite sunt excluse în mod implicit (.doc etc.). Dacă doriți, le puteți adăuga în lista de fișiere excluse.

Pentru a exclude fișierele descărcate de pe `download.domain.com`, navigați la **Setare avansată** > **Motor de detecție** > **Protecție bazată pe cloud** > **Trimiterea mostrelor** și apăsați pe **Editare** lângă **Excluderi**. Adăugați excluderea pentru `.download.domain.com`.

Dimensiunea maximă a mostrelor (MO) – Definește dimensiunea maximă a mostrelor (1-64 MO).

Filtru de excluderi pentru protecția bazată pe cloud

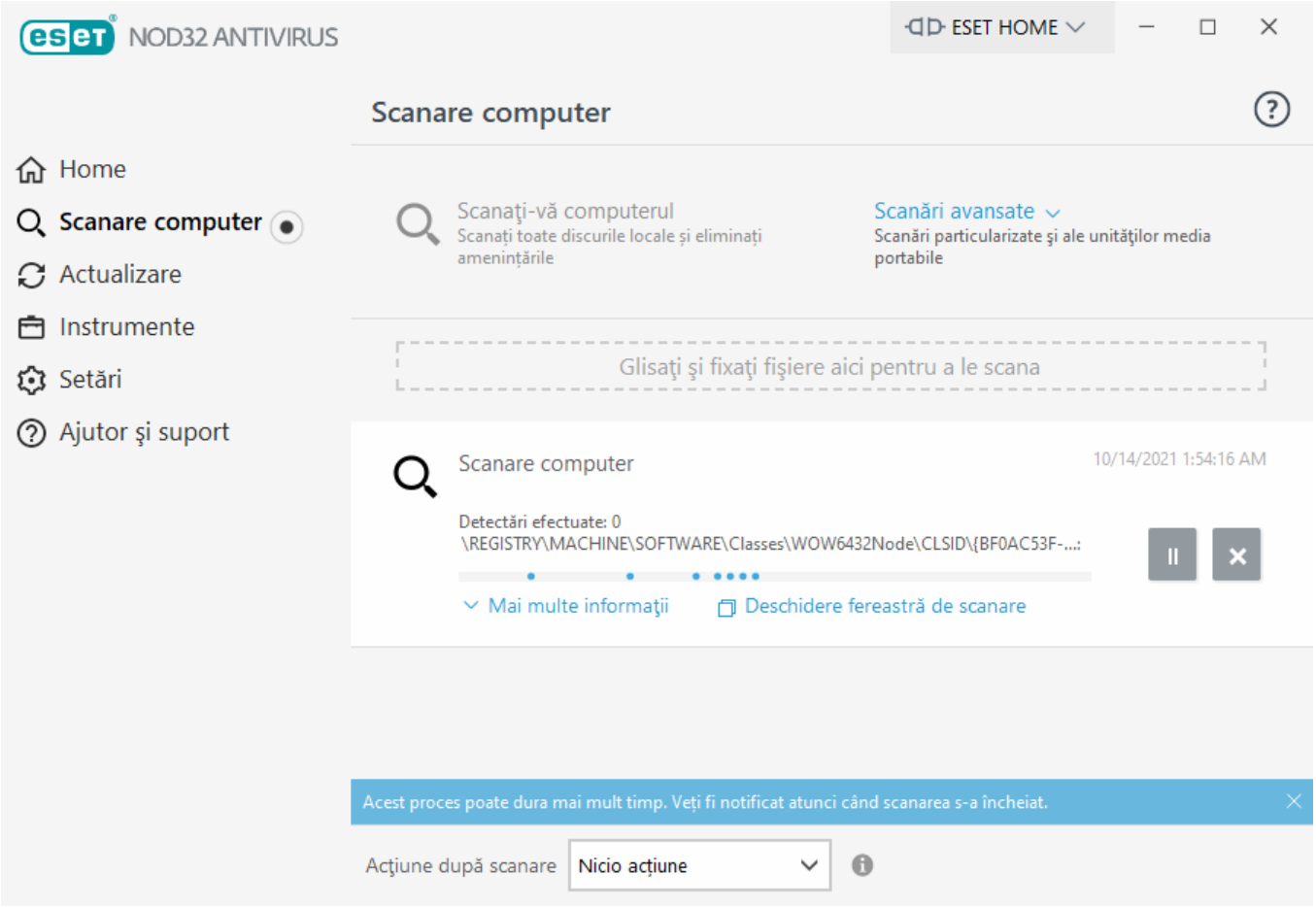
Filtrul de excluderi vă permite să excludeți anumite fișiere sau foldere atunci când trimiteți mostre. Fișierele listate nu vor fi trimise niciodată spre analiză către laboratoarele ESET, chiar dacă ele conțin cod suspect. Tipurile de fișiere obișnuite (cum ar fi .doc etc.) sunt excluse în mod implicit.

Această caracteristică poate fi utilă excluderea fișierelor care pot conține informații confidențiale, precum documente sau foi de calcul.

Pentru a exclude fișierele descărcate de pe download.domain.com, faceți clic pe **Setare avansată** > **Motor de detecție** > **Protecție bazată pe cloud** > **Trimiterea mostrelor** > **Excluderi** și adăugați excluderea *download.domain.com*.

Scanare computer

Scanner-ul la cerere este o parte importantă a soluției antivirus. Este utilizat pentru a efectua scanări de fișiere și directoare din computer. Din punctul de vedere al securității, este esențial ca scanările computerului să fie efectuate regulat, ca parte a măsurilor de securitate de rutină, nu numai când se suspectează o infecție. Vă recomandăm să efectuați regulat scanări ale sistemului în profunzime pentru a detecta viruși care nu sunt detectați de componenta Protecție în timp real a sistemului de fișiere la scrierea pe disc. Acest lucru se poate întâmpla dacă modulul Protecție în timp real a sistemului de fișiere este dezactivat în momentul respectiv, motorul de detecție este vechi sau dacă fișierul nu este detectat ca virus când se salvează pe disc.



Sunt disponibile două tipuri de **Scanare computer**. Opțiunea **Scanați-vă computerul** scanează rapid sistemul, fără a fi necesară specificarea parametrilor de scanare. Opțiunea **Scanare particularizată** (sub Scanări avansate) vă permite să selectați dintre profilurile de scanare predefinite concepute pentru anumite locații și să alegeți ținte de scanare specifice.

Consultați Progres scanare pentru informații suplimentare despre procesul de scanare.

> În mod implicit, ESET NOD32 Antivirus încearcă să curețe sau să șteargă automat detectările găsite în timpul scanării computerului. În unele cazuri, dacă nu se poate efectua nicio acțiune, primiți o alertă interactivă și trebuie să selectați o acțiune de curățare (de exemplu, ștergere sau ignorare). Pentru a modifica nivelul de curățare și pentru informații mai detaliate, consultați Curățare. Pentru a revizui scanările anterioare, consultați Fișiere log.

Scanați-vă computerul

Opțiunea **Scanați-vă computerul** vă permite să lansați cu ușurință o scanare a computerului și să curățați fișierele infectate fără intervenția dvs. Avantajul opțiunii **Scanați-vă computerul** este simplitatea operării și lipsa necesității unei configurări detaliate a scanării. Această scanare verifică toate fișierele de pe unitățile locale și curăță și șterge automat infiltrările detectate. Nivelul de curățare este setat automat la valoarea implicită. Pentru informații mai detaliate despre tipurile de curățare, consultați Curățare.

Puteți, de asemenea, să utilizați caracteristica **Scanare cu glisare și fixare** pentru a scana un fișier sau un director deplasând indicatorul mouse-ului în zona marcată, ținând apăsat și apoi eliberând butonul mouse-ului. După aceea, aplicația este mutată în fundal.

La **Scanări avansate** sunt disponibile opțiunile de scanare următoare:

Scanare personalizată

Scanarea particularizată vă permite să specificați parametri de scanare precum țintele și metodele. Avantajul **scanării particularizate** constă în faptul că puteți configura parametrii în mod detaliat. Configurațiile pot fi salvate în profiluri de scanare definite de utilizator, care pot fi utile dacă scanarea se efectuează în mod repetat cu aceiași parametri.

Scanare unități media portabile

Similară cu opțiunea **Scanați-vă computerul** – lansează rapid o scanare a unităților media portabile (cum ar fi CD/DVD/USB) conectate în mod curent la computer. Acest lucru poate fi util când conectați o unitate flash USB la un computer și doriți să-i scanați conținutul pentru a detecta programele malware și alte amenințări eventuale.

Acest tip de scanare mai poate fi inițiat făcând clic pe **Scanare personalizată**, selectând **Unități media portabile** în meniul vertical **Ținte de scanare** și făcând clic pe **Scanare**.

Repetare ultima scanare

Vă permite să lansați rapid scanarea efectuată anterior, utilizând aceleași setări ca mai înainte.

Meniul vertical **Acțiune după scanare** vă permite să setați o acțiune care va fi efectuată automat după terminarea unei scanări:

- **Nicio acțiune** – nu se efectuează nicio acțiune după terminarea unei scanări.
- **Închidere** – computerul se închide după terminarea unei scanări.
- **Repornire** – se închid toate programele deschise și se repornește computerul după terminarea unei scanări.
- **Repornire dacă este necesar** - computerul repornește numai dacă acest lucru este necesar pentru a finaliza curățarea amenințărilor detectate.
- **Repornire forțată** – Forțează închiderea tuturor programelor deschise, fără a aștepta interacțiunea cu utilizatorul, și repornește computerul după terminarea unei scanări.
- **Repornire forțată, dacă este necesară** - computerul repornește numai dacă acest lucru este necesar pentru a finaliza curățarea amenințărilor detectate.
- **Repaus** – se salvează sesiunea dvs. și se plasează computerul într-o stare cu alimentare redusă pentru a se putea relua rapid lucrul.
- **Hibernare** – se ia tot ce se execută în memoria RAM și se mută într-un fișier special de pe unitatea de stocare fixă. Computerul se închide, însă, la următoarea pornire, va reveni în starea sa anterioară.

Acțiunile **Veghe** sau **Hibernare** sunt disponibile, în funcție de setările pentru „Alimentare și repaus” ale sistemului de operare sau de funcționalitățile computerului/laptopului. Rețineți că un computer aflat în starea de veghe este în continuare în funcțiune. Computerul continuă să execute funcții de bază și să utilizeze electricitate atunci când funcționează alimentat de la baterie. Pentru a menține durata de viață a bateriei, de exemplu, atunci când părăsiți biroul, vă recomandăm să utilizați opțiunea Hibernare.

Acțiunea selectată va fi demarată după ce toate scanările în curs de executare vor fi încheiate. Când selectați **Închidere** sau **Repornire**, o fereastră de dialog de confirmare va afișa o numărătoare inversă de 30 de secunde (faceți clic pe **Anulare** pentru a dezactiva acțiunea solicitată).

> Vă recomandăm să executați o scanare a computerului cel puțin o dată pe lună. Scanarea se poate configura ca sarcină programată în **Instrumente** > **Orar**. Cum programez o scanare săptămânală a computerului?

Lansator scanare particularizată

Puteți utiliza opțiunea Scanare particularizată pentru a scana memoria sistemului de operare, rețeaua sau anumite părți ale unui disc, nu întregul disc. Pentru aceasta, faceți clic pe **Scanări avansate** > **Scanare particularizată** și selectați ținte specifice din structura (de tip arbore) a directoarelor.

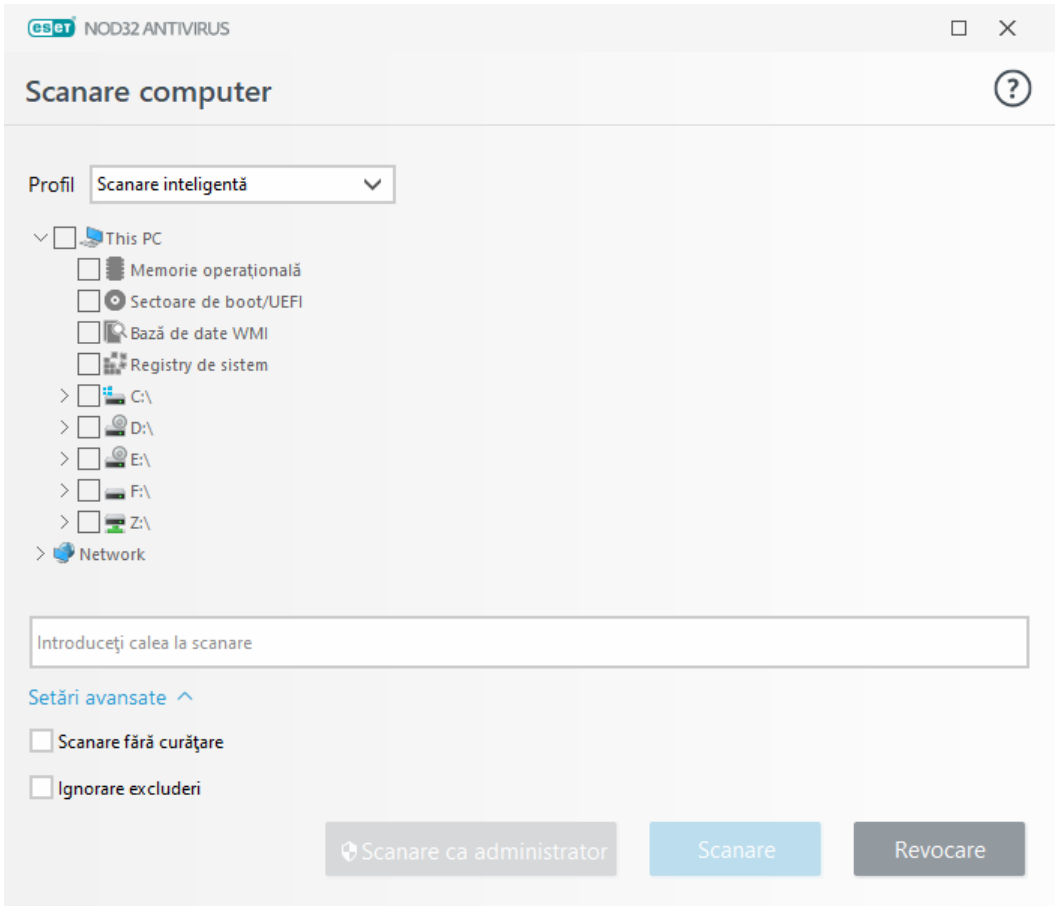
Puteți alege un profil în meniul vertical **Profil**, profil care va fi utilizat pentru scanarea anumitor ținte. Profilul implicit este **Scanare inteligentă**. Există încă trei profiluri de scanare predefinite numite **Scanare în profunzime**, **Scanare context menu** și **Scanare computer**. Aceste profiluri de scanare utilizează parametri ThreatSense diferiți. Opțiunile disponibile sunt descrise în secțiunea **Setări avansate** (F5) > **Motor de detecție** > **Scanări malware** > **Scanare la cerere** > Parametri ThreatSense.

Structura de foldere (arborele) conține și anumite ținte de scanare.

- **Memorie operațională** – Scanează toate procesele și datele utilizate în prezent de memoria operațională.
- **Sectoare de boot/UEFI** – Scanează sectoarele de boot și UEFI pentru prezența unor de programe malware. Citiți mai multe despre scanerul UEFI în glosar.
- **Baza de date WMI** – Scanează întreaga bază de date Windows Management Instrumentation (WMI), toate spațiile de nume, toate instanțele de clasă și toate proprietățile. Caută referințe la fișiere infectate sau programe malware încorporate ca date.
- **Registry de sistem** – Scanează întregul registry de sistem, toate cheile și subcheile. Caută referințe la fișiere infectate sau programe malware încorporate ca date. Când se curăță detectările, referința rămâne în registry, pentru a vă asigura că nu se vor pierde date importante.

Pentru a naviga rapid la o țintă de scanare (fișier sau folder), tastați calea acesteia în câmpul text de sub structura arbore. Calea este sensibilă la litere mari și mici. Pentru a include ținta în scanare, bifați caseta sa de selectare în structura arbore.

> Cum se programează o scanare săptămânală a computerului
> Pentru a programa o sarcină regulată, citiți capitolul Cum se programează o scanare săptămânală a computerului.



Puteți configura parametrii de curățare pentru scanare în **Setare avansată** (F5) > **Motor de detecție** > **Scanare la cerere** > **Parametri ThreatSense** > **Curățare**. Pentru a executa o scanare fără nicio acțiune de curățare, faceți clic pe **Setări avansate** și selectați **Scanare fără curățare**. Istoricul de scanare este salvat în jurnalul de scanare.

Dacă selectați **Ignorare excluderi**, fișierele cu extensiile excluse anterior vor fi scanate, fără excepție.

Faceți clic pe **Scanare** pentru a executa scanarea utilizând parametrii personalizați setați.

Scanare ca administrator vă permite să executați scanarea în contul de administrator. Utilizați această opțiune dacă utilizatorul curent nu deține privilegii pentru a accesa fișierele pe care doriți să le scanați. Acest buton nu este disponibil dacă utilizatorul curent nu poate apela operațiunile UAC ca Administrator.

Puteți vizualiza logul de scanare a computerului atunci când se finalizează o scanare făcând clic pe Afișare log.

Progres scanare

Fereastra progresului la scanare prezintă starea curentă a scanării și informații despre numărul de fișiere găsite care conțin cod dăunător.

Este normal ca unele fișiere, cum ar fi fișierele protejate prin parolă sau cele utilizate numai de către sistem (în general, fișierele *pagefile.sys* și anumite loguri), să nu poată fi scanate. Pentru detalii suplimentare, citiți articolul din baza noastră de cunoștințe.

> **Cum se programează o scanare săptămânală a computerului**
> Pentru a programa o sarcină regulată, citiți capitolul Cum se programează o scanare săptămânală a computerului.

Progres scanare – bara de progres prezintă starea obiectelor deja scanate comparativ cu obiectele ce urmează să fie scanate. Starea progresului scanării rezultă din numărul total de obiecte incluse la scanare.

Țintă – Numele obiectului scanat în mod curent și locația acestuia.

Amenințări găsite – afișează numărul total de fișiere scanate, amenințări găsite și amenințări curățate în timpul unei scanări.

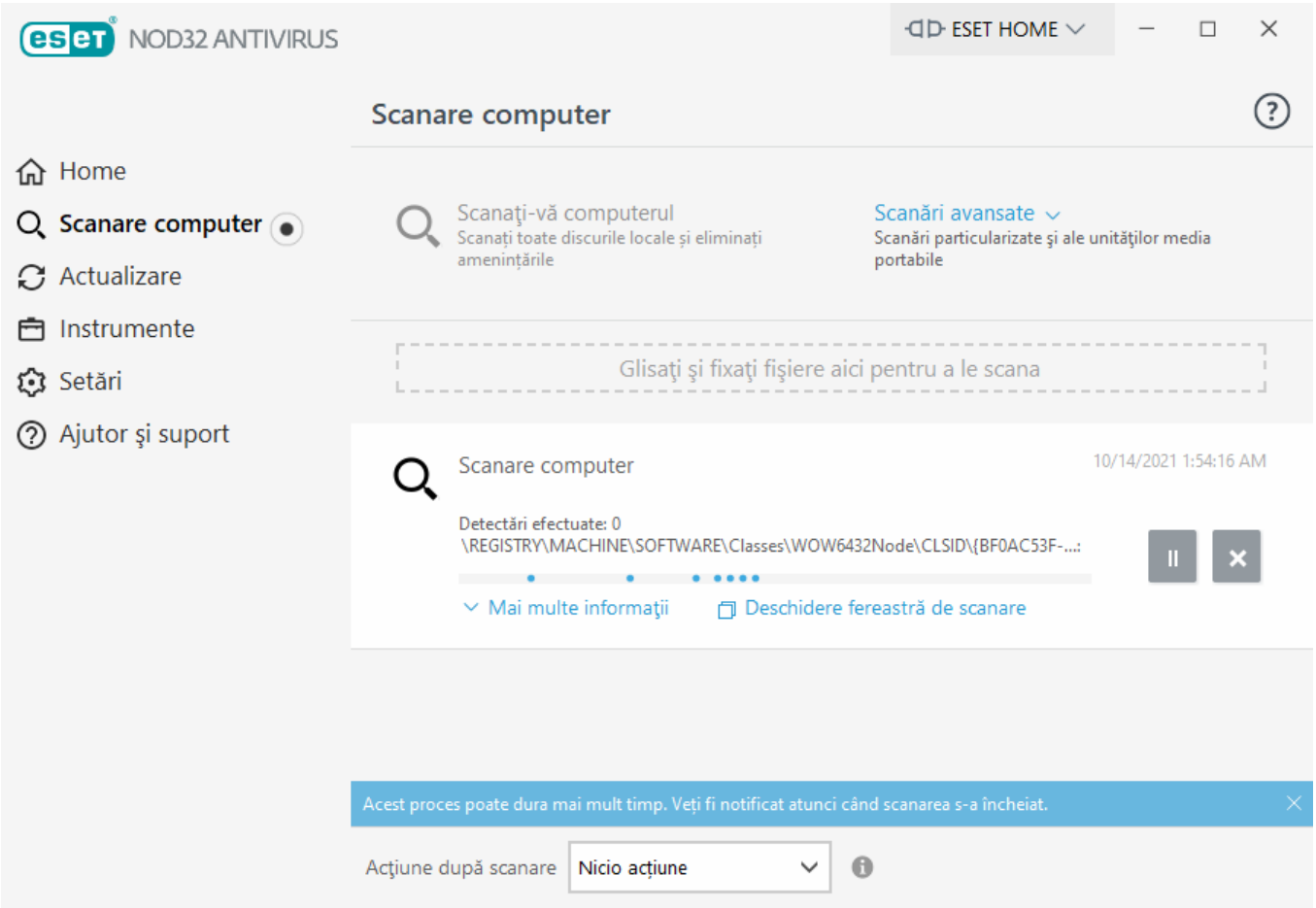
Pauză – Trece scanarea în pauză.

Reluare – această opțiune este vizibilă când s-a trecut în pauză progresul scanării. Faceți clic pe **Reluare** pentru a continua scanarea.

Oprire – Oprește scanarea.

Desfășurare log scanare – dacă se activează, logul de scanare se va desfășura automat în jos pe parcurs ce se adaugă înregistrări noi, astfel încât sunt vizibile cele mai recente înregistrări.

> Faceți clic pe lupă sau pe săgeată pentru a afișa detaliile despre scanarea care se execută în momentul respectiv. Puteți executa altă scanare paralelă făcând clic pe **Scanați computerul** sau **Scanări avansate** > **Scanare particularizată**.



Meniul vertical **Acțiune după scanare** vă permite să setați o acțiune care va fi efectuată automat după terminarea

unei scanări:

- **Nicio acțiune** – nu se efectuează nicio acțiune după terminarea unei scanări.
- **Închidere** – computerul se închide după terminarea unei scanări.
- **Repornire** – se închid toate programele deschise și se repornește computerul după terminarea unei scanări.
- **Repornire dacă este necesar** - computerul repornește numai dacă acest lucru este necesar pentru a finaliza curățarea amenințărilor detectate.
- **Repornire forțată** – Forțează închiderea tuturor programelor deschise, fără a aștepta interacțiunea cu utilizatorul, și repornește computerul după terminarea unei scanări.
- **Repornire forțată, dacă este necesară** - computerul repornește numai dacă acest lucru este necesar pentru a finaliza curățarea amenințărilor detectate.
- **Repaus** – se salvează sesiunea dvs. și se plasează computerul într-o stare cu alimentare redusă pentru a se putea relua rapid lucrul.
- **Hibernare** – se ia tot ce se execută în memoria RAM și se mută într-un fișier special de pe unitatea de stocare fixă. Computerul se închide, însă, la următoarea pornire, va reveni în starea sa anterioară.

> Acțiunile **Veghe** sau **Hibernare** sunt disponibile, în funcție de setările pentru „Alimentare și repaus” ale sistemului de operare sau de funcționalitățile computerului/laptopului. Rețineți că un computer aflat în starea de veghe este în continuare în funcțiune. Computerul continuă să execute funcții de bază și să utilizeze electricitate atunci când funcționează alimentat de la baterie. Pentru a menține durata de viață a bateriei, de exemplu, atunci când părăsiți biroul, vă recomandăm să utilizați opțiunea Hibernare.

Acțiunea selectată va fi demarată după ce toate scanările în curs de executare vor fi încheiate. Când selectați **Închidere** sau **Repornire**, o fereastră de dialog de confirmare va afișa o numărătoare inversă de 30 de secunde (faceți clic pe **Anulare** pentru a dezactiva acțiunea solicitată).

Log scanare computer

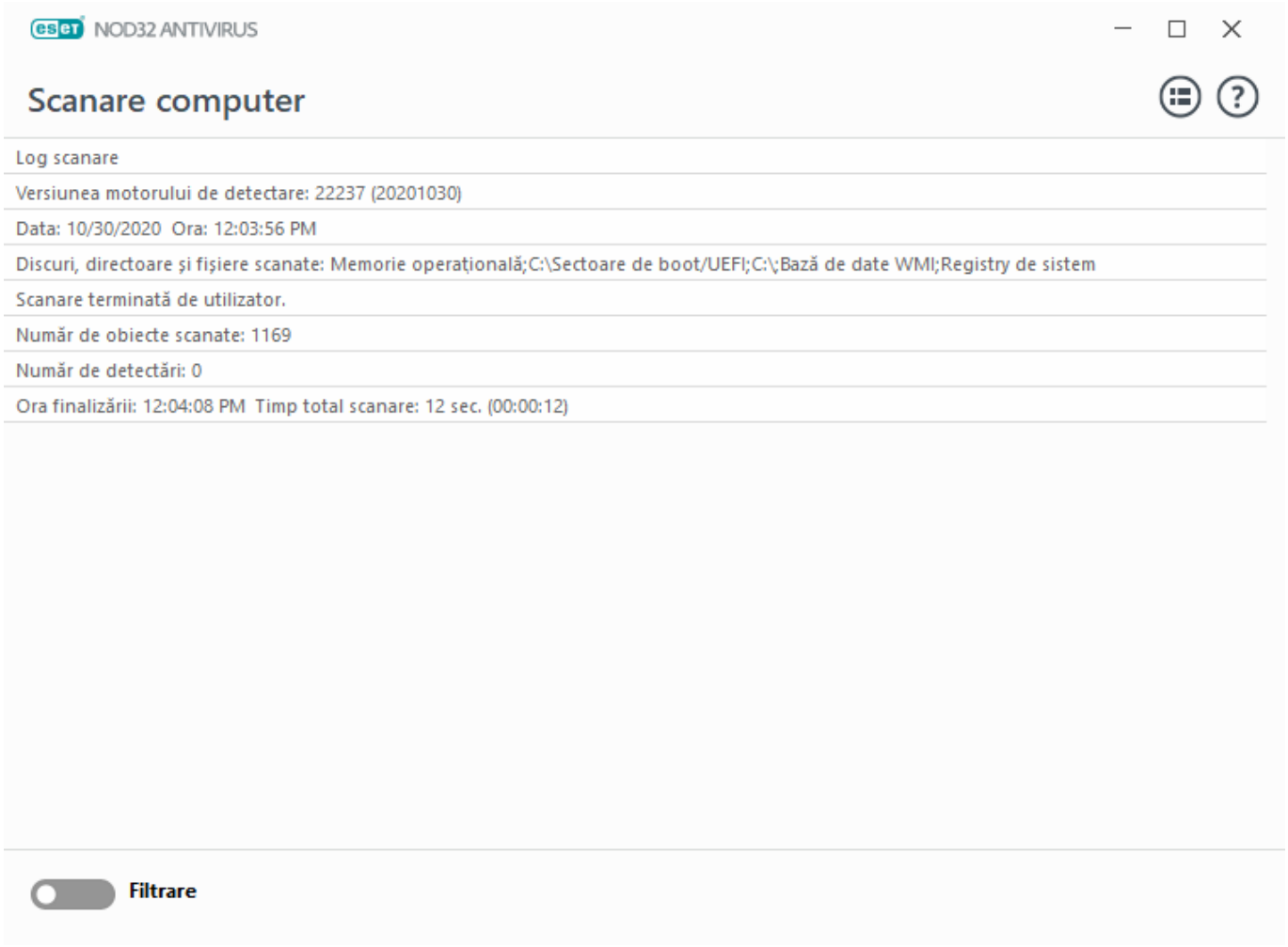
După finalizarea scanării, se deschide fereastra Log scanare computer cu toate informațiile relevante legate de această scanare particulară. Logul de scanare vă oferă informații precum:

- Versiunea motorului de detecție
- Data și ora de începere
- Listă cu discurile, directoarele și fișierele scanate
- Numele scanării planificate (numai pentru scanare planificată)
- Stare scanare
- Numărul de obiecte scanate
- Număr de detectări găsite

- Ora finalizării
- Timpul total de scanare

> Se omite un nou început al unei activități de scanare programată a computerului dacă în continuare este în curs de executare aceeași sarcină programată care a fost executată anterior. Activitatea de scanare planificată omisă va crea un jurnal de scanare a computerului cu 0 obiecte scanate și cu starea **Scanarea nu a început, deoarece scanarea anterioară era încă în curs de executare**.

Pentru a găsi jurnale de scanare anterioare, în fereastra principală a programului, selectați **Instrumente** > **Fișiere log**. În meniul vertical, selectați **Scanare computer** și faceți clic dublu pe înregistrarea dorită.



> Pentru a afla mai multe despre înregistrările „imposibil de deschis”, „eroare la deschidere” și/sau „arhivă deteriorată”, consultați articolul nostru din baza de cunoștințe ESET.

Faceți clic pe pictograma barei cu glisor **Filtrare** pentru a deschide fereastra Filtrare Log, unde puteți rafina căutarea după criterii personalizate. Pentru a vedea meniul contextual, faceți clic dreapta pe fișierul log dorit:

Acțiune	Utilizare
Filtrare înregistrări de acelaşi tip	Activează filtrarea fișierelor log. Vor fi afișate doar înregistrările de același tip cu cea selectată.
Filtrați	Această opțiune deschide fereastra Filtrare log și va permite să definiți criterii de filtrare pentru înregistrări log specifice. Scurtătura este: `Ctrl+Shift+F`

Acțiune	Utilizare
Activare filtru	Activează setările filtrului. Dacă activați pentru prima dată filtrul, trebuie să definiți setări, după care se deschide fereastra Filtrare log.
Dezactivare filtru	Dezactivează filtrul (rezultat identic cu efectuarea unui clic pe comutatorul din partea de jos).
Copiere	Copiază în clipboard înregistrările evidențiate. Scurtătura este: `Ctrl+C`
Copiere tot	Copiază toate înregistrările din fereastră.
Exportare	Exportă înregistrările evidențiate în clipboard într-un fișier XML.
Exportare toate	Această opțiune exportă toate înregistrările din fereastră într-un fișier XML.
Descriere detectare	Deschide Enciclopedia amenințărilor ESET, care conține informații detaliate despre pericolele și simptomele infiltrării evidențiate.

Scanări malware

Secțiunea **Scanări malware** poate fi accesată în meniul **Setare avansată** (F5) > **Motor de detecție** > **Scanări malware** și oferă opțiuni pentru a selecta parametrii de scanare. Această secțiune cuprinde următoarele elemente:

Profil selectat – un anumit set de parametri utilizat de scanerul la cerere. Pentru a crea un profil nou, faceți clic pe **Editare** lângă **Listă de profiluri**. Consultați Profiluri de scanare pentru mai multe detalii.

Ținte de scanare – Dacă doriți să scanați numai o anumită țintă, puteți face clic **Editare** lângă **Ținte de scanare** și alegeți o opțiune din meniul vertical sau selectați anumite ținte din structura arbore a directorului. Consultați Ținte de scanare pentru mai multe detalii.

Parametri ThreatSense – opțiuni de setare avansată, cum ar fi extensii de fișier pe care doriți să le controlați, metode de detectare utilizate etc. Faceți clic pentru a deschide o filă cu opțiuni avansate pentru scanner

Scanare stare de inactivitate

Puteți activa scanarea în stare de inactivitate în **Setare avansată** sub **Motor de detecție** > **Scanări malware** > **Scanare în modul de repaus**.

Scanare stare de inactivitate

Activați bara cu glisor de lângă **Activare scanare în stare de inactivitate** pentru a activa această caracteristică. Când computerul se află în stare de inactivitate, se efectuează o scanare silențioasă a computerului pentru toate unitățile de disc locale.

În mod implicit, scannerul în stare inactivă se execută când computerul (notebookul) este alimentat de la baterie. Puteți anula această setare activând bara cu glisor de lângă opțiunea **Se execută chiar în cazul în care computerul este alimentat de la baterie** din Setări avansate.

Activați bara cu glisor de lângă **Activare înregistrare în log** în Setare avansată pentru ca rezultatul unei scanări a computerului să se înregistreze în secțiunea Fișiere log (în fereastra principală a programului faceți clic pe **Instrumente** > **Fișiere log** și selectați **Scanare computer** în meniul vertical **Log**).

Detectare stare de inactivitate

Consultați secțiunea Ce anume declanșează detectarea stării de inactivitate pentru lista completă a condițiilor care trebuie îndeplinite pentru a declanșa scanarea în stare de inactivitate.

Faceți clic pe Setare parametri motor ThreatSense pentru a modifica parametrii de scanare (de exemplu, metodele de detectare) pentru scanarea în stare de inactivitate.

Profiluri de scanare

Există 4 profiluri de scanare predefinite în ESET NOD32 Antivirus:

- **Scanare inteligentă** – Acesta este profilul implicit de scanare avansată. Profilul Scanare inteligentă utilizează tehnologia Optimizare inteligentă, care exclude fișierele care s-au dovedit a fi curate într-o scanare anterioară și care nu au fost modificate de la acea scanare. Acest lucru permite reducerea timpilor de scanare, cu un impact minim asupra securității sistemului.

- **Scanare context menu** – Puteți începe o scanare la cerere a oricărui fișier din meniul contextual. Profilul Scanare context menu vă permite să definiți o configurație de scanare care va fi utilizată atunci când lansați scanarea în acest fel.

- **Scanare în profunzime** – Profilul Scanare în profunzime nu utilizează optimizarea inteligentă în mod implicit, astfel că niciun fișier nu este exclus de la scanare când se folosește acest profil.

- **Scanare computer** – Acesta este profilul implicit utilizat în scanarea standard a computerului.

Parametrii dvs. preferați de scanare pot fi salvați pentru scanări viitoare. Vă recomandăm să creați câte un profil diferit (cu diverse ținte de scanare, metode de scanare și alți parametri) pentru fiecare scanare utilizată în mod regulat.

Pentru a crea un profil nou, deschideți fereastra Setări avansate (F5) și faceți clic pe **Motor de detecție** > **Scanări malware** > **Scanare la cerere** > **Listă de profiluri**. Fereastra **Manager profil** include meniul vertical **Profil selectat** cu profilurile de scanare existente și opțiunea de a crea un profil de scanare nou. Pentru ajutor privind crearea unui profil de scanare adecvat cerințelor dvs., consultați secțiunea Setare parametri motor ThreatSense pentru o descriere a fiecărui parametru pentru configurarea scanării.

> Să presupunem că doriți să creați propriul dvs. profil de scanare și configurația **Scanați computerul** este parțial adecvată, însă nu doriți să scanați pachete de rutină sau aplicații potențial periculoase și, de asemenea, doriți să aplicați **Remediați întotdeauna detectarea**. Introduceți numele profilului nou în fereastra **Manager profil** și faceți clic pe **Adăugare**. Selectați profilul nou din meniul vertical **Profil selectat**, modificați parametrii rămași astfel încât să îndeplinească cerințele dvs., apoi faceți clic pe **OK** pentru a salva profilul nou.

Ținte de scanare

Meniul vertical **Ținte de scanare** vă permite să selectați ținte de scanare predefinite.

- **După setările de profil** – selectează țintele specificate de către profilul de scanare selectat.
- **Medii portabile** – Selectează dischete, dispozitive de stocare USB, CD/DVD.

- **Discuri locale** – Selectează toate unitățile de hard disk ale sistemului.
- **Discuri de rețea** – Selectează toate unitățile de rețea mapate.
- **Selecție personalizată** – Anulează toate selecțiile anterioare.

Structura de foldere (arborele) conține și anumite ținte de scanare.

- **Memorie operațională** – Scanează toate procesele și datele utilizate în prezent de memoria operațională.
- **Sectoare de boot/UEFI** – Scanează sectoarele de boot și UEFI pentru prezența unor de programe malware. Citiți mai multe despre scanerul UEFI în glosar.
- **Baza de date WMI** – Scanează întreaga bază de date Windows Management Instrumentation (WMI), toate spațiile de nume, toate instanțele de clasă și toate proprietățile. Caută referințe la fișiere infectate sau programe malware încorporate ca date.
- **Registry de sistem** – Scanează întregul registry de sistem, toate cheile și subcheile. Caută referințe la fișiere infectate sau programe malware încorporate ca date. Când se curăță detectările, referința rămâne în registry, pentru a vă asigura că nu se vor pierde date importante.

Pentru a naviga rapid la o țintă de scanare (fișier sau folder), tastați calea acesteia în câmpul text de sub structura arbore. Calea este sensibilă la litere mari și mici. Pentru a include ținta în scanare, bifați caseta sa de selectare în structura arbore.

Control dispozitiv

ESET NOD32 Antivirus asigură controlul automat asupra dispozitivelor (CD/DVD/USB/...). Acest modul vă permite să blocați sau să ajustați filtrele/permisiunile extinse și să definiți modul în care utilizatorul poate accesa și lucra cu un anumit dispozitiv. Acest lucru poate fi util dacă administratorul computerului dorește să prevină utilizarea dispozitivelor cu conținut nesolicitat.

Dispozitive externe acceptate:

- Stocare disc (HDD, disc amovibil USB)
- CD/DVD
- Imprimantă USB
- Stocare FireWire
- Bluetooth Dispozitiv
- Cititor de carduri inteligente
- Dispozitiv creare imagini
- Modem
- LPT/COM port

- Dispozitiv portabil
- Toate tipurile de dispozitive

Opțiunile de setare a controlului dispozitivului se poate modifica în **Setări avansate** (F5) > **Control dispozitiv**.

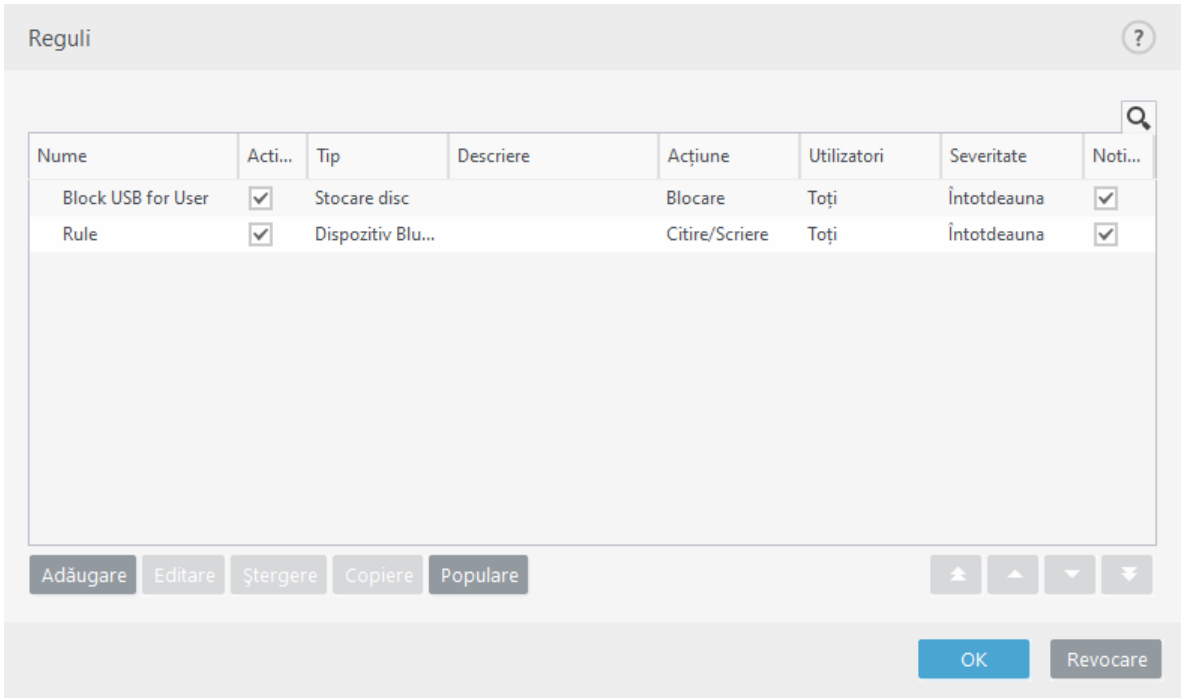
Activați bara cu glisor de lângă opțiunea **Activare control dispozitiv** pentru a activa caracteristica Control dispozitiv în ESET NOD32 Antivirus; va trebui să reporniți computerul pentru ca această modificare să intre în vigoare. După activarea caracteristicii Control dispozitiv, opțiunea **Reguli** va deveni activă, permițându-vă să deschideți fereastra Editor de reguli.

> Puteți crea diverse grupuri de dispozitive pentru care se vor aplica reguli diferite. De asemenea, puteți crea numai un singur grup de dispozitive pentru care va fi aplicată regula cu acțiunea **Citire/Scriere** sau **Numai citire**. Acest lucru asigură blocarea dispozitivelor nerecunoscute de funcția Control dispozitive atunci când sunt conectate la computerul dvs.

Dacă se introduce un dispozitiv care este blocat de o regulă existentă, se va afișa o fereastră de notificare și nu se va permite accesul la dispozitiv.

Editor reguli de control dispozitiv

Fereastra **Editor reguli de control dispozitiv** afișează regulile existente și permite controlul precis al dispozitivelor externe pe care utilizatorii le conectează la computer.



Anumite dispozitive pot fi permise sau blocate pentru un utilizator sau un grup de utilizatori, în funcție de parametri suplimentari pentru dispozitiv care se pot specifica în configurarea regulii. Lista regulilor cuprinde mai multe descrieri ale unei reguli, cum ar fi numele, tipul dispozitivului extern, acțiunea de efectuat după conectarea unui dispozitiv extern la computer și înregistrarea în log a gravității. Consultați și Adăugarea regulilor de control dispozitiv.

Faceți clic pe **Adăugare** sau pe **Editare** pentru a gestiona o regulă. Faceți clic pe **Copiere** pentru a crea o regulă nouă cu opțiuni predefinite utilizate pentru altă regulă selectată. Șirurile XML afișate când faceți clic pe o regulă se

pot copia în clipboard pentru a ajuta administratorii de sistem să exporte/importe și să utilizeze aceste date, de exemplu,în .

Apăsând pe **CTRL** și făcând clic puteți să selectați mai multe reguli și să aplicați acțiuni precum ștergerea sau mutarea acestora în sus sau în jos în listă, pentru toate regulile selectate. Caseta de selectare **Activată** dezactivează sau activează o regulă; acest lucru poate fi util dacă nu doriți să ștergeți definitiv regula, în cazul în care doriți să o utilizați ulterior.

Controlul este efectuat de reguli sortate în ordinea priorității, cu regulile cu cea mai mare prioritate la început.

Înregistrările din log se pot vizualiza în fereastra principală din ESET NOD32 Antivirus în **Instrumente**. > **Fișiere log**.

Logul Control dispozitiv înregistrează toate aparițiile unde este declanșată funcția Control dispozitiv.

Dispozitive detectate

Butonul **Populare** furnizează o prezentare generală a tuturor dispozitivelor conectate curent, precum și informații despre: tipul, vânzătorul, modelul și numărul de serie (dacă este disponibil) ale fiecărui dispozitiv.

Selectați un dispozitiv din lista Dispozitive detectate și faceți clic pe **OK** pentru a adăuga o regulă de control dispozitiv cu informații predefinite (toate setările pot fi ajustate).

Dispozitivele în modul putere redusă (repaus) sunt marcate cu o pictogramă de avertizare . Pentru a activa butonul **OK** și a adăuga o regulă pentru acest dispozitiv:

- Reconectați dispozitivul
- Utilizați dispozitivul (de exemplu, porniți aplicația Cameră în Windows pentru a trezi o cameră web)

Grupuri de dispozitive

⚠ Dispozitivul conectat la computerul dvs. poate constitui un risc de securitate.

Fereastra Grupuri de dispozitive este împărțită în două. Partea din dreapta a ferestrei conține o listă cu dispozitivele aparținând grupului respectiv, iar partea stângă conține grupurile create. Selectați un grup cu o listă de dispozitive care doriți să fie afișate în panoul din dreapta.

Atunci când deschideți fereastra Grupuri de dispozitive și selectați un grup, puteți adăuga sau elimina dispozitive din listă. Altă modalitate de a adăuga dispozitive la grup este importarea lor dintr-un fișier. Ca alternativă, puteți face clic pe butonul **Populare** pentru ca toate dispozitivele conectate la computerul dvs. să fie listate în fereastra **Dispozitive detectate**. Selectați un dispozitiv din lista populată pentru a-l adăuga la grup făcând clic pe **OK**.

Elemente de control

Adăugare – puteți adăuga un grup introducându-i numele sau puteți adăuga un dispozitiv la grupul existent (opțional, puteți specifica detalii precum numele producătorului, modelul și numărul de serie), în funcție de partea ferestrei unde ați făcut clic pe buton.

Editare – vă permite să schimbați numele grupului selectat sau parametrii dispozitivului (producător, model, număr de serie).

Ștergere – șterge grupul sau dispozitivul selectat în funcție de partea ferestrei unde ați făcut clic pe buton.

Import – importă o listă de dispozitive dintr-un fișier text. Importul dispozitivelor dintr-un fișier text necesită o formatare corectă:

- Fiecare dispozitiv începe pe un rând nou.
- **Furnizorul**, **Modelul** și **Numărul de serie** trebuie să fie prezente pentru fiecare dispozitiv și trebuie să fie separate prin virgulă.

Iată un exemplu de conținut pentru fișierul text:

```
Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101
```

Export – exportă o listă de dispozitive într-un fișier.

Butonul **Populare** furnizează o prezentare generală a tuturor dispozitivelor conectate curent, precum și informații despre: tipul, vânzătorul, modelul și numărul de serie (dacă este disponibil) ale fiecărui dispozitiv.

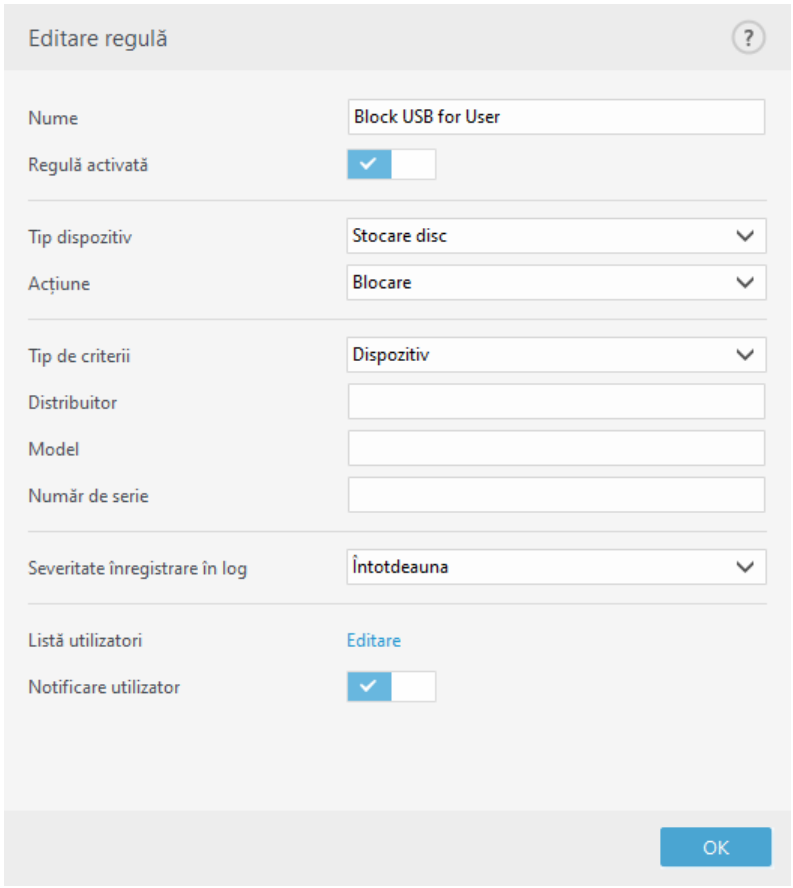
După ce terminați particularizarea, faceți clic pe **OK**. Faceți clic pe **Revocare** dacă doriți să părăsiți fereastra **Grupuri de dispozitive** fără a salva setările.

Puteți crea diverse grupuri de dispozitive pentru care se vor aplica reguli diferite. De asemenea, puteți crea numai un singur grup de dispozitive pentru care va fi aplicată regula cu acțiunea **Citire/Scriere** sau **Numai citire**. Acest lucru asigură blocarea dispozitivelor nerecunoscute de funcția Control dispozitive atunci când sunt conectate la computerul dvs.

Rețineți că nu sunt disponibile toate acțiunile (permisiunile) pentru toate tipurile de dispozitive. Dacă este un dispozitiv de stocare, sunt disponibile toate cele patru acțiuni. Pentru dispozitivele care nu sunt de stocare sunt disponibile numai trei acțiuni (de exemplu, acțiunea **Numai citire** nu este disponibilă pentru Bluetooth, deci accesul la dispozitive Bluetooth poate fi doar permis, blocat sau avertizat).

Adăugarea regulilor de control al dispozitivului

O regulă de control al dispozitivului definește acțiunea de efectuat atunci când la computer se conectează un dispozitiv care îndeplinește criteriile regulii.



Introduceți o descriere a regulii în câmpul **Nume** pentru o identificare mai bună. Faceți clic pe bara cu glisor de lângă opțiunea **Regulă activată** pentru a dezactiva sau a activa această regulă; acest lucru poate fi util dacă nu doriți să ștergeți regula definitiv.

Tip dispozitiv

Alegeți tipul de dispozitiv extern din meniul vertical (Disk storage/Portable device/Bluetooth/FireWire/...). Informațiile despre tipul de dispozitiv este colectat din sistemul de operare și poate fi văzut în managerul de dispozitive al sistemului dacă există un dispozitiv conectat la computer. Dispozitivele de stocare inclus discuri externe sau cititoare obișnuite de carduri de memorie conectate prin USB sau FireWire. Cititoarele de carduri inteligente inclus toate cititoarele de carduri inteligente cu un circuit integrat încorporat, cum ar fi cartelele SIM sau cartelele de autentificare. Exemple de dispozitive de creare a imaginilor sunt scanerele sau camerele. Deoarece aceste dispozitive furnizează informații numai despre acțiunile lor și nu despre utilizatori, ele pot fi blocate doar global.

Acțiune

Accesul la dispozitive fără stocare poate fi permis sau blocat. În schimb, regulile pentru dispozitive de stocare permit selectarea unuia dintre drepturile următoare:

- **Citire/Scriere** – va fi permis accesul complet la dispozitiv.
- **Blocare** – accesul la dispozitiv va fi blocat.
- **Numai citire** – va fi permis numai accesul pentru citirea de pe dispozitiv.
- **Avertizare** – de fiecare dată când un dispozitiv este conectat, utilizatorul va fi notificat dacă acesta este permis/blocat și se va crea o intrare în log. Dispozitivele nu sunt memorate și se vor afișa notificări la conectările ulterioare ale aceluiași dispozitiv.

Rețineți că nu sunt disponibile toate acțiunile (permisiunile) pentru toate tipurile de dispozitive. Dacă este un dispozitiv de stocare, sunt disponibile toate cele patru acțiuni. Pentru dispozitivele care nu sunt de stocare sunt disponibile numai trei acțiuni (de exemplu, acțiunea **Numai citire** nu este disponibilă pentru Bluetooth, deci accesul la dispozitive Bluetooth poate fi doar permis, blocat sau avertizat).

Tip de criterii

Selectați **Grup de dispozitive** sau **Dispozitiv**.

Parametrii suplimentari arătați mai jos pot fi utilizați pentru reglarea fină a regulilor și particularizarea acestora pentru anumite dispozitive. Parametrii nu fac diferențierea între literele mari și mici:

- **Vânzător** – filtrare după nume sau ID vânzător.
- **Model** – Numele dispozitivului.
- **Număr de serie** – dispozitivele externe au, în general, numere de serie proprii. În cazul unei unități CD/DVD, acesta este numărul de serie al unității media respective, nu al unității CD.

Dacă acești parametri nu sunt definiți, regula va ignora aceste câmpuri la verificarea potrivirii. Pentru parametrii de filtrare din toate câmpurile de text nu se face diferențierea între literele mari și mici și nu sunt acceptate metacaracterele (*, ?).

Pentru a vizualiza informații despre un dispozitiv, creați o regulă pentru tipul respectiv de dispozitiv, conectați dispozitivul la computer și apoi verificați detaliile despre dispozitiv în Log control dispozitiv.

Severitate înregistrare în log

ESET NOD32 Antivirus salvează toate evenimente importante într-un fișier log care poate fi vizualizat direct în meniul principal. Faceți clic pe **Instrumente** > **Fișiere log**, apoi selectați **Control dispozitiv** în meniul vertical **Jurnal scanare**.

- **Întotdeauna** – se înregistrează în log toate evenimentele.
- **Diagnostic** – înregistrează informațiile necesare pentru reglarea fină a programului.
- **Informații** – înregistrează mesajele informative, inclusiv mesajele privind actualizarea cu succes plus toate înregistrările de mai sus.
- **Avertisment** – înregistrează erori critice și mesaje de avertisment.
- **Niciunul** – nu se vor înregistra loguri.

Listă utilizatori

Regulile pot fi limitate la anumiți utilizatori sau anumite grupuri de utilizatori prin adăugarea lor în lista Utilizatori, apăsând pe **Editare** lângă **Listă utilizatori**.

- **Adăugare** – deschide fereastra de dialog **Tipuri de obiecte: Utilizatori sau grupuri**, care vă permite să selectați utilizatorii doriți.

- **Eliminare** – elimină utilizatorul selectat de la filtrare.

Limitări pentru lista de utilizatori

Lista de utilizatori nu poate fi definită pentru reguli cu anumite tipuri de dispozitive:

- Imprimantă USB
- Dispozitiv Bluetooth
- Cititor de carduri inteligente
- Dispozitiv creare imagini
- Modem
- Port LPT/COM

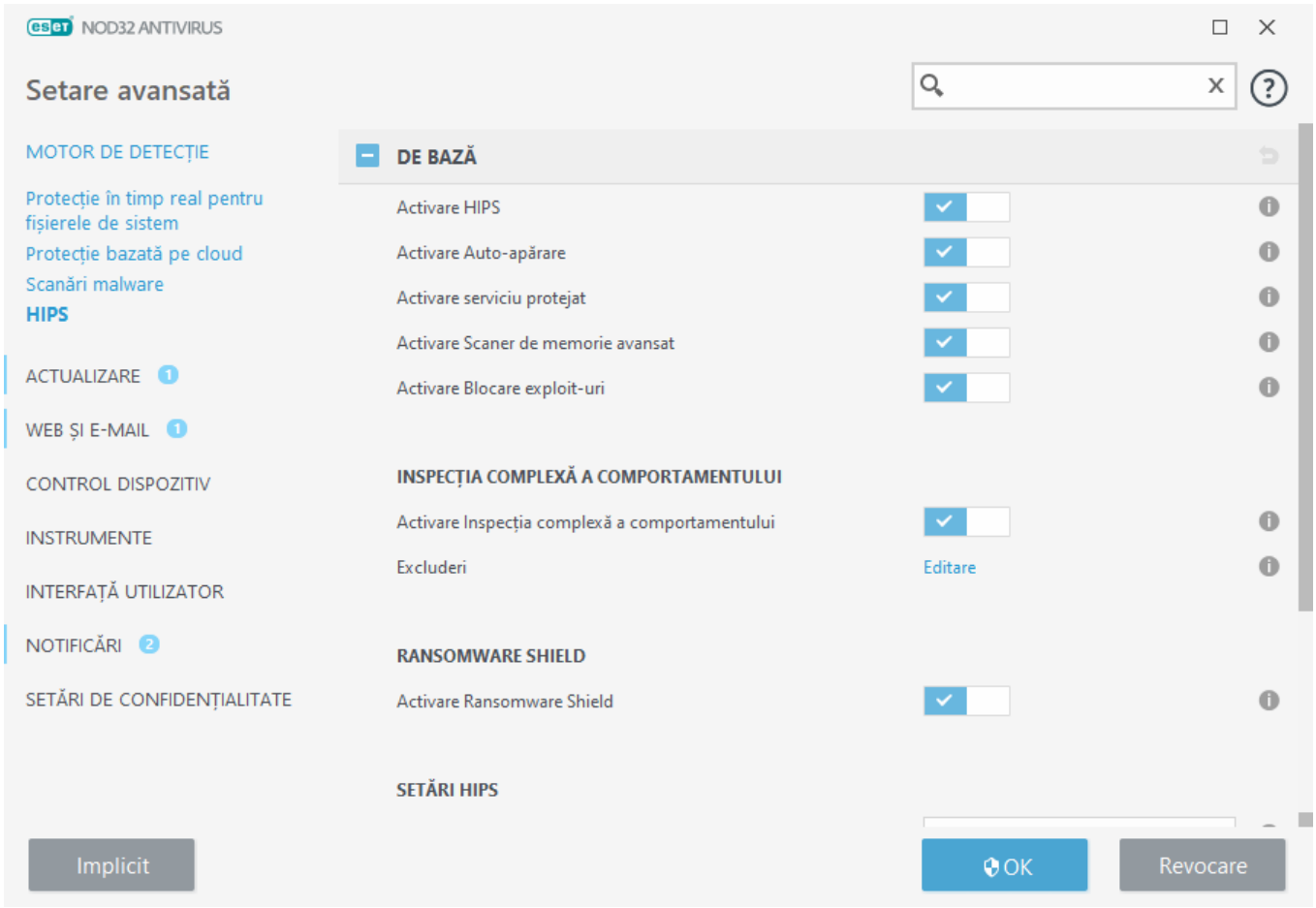
Notificare utilizator – Dacă se introduce un dispozitiv care este blocat de o regulă existentă, se va afișa o fereastră de notificare.

Componenta Sistem de prevenire a intruziunilor la nivel host (HIPS)

Modificarea setărilor pentru HIPS se va efectua numai de către un utilizator experimentat. Configurarea incorectă a setărilor pentru HIPS poate cauza instabilitatea sistemului.

Sistemul de protecție a gazdei împotriva intruziunilor (HIPS) vă protejează sistemul de programe malware și de activități nedorite care încearcă să vă afecteze negativ computerul. HIPS utilizează analiza comportamentală avansată împreună cu capacitatea de detectare a filtrului de rețea pentru a monitoriza procesele în curs de execuție, fișiere și chei de registry. HIPS este o componentă separată de protecția în timp real a sistemului de fișiere și nu este o protecție firewall; aceasta monitorizează numai procesele care se execută în cadrului sistemului de operare.

Setările pentru HIPS pot fi găsite în **Setări avansate** (F5) > **Motor de detecție** > **HIPS** > **De bază**. Starea HIPS (activat/dezactivat) este afișată în fereastra principală a programului ESET NOD32 Antivirus, în **Configurare** > **Protecție computer**.



De bază

Activare HIPS – HIPS este activat în mod implicit în ESET NOD32 Antivirus. Dezactivarea HIPS va dezactiva celelalte caracteristici HIPS, cum ar fi Blocare exploit-uri.

Activare Auto-apărare – ESET NOD32 Antivirus utilizează tehnologia încorporată **Auto-apărare** ca parte a HIPS, pentru a împiedica software-ul rău intenționat să deterioreze sau să dezactiveze protecția antivirus și antispyware. Auto-apărarea protejează împotriva modificărilor procesele critice de sistem ale ESET, cheile de registry și fișierele.

Activare serviciu protejat – activează protecția pentru serviciul ESET (ekrn.exe). Atunci când opțiunea este activată, serviciul este pornit ca proces Windows protejat, pentru a proteja de atacuri din partea programelor malware. Opțiunea este disponibilă în Windows 8.1 și versiuni ulterioare.

Activare scanner de memorie avansat lucrează în combinație cu opțiunea Blocare exploit-uri pentru a întări protecția împotriva programelor malware concepute să eludeze detectarea de către produsele antimalware utilizând confuzia sau criptarea. Scanerul de memorie avansat este activat în mod implicit. Citiți detalii despre acest tip de protecție în glosar.

Activare blocare exploit-uri este o opțiune concepută pentru a întări tipurile de aplicații exploatate frecvent, cum ar browserele web, cititoarele PDF, clienții de email și componentele MS Office. Blocarea exploit-urilor este activată în mod implicit. Citiți detalii despre acest tip de protecție în glosar.

Inspecția complexă a comportamentului

Activare Inspecția complexă a comportamentului – un nivel suplimentar de protecție care face parte din

caracteristica HIPS. Această extensie HIPS analizează comportamentul tuturor programelor care rulează pe computer și vă avertizează dacă comportamentul procesului este rău intenționat.

Opțiunea Excluderi HIPS de la Inspecția complexă a comportamentului vă permite să excludeți procese de la analiză. Pentru a vă asigura că sunt scanate toate procesele pentru detectarea posibilelor amenințări, vă recomandăm să creați excluderi numai dacă este absolut necesar.

Scut ransomware

Activare scut ransomware reprezintă un alt nivel de protecție care funcționează ca parte a caracteristicii HIPS. Trebuie să aveți activat sistemul bazat pe reputație ESET LiveGrid® pentru funcționarea Scutului ransomware. Citiți mai multe despre acest tip de protecție aici.

Setări HIPS

Mod de filtrare poate avea una dintre următoarele valori:

Mod de filtrare	Descriere
Mod Automat	Operațiunile sunt permise, cu excepția celor blocate de reguli predefinite care protejează sistemul.
Mod Inteligent	Utilizatorul va fi notificat numai despre evenimentele foarte suspecte.
Mod Interactiv	Utilizatorului i se va solicita confirmarea operațiunilor.
Mod bazat pe politici	Blochează toate operațiunile care nu sunt permise în mod explicit de o regulă.
Mod de învățare	Operațiunile sunt activate și se creează o regulă după fiecare operațiune. Regulile create în acest mod pot fi vizualizate în editorul **Reguli HIPS**, dar prioritatea acestora este mai mică decât cea a regulilor create manual sau a regulilor create în modul automat. Atunci când selectați **modul Învățare** din meniul vertical **Mod Filtrare**, setarea **Modul Învățare se va încheia pe** va deveni disponibilă. Selectați intervalul de activare a modului Învățare. După trecerea perioadei specificate, vi se va solicita să editați regulile create de HIPS în timp ce era în modul Învățare. De asemenea, puteți să alegeți alt mod de filtrare sau să amânați decizia și să continuați utilizarea modului Învățare.

Mod setat după expirarea modului Învățare – selectați modul de filtrare care va fi utilizat după expirarea modului Învățare. După expirare, opțiunea **Întrebare utilizator** necesită privilegii administrative pentru a modifica modul de filtrare HIPS.

Sistemul HIPS monitorizează evenimente din sistemul de operare și reacționează conform unor reguli similare celor utilizate de componenta Firewall. Faceți clic pe **Editare** lângă **Reguli** pentru a deschide editorul de **Reguli HIPS**. În fereastra regulilor HIPS puteți selecta, adăuga, edita sau elimina reguli. Detalii suplimentare despre crearea regulilor și operațiunile HIPS se pot găsi în secțiunea Editați o regulă HIPS.

Fereastra interactivă HIPS

Fereastra de notificare HIPS vă permite să creați o regulă în baza unor acțiuni noi pe care HIPS le detectează și să definiți apoi condițiile în care permiteți sau interziceți acțiunea respectivă.

Regulile create în fereastra de notificare sunt considerate echivalentul regulilor create manual. O regulă creată într-o fereastră de notificare poate fi mai puțin specifică decât regula care a declanșat fereastra de dialog

respectivă. Acest lucru înseamnă că, după crearea unei reguli în caseta de dialog, aceeași operațiune poate declanșa aceeași fereastră. Pentru mai multe informații, consultați Prioritatea regulilor HIPS.

Dacă acțiunea implicită pentru o regulă este setată la **Întreabă de fiecare dată**, se va afișa o fereastră de dialog de fiecare dată când se declanșează regula. Puteți alege **Interzicere** sau **Permitere** pentru operațiune. Dacă nu alegeți o acțiune în timpul acordat, se selectează o acțiune nouă în funcție de reguli.

Opțiunea **Se memorează până la ieșirea din aplicație** face ca acțiunea (**Permitere/Refuzare**) să fie utilizată până la modificarea regulilor sau a modului de filtrare, până la actualizarea modulului HIPS sau până la repornirea sistemului. Regulile temporare se vor șterge după oricare dintre aceste trei acțiuni.

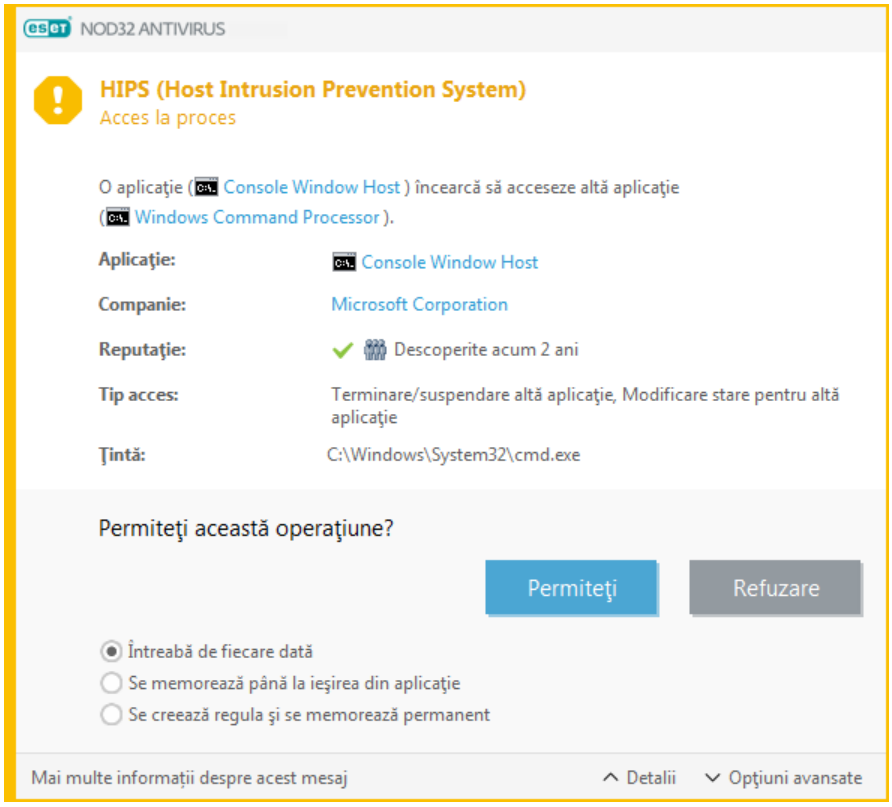
Opțiunea **Se creează regula și se memorează permanent** va crea o regulă HIPS nouă care poate fi modificată ulterior în secțiunea Gestionare regulă HIPS (acțiunea necesită privilegii de administrare).

Faceți clic pe **Detalii** în partea de jos pentru a vedea ce aplicație declanșează operațiunea, care este reputația fișierului sau pentru ce tip de operațiune vi se solicită să alegeți între permitere sau interzicere.

Setările pentru parametrii mai detaliați ai regulii pot fi accesate făcând clic pe **Opțiuni avansate**. Opțiunile de mai jos sunt disponibile dacă alegeți **Se creează regula și se memorează permanent**:

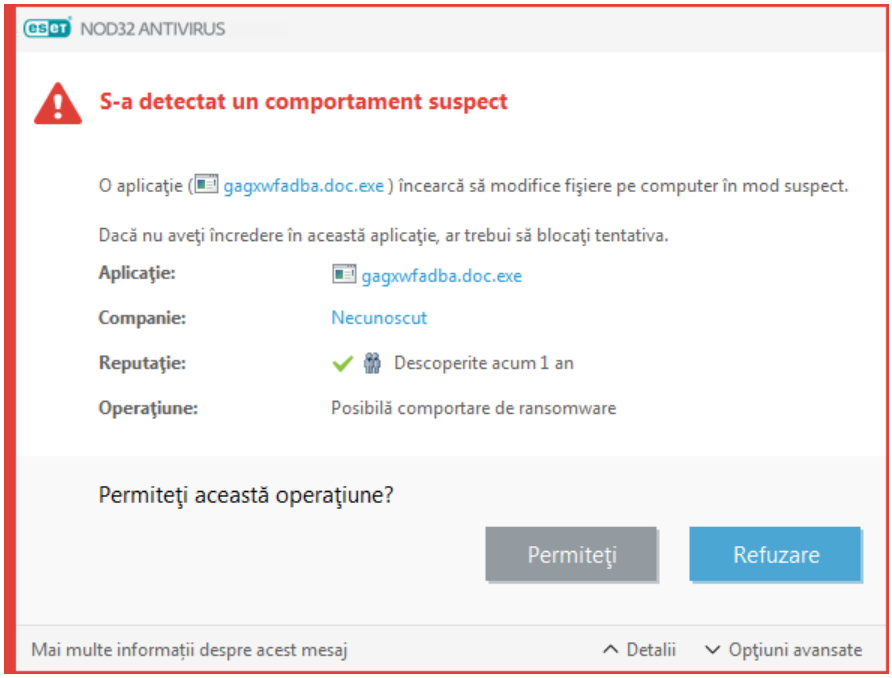
- **Creați o regulă valabilă numai pentru această aplicație** – dacă debifați această casetă de selectare, regula va fi creată pentru toate aplicațiile sursă.
- **Numai pentru operațiunea** – alegeți operațiunile pentru fișier/aplicație/regiștri din regulă. Consultați descrierile pentru toate operațiunile HIPS.
- **Numai pentru ținta** – alegeți țintele pentru fișier/aplicație/regiștri din regulă.

> **Notificări HIPS fără sfârșit?**
> Pentru a opri apariția notificărilor, schimbați modul de filtrare la **Mod Automat** în **Setare avansată** (F5) > **Motor de detecție** > **HIPS** > **De bază**.



S-a detectat un posibil comportament de ransomware

Această fereastră interactivă apare atunci când este detectat un posibil comportament de ransomware. Puteți alege **Interzicere** sau **Permitere** pentru operațiune.



Faceți clic pe **Detalii** pentru a vedea parametrii de detectare specifici. Fereastra de dialog permite acțiunile **Trimitere spre analiză** sau **Excludere de la detectare**.

Aplicația ESET LiveGrid® trebuie activată pentru ca Protecție antiransomware să funcționeze corespunzător.

Gestionare regulă HIPS

O listă cu regulile definite de utilizator și adăugate automat din sistemul HIPS. Detalii suplimentare despre crearea regulilor și operațiunile HIPS se pot găsi în capitolul Setări pentru regulă HIPS. Consultați și Principiul general al sistemului HIPS.

Coloane

Regulă – nume de regulă definit de utilizator sau ales automat.

Activată – Dezactivați bara cu glisor dacă doriți să păstrați regula în listă, dar nu doriți să o utilizați.

Acțiune – regula specifică o acțiune - **Permitere**, **Blocare** sau **Întreabă** – care trebuie efectuată dacă sunt îndeplinite condițiile.

Surse – regula se va utiliza numai dacă evenimentul este declanșat de o aplicație (sau aplicații).

Ținte – regula va fi utilizată numai dacă operațiunea este corelată cu un anumit fișier, o anumită aplicație sau o anumită intrare de registry.

Severitate înregistrare în log – dacă activați această opțiune, informațiile despre această regulă se vor scrie în Log HIPS.

Notificare – se afișează o fereastră pop-up mică în colțul din dreapta-jos dacă este declanșat un eveniment.

Elemente de control

Adăugare – creează o regulă nouă.

Editare – vă permite să editați intrările selectate.

Ștergere – elimină intrările selectate.

Prioritatea regulilor HIPS

Nu există opțiuni pentru ajustarea nivelului de prioritate pentru regulile HIPS folosind butoane sus/jos.

- Toate regulile pe care le creați au aceeași prioritate
- Cu cât o regulă este mai specifică, cu atât prioritatea ei este mai mare (de exemplu, o regulă pentru o anumită aplicație are o prioritate mai mare decât o regulă pentru toate aplicațiile)
- La nivel intern, HIPS conține reguli cu prioritate mai mare care nu vă sunt accesibile (de exemplu, nu puteți să anulați regulile definite pentru Auto-protecție)
- O regulă pe care o creați și care este posibil să vă blocheze sistemul de operare nu va fi aplicată (va avea prioritatea cea mai mică)

Editați o regulă HIPS

Consultați mai întâi secțiunea privind gestionarea regulilor HIPS.

Nume regulă – nume de regulă definit de utilizator sau ales automat.

Acțiune – specifică o acțiune – **Permitere**, **Blocare** sau **Întreabă** – care se va efectua dacă sunt corecte condițiile.

Operațiuni afectate – trebuie să selectați tipul de operațiune pentru care se va aplica regula. Regula se va utiliza numai pentru acest tip de operațiune și pentru ținta selectată.

Activată – dezactivați bara cu glisor dacă doriți să păstrați regula în listă, însă nu doriți să o aplicați.

Severitate înregistrare în log – dacă activați această opțiune, informațiile despre această regulă se vor scrie în Log HIPS.

Notificare utilizator – în colțul din dreapta, jos, se afișează o fereastră pop-up mică dacă se declanșează un eveniment.

Regula este formată din părți care descriu condițiile care declanșează această regulă:

Aplicații sursă– Regula se va utiliza numai dacă evenimentul este declanșat de această aplicație (sau aplicații). Selectați **Aplicații specifice** din meniul vertical și faceți clic pe **Adăugare** pentru a adăuga fișiere noi sau puteți selecta **Toate aplicațiile** din meniul vertical pentru a adăuga toate aplicațiile.

Fișiere țintă– regula se va utiliza numai dacă operațiunea este asociată acestei ținte. Selectați **Fișiere specifice** în meniul vertical și faceți clic pe **Adăugare** pentru a adăuga fișiere sau directoare noi sau puteți selecta **Toate fișierele** în meniul vertical pentru a adăuga toate fișiere.

Aplicații– regula se va utiliza numai dacă operațiunea este asociată acestei ținte. Selectați **Aplicații specifice** din meniul vertical și faceți clic pe **Adăugare** pentru a adăuga fișiere sau directoare noi sau puteți selecta **Toate aplicațiile** din meniul vertical pentru a adăuga toate aplicațiile.

Intrări de registry– regula se va utiliza numai dacă operațiunea este asociată acestei ținte. Selectați **Intrări specifice** în meniul vertical și faceți clic pe **Adăugare** pentru a o tasta manual sau puteți face clic pe **Deschidere editor registry** pentru a select o cheie din registry. De asemenea, puteți selecta **Toate intrările** din meniul vertical pentru a adăuga toate aplicațiile.

> Unele operațiuni ale regulilor specifice predefinite de HIPS nu se pot bloca și nu sunt permise în mod implicit. În plus, HIPS nu monitorizează toate operațiunile sistemului. HIPS monitorizează operațiunile care pot fi considerate periculoase.

Descrierea operațiunilor importante:

Operațiuni de fișier

- **Ștergere fișier** – aplicația solicită permisiune pentru a șterge fișierul țintă.
- **Scriere în fișier** – aplicația solicită permisiune pentru a scrie în fișierul țintă.
- **Acces direct la disc** – aplicația încearcă să citească de pe/să scrie pe un disc într-o modalitate

nestandardizată, care va ocoli procedurile obișnuite din Windows. Acest lucru poate duce la fișiere modificate fără aplicarea regulii corespunzătoare. Această operațiune poate fi provocată de un cod dăunător care încearcă să eludeze detectarea, de un software de copiere de rezervă care încearcă să efectueze o copie exactă a discului sau de un manager de partiție care încearcă să reorganizeze volumele discului.

- **Instalare racord global** – se referă la apelarea funcției SetWindowsHookEx din biblioteca MSDN.

- **Încărcare driver** – instalare și încărcare de drivere în sistem.

Operațiuni legate de aplicații

- **Depanare altă aplicație** – atașare a unui depanator la proces. La depanarea unei aplicații, se pot vizualiza și modifica multe detalii ale comportamentului acesteia și i se pot accesa datele.

- **Interceptare evenimente de la altă aplicație** – aplicația sursă încearcă să surprindă evenimentele vizate la o anumită aplicație (de exemplu, un program de înregistrare a apăsărilor de taste care încearcă să surprindă evenimentele de browser).

- **Terminare/suspendare altă aplicație** – suspendare, reluare sau terminare a unui proces (se poate acces direct din Explorer procese sau din panoul Procese).

- **Pornire aplicație nouă** – pornire a unei aplicații noi sau a unui proces nou.

- **Modificare stare pentru altă aplicație** – aplicația sursă încearcă să scrie în memoria aplicației țintă sau să execute un cod în numele acesteia. Această funcționalitate poate fi utilă pentru a proteja o aplicație esențială prin configurarea acesteia ca aplicație țintă într-o regulă care blochează utilizarea acestei operațiuni.

> Nu se pot intercepta operațiuni de proces pe versiunea de Windows XP pe 64 de biți.

Operațiuni legate de registry

- **Modificare setări pornire** – orice modificare a setărilor care definesc aplicațiile care se vor executa la pornirea sistemului Windows. Acestea se pot găsi, de exemplu, căutând cheia Run în registry Windows.

- **Ștergere din registry** – ștergere a unei chei de registry sau a valorii acesteia.

- **Redenumire cheie registry** – redenumire a unor chei de registry.

- **Modificare registry** – creare a unor valori noi pentru cheile de registry, modificare a valorilor existente, mutare a datelor în structura de tip arbore a bazei de date sau setare a drepturilor de utilizator sau de grup pentru cheile de registry.

> Puteți utiliza metacaractere cu anumite restricții când introduceți o țintă. În locul unei anumite chei, se poate utiliza simbolul * (asterisc) în calea de registry. De exemplu, *HKEY_USERS*\software* poate însemna *HKEY_USER\.default\software*, dar nu *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*.
> *HKEY_LOCAL_MACHINE\system\ControlSet** nu este o cale corectă de cheie de registry. O cale de cheie de registry care conține * definește „această cale sau orice cale, la orice nivel, după simbolul respectiv”. Aceasta este singura modalitate de utilizare a metacaracterelor pentru țintele fișierelor. Mai întâi se evaluează partea specifică a unei căi și apoi calea după simbolul metacaracterului (*).

⚠ Dacă creați o regulă foarte generică, se va afișa avertismentul despre acest tip de regulă.

În exemplul următor, vom demonstra modul de restricționare a comportamentului nedorit a unei aplicații specifice:

1. Numiți regula și selectați **Blocare** (sau **Întrebare**, dacă preferați să alegeți mai târziu) în meniul vertical **Acțiune**.

2. Activați bara cu glisor de lângă **Notificare utilizator** pentru a afișa o notificare de fiecare dată când se aplică o regulă.

3. Selectați cel puțin o operațiune în secțiunea **Operațiuni afectate** pentru care se va aplica regula.

4. Faceți clic pe **Înainte**.

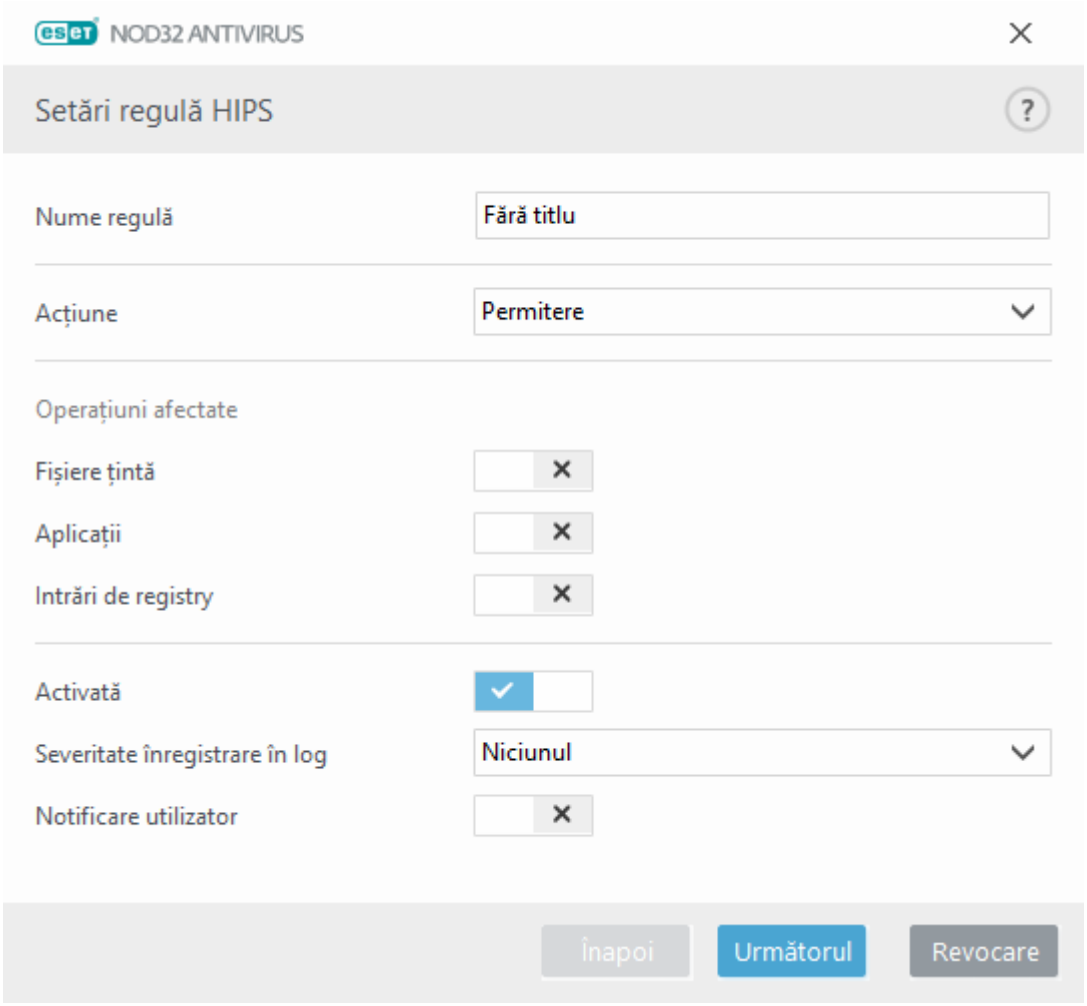
5. În fereastra **Aplicații sursă**, selectați **Aplicații specifice** din meniul vertical pentru a aplica regula nouă tuturor aplicațiilor care încearcă să efectueze oricare dintre operațiunile selectate asupra aplicațiilor specificate.

6. Faceți clic pe **Adăugare**, apoi pe **...** pentru a alege calea către o aplicație specifică, apoi apăsați pe **OK**. Dacă doriți, adăugați și alte aplicații.
Exemplu: *C:\Program Files (x86)\Untrusted application\application.exe*

7. Selectați operațiunea **Scriere în fișier**.

8. Selectați **Toate fișierele** în meniul vertical. Astfel toate încercările aplicațiilor selectate la pasul precedent de a scrie vreun fișier vor fi blocate.

9. Faceți clic pe **Terminare** pentru a salva regula nouă.



Adăugare aplicație/cale registry pentru HIPS

Selectați a calea fișierului unui aplicații făcând clic pe opțiunea **...**. Când selectați un director, se vor include toate aplicațiile din locația respectivă.

Opțiunea **Deschidere editor registry** va porni editorul de registry din Windows (regedit). Când adăugați o cale de registry, introduceți locația corectă în câmpul **Valoare**.

Exemple de cale de fișier sau registry:

- *C:\Program Files\Internet Explorer\iexplore.exe*
- *HKEY_LOCAL_MACHINE\system\ControlSet*

Setare avansată HIPS

Opțiunile următoare sunt utile pentru depanarea și analizarea comportamentului unei aplicații:

Încărcare drivere permisă întotdeauna – încărcarea driverelor selectate este permisă întotdeauna indiferent de modul de filtrare configurat, exceptând cazul când sunt blocate explicit de regula utilizatorului.

Înregistrați toate operațiunile blocate – Toate operațiunile blocate vor fi scrise în jurnalul HIPS. Utilizați această funcționalitate numai atunci când depanați sau când vi se solicită acest lucru de către asistența tehnică ESET,

deoarece poate genera un fișier jurnal imens și vă poate încetini computerul.

Notifică apariția modificărilor în aplicațiile lansate la pornirea sistemului – Afișează o notificare pe desktop de fiecare dată când o aplicație este adăugată la/eliminată de la pornirea sistemului.

Încărcare drivere permisă întotdeauna

Driverele arătate în această listă vor avea întotdeauna permisiune de încărcare, indiferent de modul de filtrare HIPS, cu excepția cazului când sunt blocate explicit de o regulă de utilizator.

Adăugare – adaugă un driver nou.

Editare – editează un driver selectat.

Eliminare – elimină un driver din listă.

Resetare – reîncarcă un set de drivere de sistem.

Faceți clic pe **Resetare** dacă nu doriți să fie incluse driverele pe care le-ați adăugat manual. Această acțiune poate fi utilă dacă ați adăugat mai multe drivere și nu le puteți șterge manual din listă.

Mod Gamer

Modul Gamer este o caracteristică destinată utilizatorilor de jocuri care doresc utilizarea neîntreruptă a software-ului, nu doresc să fie deranjați de ferestre pop-up și vor să minimizeze utilizarea CPU-ului. Modul Gamer se mai poate utiliza în timpul prezentărilor care nu pot fi întrerupte de activitatea antivirusului. Activând această caracteristică, toate ferestrele pop-up se dezactivează, iar activitatea Orarului va fi oprită în totalitate. Protecția sistemului se execută în continuare în fundal, dar nu necesită intervenția utilizatorului.

Puteți activa sau dezactiva modul Gamer în fereastra principală a programului, sub **Setare** > **Protecție computer** făcând clic pe  sau pe  lângă **Mod Gamer**. Activarea modului Gamer este un risc de securitate potențial; de aceea, pictograma stării protecției din bara de activități va deveni portocalie și se va afișa o avertizare. De asemenea, veți vedea acest avertisment în fereastra principală a programului, unde va apărea mesajul **Mod pentru jocuri activ** cu culoarea portocalie.

Selectați **Activați mod Gamer când se execută automat aplicații pe ecran complet** în **Setări avansate** (F5) > **Instrumente** > **Mod Gamer** pentru ca modul Gamer să pornească de fiecare dată atunci când deschideți o aplicație pe ecran complet și să se oprească după ce închideți aplicația.

Selectați **Dezactivați automat mod Gamer după** pentru a defini perioada de timp după care modul Gamer se va dezactiva în mod automat.

Scanare la pornire

În mod implicit, verificarea automată a fișierelor la pornire se va efectua la pornirea sistemului și la actualizarea motorului de detecție. Această scanare depinde de configurația și sarcinile orarului.

Opțiunile de scanare la pornire fac parte dintr-o sarcină a orarului, **Verificare fișiere la pornire sistem**. Pentru a-i modifica setările, navigați la **Instrumente** > **Orar**, faceți clic pe **Verificare automată fișiere la pornire** și pe **Editare**.

La ultimul pas se va afișa fereastra Verificare automată a fișierelor la pornire (consultați capitolul următor pentru detalii suplimentare).

Pentru instrucțiuni detaliate despre crearea și gestionarea sarcinii orarului, consultați Creare sarcini noi.

Verificare automată fișiere la pornire

Când creați o sarcină planificată de verificare a fișierelor la pornirea sistemului, aveți mai multe opțiuni de reglare a parametrilor următori:

Meniul vertical **Țintă de scanare** specifică adâncimea de scanare pentru fișierele executate la pornirea sistemului pe baza unui algoritm sofisticat. Fișierele sunt aranjate în ordine descrescătoare în funcție de următoarele criterii:

- **Toate fișierele înregistrate** (cel mai mare număr de fișiere scanate)
- **Fișiere utilizate rar**
- **Fișiere utilizate în mod obișnuit**
- **Fișiere utilizate frecvent**
- **Numai fișierele utilizate cel mai frecvent** (cel mai mic număr de fișiere scanate)

Mai sunt incluse două grupuri specifice:

- **Fișiere executate înainte de conectarea utilizatorului** – Conține fișiere din locații care pot fi accesate fără conectarea utilizatorului (include aproape toate locațiile de pornire a sistemului, cum ar fi serviciile, obiectele de ajutor în navigare, notificarea Winlogon, înregistrările din orarul Windows, fișiere dll cunoscute etc.).
- **Fișiere executate după conectarea utilizatorului** - Conține fișiere din locații care pot fi accesate numai după conectarea unui utilizator (include fișiere executate numai de un anumit utilizator, de obicei fișierele din *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Listele de fișiere care trebuie scanate sunt fixe pentru fiecare grup de mai sus. Dacă alegeți o adâncime de scanare mai mică pentru fișierele rulate la pornirea sistemului, fișierele care nu sunt scanate vor fi scanate la deschidere sau la executare.

Prioritate scanare – Nivelul priorității utilizate pentru a stabili când va începe scanarea:

- **La inactivitate** – sarcina se va efectua numai dacă sistemul este inactiv;
- **Cel mai scăzut** – când încărcarea sistemului este la cel mai scăzut nivel posibil;
- **Mai scăzut** – la o încărcare scăzută a sistemului;
- **Normal** – la o încărcare medie a sistemului.

Protecție documente

Caracteristica Protecție documente scanează documente Microsoft Office înainte de deschiderea acestora, dar și fișiere descărcate automat de Internet Explorer, cum ar fi elemente Microsoft ActiveX. Caracteristica Protecție documente vă oferă un nivel de protecție pe lângă protecția în timp real a sistemului de fișiere și se poate dezactiva pentru a îmbunătăți performanțele pe sistemele care nu gestionează un număr ridicat de documente Microsoft Office.

Pentru a activa Protecție documente, deschideți **Setare avansată** (F5) > **Motor de detecție** > **Scanări malware** > **Protecție documente** și faceți clic pe bara cu glisor de lângă **Activare Protecție documente**.

> Această caracteristică este activată de aplicații care utilizează Microsoft Antivirus API (de exemplu, Microsoft Office 2000 și versiuni ulterioare sau Microsoft Internet Explorer 5.0 și versiuni ulterioare).

Excluderi

Excluderile vă permit să excludeți obiecte de la motorul de detecție. Pentru a vă asigura că sunt scanate toate obiectele, vă recomandăm să creați excluderi numai dacă este absolut necesar. Există situații în care poate fi necesar să excludeți un obiect, de exemplu, atunci când scanarea unor înregistrări mari de baze de date ar încetini computerul în timpul unei scanări sau atunci când există programe software care intră în conflict cu scanarea.

Excluderile de performanță vă permit să excludeți de la scanare fișiere și directoare. Excluderile de performanță sunt utile pentru a exclude scanarea la nivel de fișier pentru jocuri sau atunci când scanarea ar provoca un comportament anormal al fișierului sau ar spori performanțele.

Excluderile de la detectare vă permit să excludeți de la detectare obiecte, folosind numele detectării, calea obiectului sau codul hash al obiectului. Excluderile de la detectare nu exclud fișiere și directoare de la scanare așa se întâmplă în cazul excluderilor de performanță. Excluderile de la detectare exclud obiecte numai atunci când acestea sunt detectate de către motorul de detecție și o regulă corespunzătoare este prezentă în lista de excluderi.

A nu se confunda cu alte tipuri de excluderi:

- Excluderi de procese – Toate operațiunile cu fișiere atribuite proceselor de aplicații excluse sunt excluse de la scanare (această opțiune ar putea fi necesară pentru a îmbunătăți viteza copierii de rezervă și disponibilitatea serviciului).
- Extensii de fișier excluse
- Excluderi HIPS
- Filtru de excluderi pentru protecția bazată pe cloud

Excluderi de performanță

Excluderile de performanță vă permit să excludeți de la scanare fișiere și directoare.

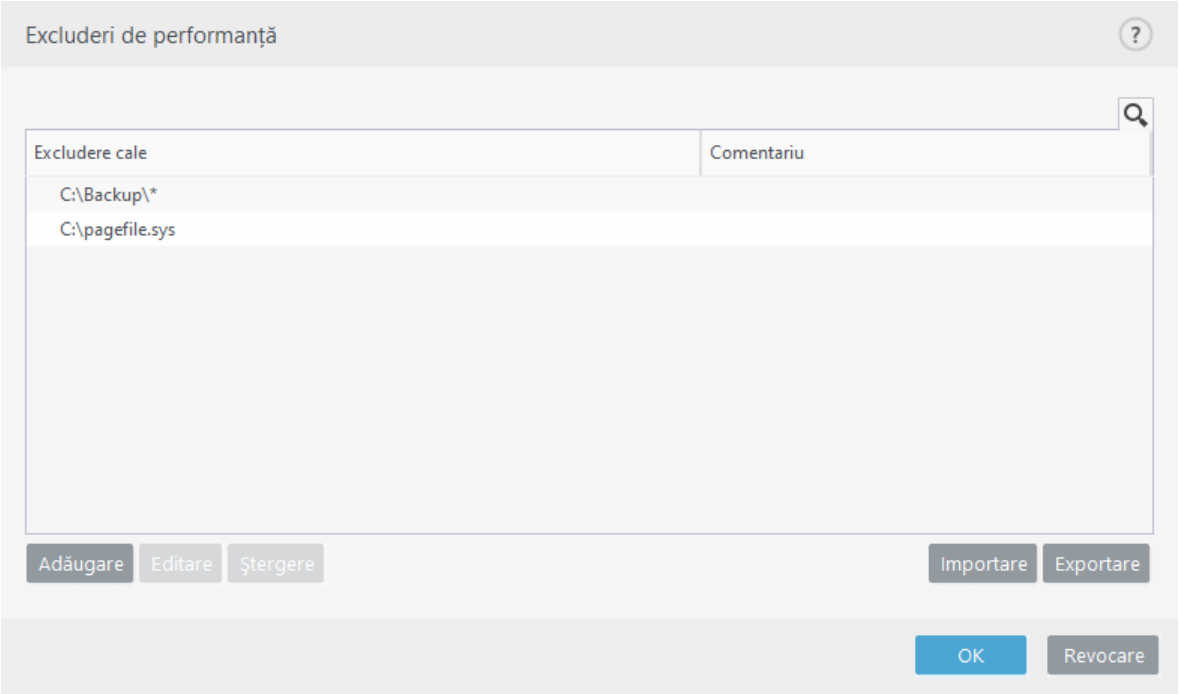
Pentru a vă asigura că sunt scanate toate obiectele pentru detectarea amenințărilor, vă recomandăm să creați excluderi numai dacă este absolut necesar. Totuși, există situații în care doriți să excludeți un obiect, de exemplu,

înregistrări mari de baze de date care ar încetini computerul în timpul scanării sau software care intră în conflict cu scanarea.

Puteți adăuga fișiere și directoare care să fie excluse de la scanare în lista de excluderi, în **Setare avansată** (F5) > **Motor de detecție** > **Excluderi** > **Excluderi de performanță** > **Editare**.

Nu confundați cu Excluderile de la detectare, Extensiile de fișiere excluse, Excluderile HIPS sau Excluderile de procese.

Pentru a exclude un obiect (cale: fișier sau director) de la scanare, faceți clic pe **Adăugare** și introduceți calea dorită sau selectați obiectul respectiv în structura arbore.



O amenințare dintr-un fișier nu va fi detectată de modulul **Protecție în timp real pentru fișierele de sistem** sau de modulul **Scanare computer** dacă un fișier întrunește criteriile de excludere de la scanare.

Elemente de control

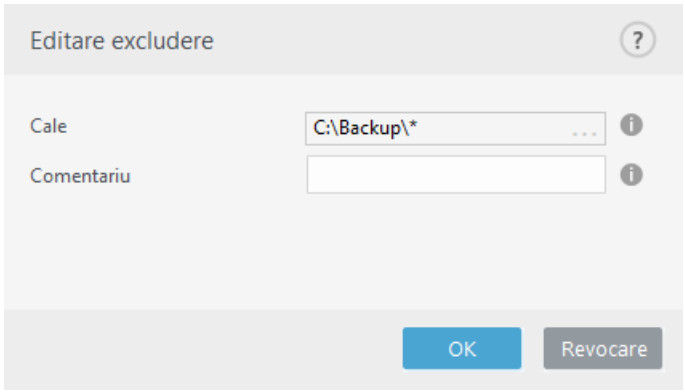
- **Adăugare** – exclude obiecte de la detectare.
- **Editare** – vă permite să editați intrările selectate.
- **Ștergere** – Elimină înregistrările selectate (folosiți CTRL + clic pentru a selecta înregistrări multiple).

Adăugarea sau editarea excluderilor de performanță

Această fereastră de dialog exclude o cale specifică (fișier sau director) pentru acest computer.

Alegerea unei căi sau introducerea manuală

Pentru a alege o cale adecvată, faceți clic pe **...** în câmpul **Cale**.
Atunci când introduceți în mod manual, vedeți mai jos mai multe exemple pentru formatul excluderilor.



Puteți utiliza metacaractere pentru a exclude un grup de fișiere. Un semn de întrebare (*?*) reprezintă un singur caracter, iar un asterisc (***) reprezintă un șir cu zero sau mai multe caractere.

Format excludere

• Dacă doriți să excludeți toate fișierele și subdirectoarele dintr-un director, introduceți calea către director și utilizați masca ***
• Dacă doriți să excludeți numai fișierele de tip doc, utilizați masca **.doc*
• Dacă numele unui fișier executabil are un anumit număr de caractere (și caracterele sunt diferite) și cunoașteți numai primul caracter (de exemplu „D"), folosiți următorul format:
D????.exe (semnele de întrebare înlocuiesc caracterele lipsă/necunoscute)

Exemple:
• *C:\Tools** – Calea trebuie să se încheie cu backslash (\) și asterisc (*) pentru a indica faptul că este vorba despre un director și întregul conținut al directorului (fișiere și subdirectoare) va fi exclus.
• *C:\Tools*.** – Același comportament ca și în cazul *C:\Tools**
• Directorul *C:\Tools* – *Tools* nu va fi exclus. Din punctul de vedere al scanerului, *Tools* poate fi și nume de fișier.
• *C:\Tools*.dat* – Se vor exclude fișierele .dat din directorul *Tools*.
• *C:\Tools\sg.dat* - Se va exclude acest fișier specific locat în calea exactă menționată.

Variabilele de sistem în excluderi

Puteți folosi variabile de sistem, cum ar fi %PROGRAMFILES%, pentru a defini excluderi de la scanare.
• Pentru a exclude directorul Program Files folosind această variabilă de sistem, folosiți calea *%PROGRAMFILES%** (nu uitați să adăugați o bară oblică inversă și un asterisc după cale) atunci când adăugați la excluderi.
• Pentru a exclude toate fișierele și directoarele dintr-un subdirector *%PROGRAMFILES%*, folosiți calea *%PROGRAMFILES%\Director_exclus**

Listă extinsă cu variabilele de sistem acceptate

Următoarele variabile pot fi folosite în formatul de excludere pentru căi:
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*

Nu sunt acceptate variabilele de sistem specifice utilizatorului (cum ar fi *%TEMP%* sau *%USERPROFILE%*) sau variabilele de mediu (precum *%PATH%*).

Metacaractere la mijlocul unei căi nu sunt acceptate

Utilizarea metacaracterelor la mijlocul unei căi (de *C:\Tools*\Data\file.dat* exemplu) este posibil să funcționeze, dar nu este acceptată oficial pentru excluderile de performanță. Consultați următorul articol din Baza de cunoștințe pentru mai multe informații.
Când utilizați excluderi de la detectare, nu există restricții privind utilizarea metacaracterelor la mijlocul unei căi.

Ordinea excluderilor

- Nu există opțiuni pentru ajustarea nivelului de prioritate pentru excluderi folosind butoanele sus/jos.
- Când scanerul găsește o corespondență pentru prima regulă aplicabilă, a doua regulă aplicabilă nu va mai fi evaluată.
- Cu cât sunt mai puține reguli, cu atât performanța la scanare este mai bună.
- Evitați crearea unor reguli concurente.

Formatul pentru excluderea unei căi

Puteți utiliza metacaractere pentru a exclude un grup de fișiere. Un semn de întrebare (*?*) reprezintă un singur caracter, iar un asterisc (*) reprezintă un șir cu zero sau mai multe caractere.

Format excludere

- Dacă doriți să excludeți toate fișierele și subdirectoarele dintr-un director, introduceți calea către director și utilizați masca *
- Dacă doriți să excludeți numai fișierele de tip doc, utilizați masca **.doc*
- Dacă numele unui fișier executabil are un anumit număr de caractere (și caracterele sunt diferite) și cunoașteți numai primul caracter (de exemplu „D”), folosiți următorul format:
D????.exe (semnele de întrebare înlocuiesc caracterele lipsă/necunoscute)

Exemple:

- *C:\Tools** – Calea trebuie să se încheie cu backslash (\) și asterisc (*) pentru a indica faptul că este vorba despre un director și întregul conținut al directorului (fișiere și subdirectoare) va fi exclus.
- *C:\Tools*.** – Același comportament ca și în cazul *C:\Tools**
- Directorul *C:\Tools* – *Tools* nu va fi exclus. Din punctul de vedere al scanerului, *Tools* poate fi și nume de fișier.
- *C:\Tools*.dat* – Se vor exclude fișierele .dat din directorul *Tools*.
- *C:\Tools\sg.dat* - Se va exclude acest fișier specific locat în calea exactă menționată.

Variabilele de sistem în excluderi

Puteți folosi variabile de sistem, cum ar fi %PROGRAMFILES%, pentru a defini excluderi de la scanare.

- Pentru a exclude directorul Program Files folosind această variabilă de sistem, folosiți calea *%PROGRAMFILES%** (nu uitați să adăugați o bară oblică inversă și un asterisc după cale) atunci când adăugați la excluderi.
- Pentru a exclude toate fișierele și directoarele dintr-un subdirector *%PROGRAMFILES%*, folosiți calea *%PROGRAMFILES%\Director_exclus**

Listă extinsă cu variabilele de sistem acceptate

Următoarele variabile pot fi folosite în formatul de excludere pentru căi:

- *%ALLUSERSPROFILE%*
- *%COMMONPROGRAMFILES%*
- *%COMMONPROGRAMFILES(X86)%*
- *%COMSPEC%*
- *%PROGRAMFILES%*
- *%PROGRAMFILES(X86)%*
- *%SystemDrive%*
- *%SystemRoot%*
- *%WINDIR%*
- *%PUBLIC%*

Nu sunt acceptate variabilele de sistem specifice utilizatorului (cum ar fi *%TEMP%* sau *%USERPROFILE%*) sau variabilele de mediu (precum *%PATH%*).

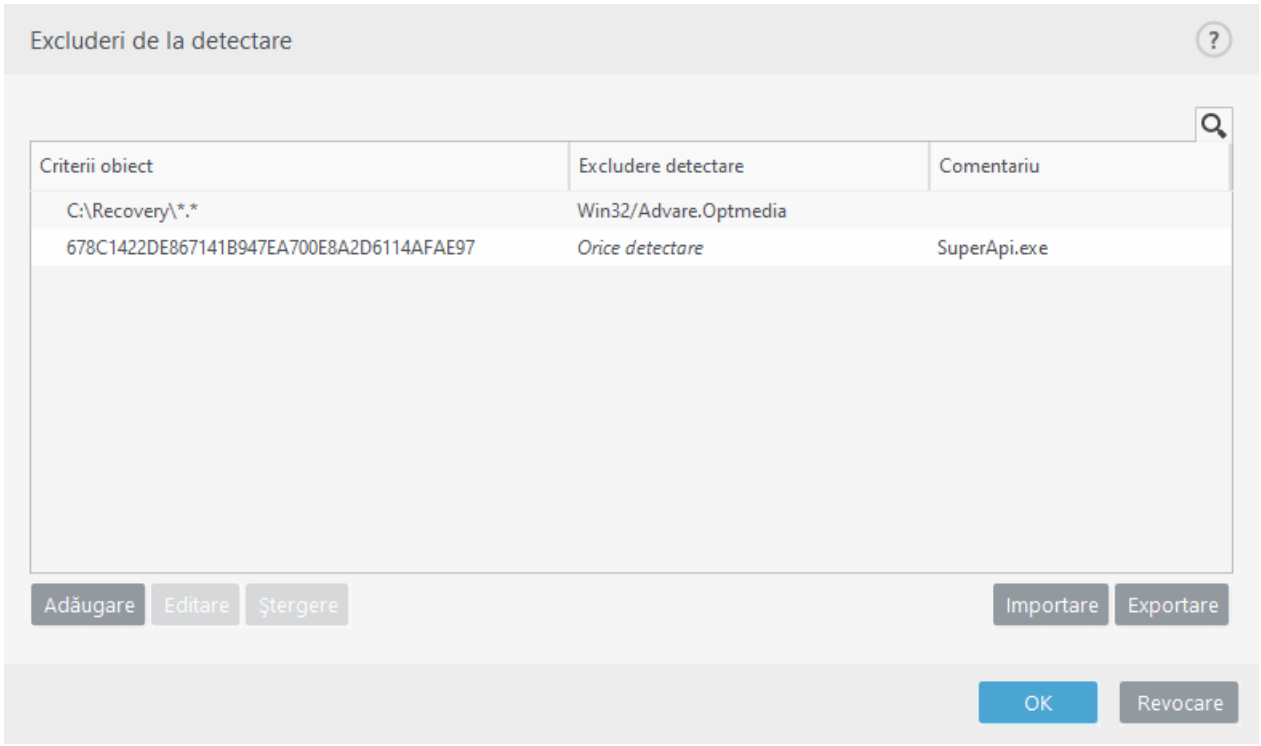
Excluderi de la detectare

Excluderile de la detectare vă permit să excludeți obiecte de la procesul de detectare filtrând după numele detectării, calea obiectului sau codul hash al obiectului.

Cum funcționează excluderile de la detectare

Excluderile de la detectare nu exclud fișiere și directoare de la scanare așa cum o face opțiunea Excluderi de performanță. Excluderile de la detectare exclud obiecte numai atunci când acestea sunt detectate de către motorul de detecție și o regulă corespunzătoare este prezentă în lista de excluderi.

De exemplu (în primul rând din imaginea de mai jos), atunci când un obiect este detectat ca Win32/Adware.Optmedia, iar fișierul detectat este *C:\Recovery\file.exe*. Pentru al doilea rând, fiecare fișier cu codul hash SHA-1 adecvat va fi exclus întotdeauna, indiferent de numele detectării.



Pentru a vă asigura că sunt detectate toate amenințările, vă recomandăm să creați excluderi pentru directoare numai atunci când acest lucru este absolut necesar.

Puteți adăuga fișiere și directoare care să fie excluse de la scanare în lista de excluderi, navigați la **Setare avansată** (F5) > **Motor de detecție** > **Excluderi** > **Excluderi de la detectare** > **Editare**.

> Nu confundați cu Excluderile de performanță, Extensiile de fișiere excluse, Excluderile HIPS sau Excluderile de procese.

Pentru a exclude un obiect (după numele detectării sau după codul hash) de la motor de detecție, apăsați pe **Adăugare**.

Pentru Aplicații potențial nedorite și Aplicații potențial periculoase, puteți crea și o excludere după numele detectării:

- În fereastra de avertizare care raportează detectarea (faceți clic pe **Afișare opțiuni avansate**, apoi selectați **Excludere de la detectare**).
- Din meniul contextual Fișiere log, utilizând Expertul pentru crearea unei excluderi de la detectare.
- Făcând clic pe **Instrumente** > **Carantină**, apoi făcând clic dreapta pe fișierul din carantină și selectând **Restaurare și excludere de la scanare** în meniul contextual.

Criterii pentru obiect la excluderi de la detectare

- **Cale** – Limită pentru o excludere de la detectare pentru o cale specificată (sau pentru toate căile).
- **Nume detectare** – Dacă lângă un fișier exclus există un nume de detectare, înseamnă că fișierul este exclus numai pentru detectarea dată, nu este exclus total. Dacă fișierul respectiv este infectat ulterior cu alte programe malware, el va fi detectat.
- **Hash** – Exclude un fișier pe baza codului hash specificat SHA-1, indiferent de tipul fișierului, de locația sau

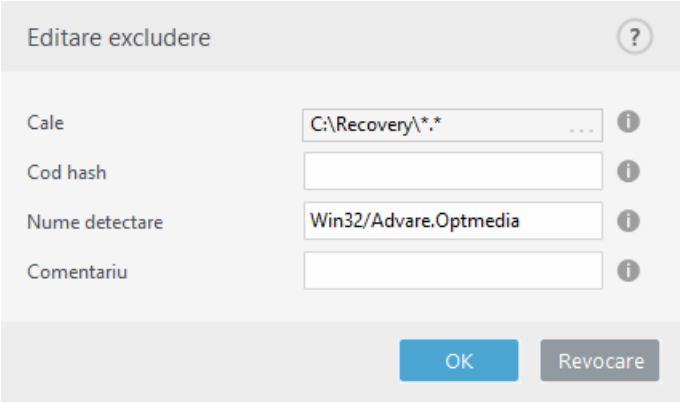
de extensia sa.

Adăugare sau editare excludere de la detectare

Excludere detectare

Trebuie să furnizați un nume ESET valid de detecție. Pentru nume de detecție valide, consultați Fișiere log, apoi selectați **Detectări** în meniul vertical Fișiere log. Opțiunea este utilă atunci când o mostră fals pozitivă este detectată de ESET NOD32 Antivirus. Excluderile unor infiltrări reale sunt foarte periculoase, ar trebui să aveți în vedere excluderea numai a fișierelor/directoarelor afectate apăsând pe **...** în câmpul **Cale** și/sau numai pentru o perioadă limitată. Excluderile se aplică și pentru aplicații potențial nedorite, aplicații potențial periculoase și aplicații suspecte.

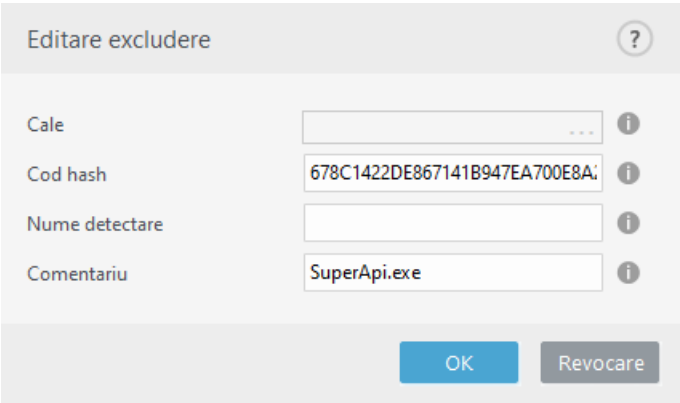
Consultați și Formatul pentru excluderea unei căi.



Consultați mai jos secțiunea Exemplu de excludere de la detectare.

Excludere cod hash

Exclude un fișier pe baza codului hash specificat SHA-1, indiferent de tipul fișierului, de locația sau de extensia sa.



Excluderi după numele detectării

Pentru a exclude o anumită detectare pe baza numelui acesteia, introduceți un nume de detectare valid:
Win32/Adware.Optmedia
Puteți folosi și următorul format pentru a exclude o detectare din fereastra de alertă ESET NOD32 Antivirus:
@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
@NAME=Win32/Bagle.D@TYPE=worm

Elemente de control

- **Adăugare** – exclude obiecte de la detectare.
- **Editare** – vă permite să editați intrările selectate.
- **Ștergere** – Elimină înregistrările selectate (folosiți CTRL + clic pentru a selecta înregistrări multiple).

Expertul pentru crearea unei excluderi de la detectare

Puteți crea o excludere de la detectare și în meniul contextual Fișiere log (opțiunea nu este disponibilă pentru detectările de malware):

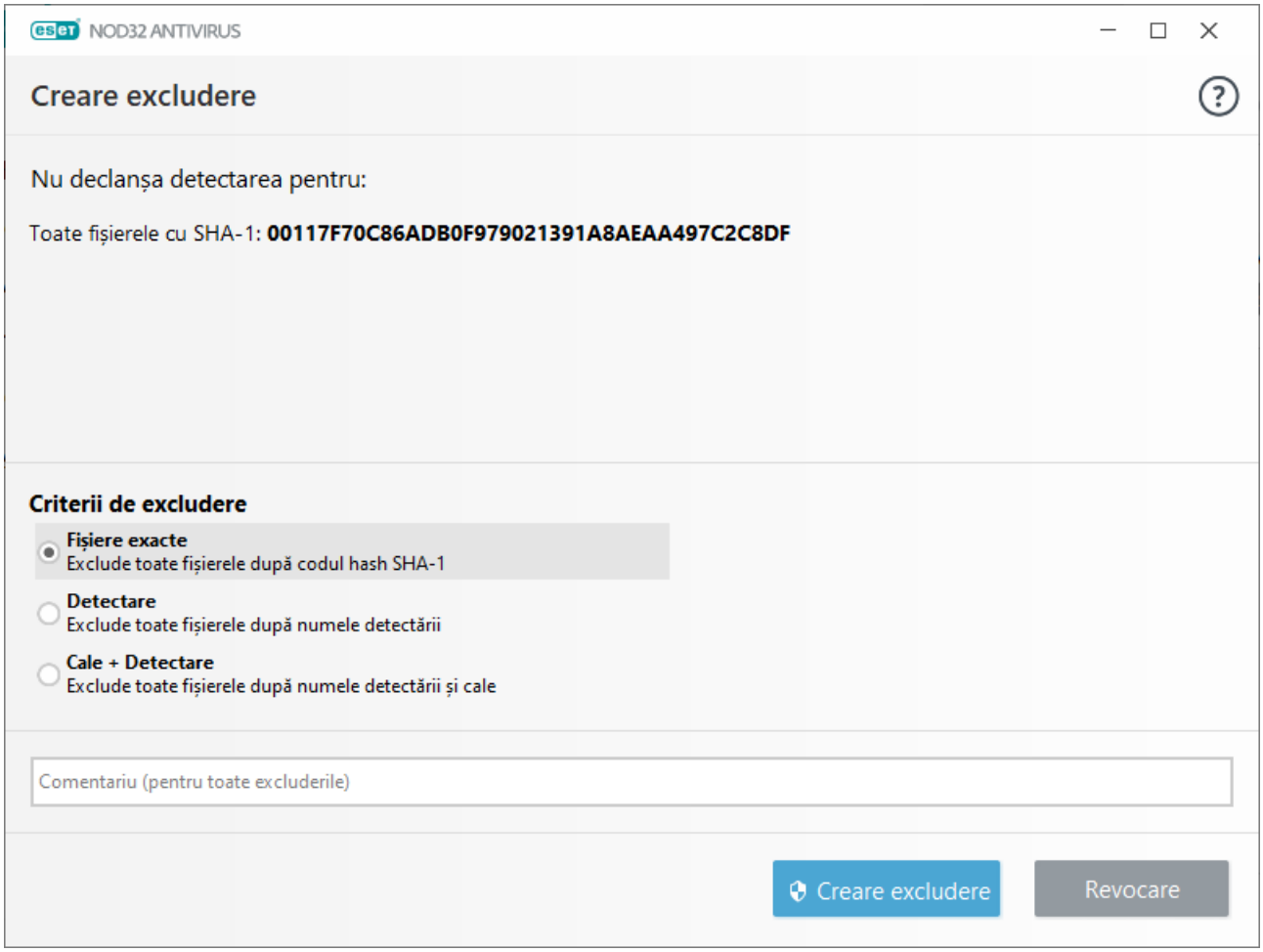
1. În fereastra principală a programului, faceți clic pe **Instrumente** > **Fișiere log**.
2. Faceți clic dreapta pe o detectare în **jurnalul Detectări**.
3. Faceți clic pe **Creare excludere**.

Pentru a exclude una sau mai multe detectări pe baza **criteriilor de excludere**, faceți clic pe **Schimbare criterii**:

- **Fișiere exacte** – Exclude toate fișierele după codul hashSHA-1.
- **Detectare** – Exclude toate fișierele după numele detectării.
- **Cale + Detectare** – Exclude toate fișierele după numele detectării și cale, inclusiv numele fișierului (de exemplu, *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

Opțiunea recomandată este preselectată, în funcție de tipul de detectare.

Opțional, puteți adăuga un **Comentariu** înainte de a face clic pe **Creare excludere**.



Excluderi HIPS

Excluderile vă permit să excludeți procese de la analiza prin HIPS Inspecția complexă a comportamentului.

Pentru a edita excluderile HIPS, navigați la **Setare avansată** (F5) > **Motor de detecție** > **HIPS** > **De bază** > **Excluderi** > **Editare**.

> Nu confundați cu Extensiile de fișiere excluse, Excluderile de la detectare, Excluderile de performanță sau Excluderile de procese.

Pentru a exclude un obiect, faceți clic pe **Adăugare** și introduceți calea spre un obiect sau selectați-l din structura arbore. Puteți și să alegeți Editare sau Șterge pentru înregistrările selectate.

Parametri ThreatSense

ThreatSense este o tehnologie care cuprinde numeroase metode complexe de detectare a amenințărilor. Această tehnologie este proactivă, adică oferă protecție inclusiv în faza incipientă de răspândire a unei amenințări noi. Ea folosește o combinație de analiză de cod, emulare de cod, semnături generice și semnături de virale care funcționează împreună pentru a îmbunătăți semnificativ securitatea sistemului. Motorul de scanare poate controla simultan mai multe fluxuri de date, maximizând rata de eficiență și de detecție. De asemenea, tehnologia ThreatSense elimină cu succes rootkiturile.

Opțiunile de setare a motorului ThreatSense vă permit să specificați mai mulți parametri de scanare:

- tipurile și extensiile de fișiere ce urmează a fi scanate,
- combinația dintre diverse metode de detecție,
- nivelurile de curățare etc.

Pentru a intra în fereastra de setare, faceți clic pe **Parametri ThreatSense** în fereastra Setări avansate din oricare modul care folosește tehnologia ThreatSense (vedeți mai jos). Diferite scenarii de securitate pot necesita configurații diferite. Ținând cont de acest lucru, ThreatSense se poate configura individual pentru următoarele module de protecție:

- Protecție în timp real a sistemului de fișiere
- Scanare în stare de inactivitate
- Scanare la pornire
- Protecție documente
- Protecție client email
- Protecție acces Web
- Scanare computer

Parametrii ThreatSense sunt optimizați pentru fiecare modul, iar modificarea acestora poate influența semnificativ funcționarea sistemului. De exemplu, modificarea parametrilor pentru scanarea permanentă a pachetelor de rutină sau activarea euristicii avansate în modulul Protecție în timp real a sistemului de fișiere poate conduce la o încetinire a sistemului (în mod normal, numai fișierele nou create se scanează folosind aceste metode). Recomandăm să lăsați parametrii ThreatSense impliciți nemodificați pentru toate modulele, cu excepția Scanare computer.

Obiecte de scanat

Această secțiune vă permite să definiți componentele computerului și fișierele care vor fi scanate pentru infiltrări.

Memorie operațională – se scanează amenințările care atacă memoria operațională a sistemului.

Sectoare de boot/UEFI – Scanează sectoarele de boot pentru prezența unor malware în Master Boot Record. Citiți mai multe despre UEFI în glosar.

Fișiere de email – programul acceptă următoarele extensii: DBX (Outlook Express) și EML.

Arhive – Programul acceptă următoarele extensii: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE și multe altele.

Arhive SFX – arhivele cu extragere automată (SFX) sunt arhive care se pot extrage automat.

Arhivatoare runtime – după executare, arhivatoarele runtime (spre deosebire de tipurile de arhive standard) se decomprimă în memorie. Pe lângă arhivatoarele statice standard (UPX, yoda, ASPack, FSG etc.), scanner-ul poate recunoaște câteva tipuri suplimentare de arhivatoare prin utilizarea emulării codului.

Opțiuni de scanare

Selectați metodele utilizate la scanarea sistemului pentru infiltrări. Sunt disponibile următoarele opțiuni:

Euristică – euristica este un algoritm care analizează activitatea (dăunătoare) a programelor. Avantajul principal al acestei tehnologii îl constituie capacitatea de a identifica software dăunător care nu exista sau care nu era cunoscut de versiunile anterioare ale motorului de detectare. Dezavantajul constă în probabilitatea (foarte mică) a unor alarme false.

Euristică avansată/Semnături DNA – euristica avansată constă într-un algoritm euristic unic dezvoltat de ESET, optimizat pentru detectarea viermilor de computer și a troienilor ce sunt scriși în limbaje de programare de nivel ridicat. Utilizarea euristicii avansate sporește semnificativ capacitatea de detectare a amenințărilor a produselor ESET. Semnăturile pot detecta și identifica viruși cu fiabilitate. Datorită utilizării sistemului automat de actualizare, sunt disponibile semnături noi în doar câteva ore. Dezavantajul semnăturilor este că detectează numai virușii pe care îi cunosc (sau versiuni ușor modificate ale acestor viruși).

Curățare

Setările de curățare determină comportamentul ESET NOD32 Antivirus în timpul curățării fișierelor infectate. Există 4 niveluri de curățare:

Parametrii ThreatSense au următoarele niveluri de remediere (adică curățare).

Remedierea în ESET NOD32 Antivirus

Nivel de curățare	Descriere
Remediați întotdeauna detectarea	Se încearcă remedierea detectării curățând obiectele fără intervenția utilizatorului final. În unele cazuri rare (de exemplu, fișiere de sistem), dacă detectarea nu poate fi remediată, obiectul raportat este lăsat în locația sa originală.
Se remediază detectarea dacă este sigur, altminteri se păstrează	Se încearcă remedierea detectării curățând obiectele fără intervenția utilizatorului final. În unele cazuri (de exemplu, fișiere de sistem sau arhive care conțin atât fișiere curate, cât și infectate), dacă o detectare nu poate fi remediată, obiectul raportat este lăsat în locația sa originală.
Se remediază detectarea dacă este sigur, altminteri se întreabă	Se încearcă remedierea detectării curățând obiectele. În unele cazuri, dacă nu se poate efectua nicio acțiune, utilizatorul final primește o alertă interactivă și trebuie să selecteze o acțiune de remediere (de exemplu, Ștergere sau Ignorare). Această setare este recomandată în majoritatea cazurilor.
Întrebați întotdeauna utilizatorul final	Se afișează o fereastră interactivă utilizatorului final atunci când se curăță obiecte, în care acesta trebuie să selecteze o acțiune de remediere (de exemplu, Ștergere sau Ignorare). Acest nivel este destinat utilizatorilor mai avansați, care știu ce pași să urmeze în eventualitatea unei detectări.

Excluderi

O extensie este partea unui nume de fișier separată printr-un punct. Extensia definește tipul și conținutul fișierului. Această secțiune din setarea parametrilor ThreatSense vă permite să definiți tipurile de fișiere de scanat.

Altele

La configurarea parametrilor motorului ThreatSense pentru Scanare computer la cerere, mai sunt disponibile următoarele opțiuni în secțiunea **Altele**:

Scanare fluxuri de date alternative (ADS) – fluxurile de date alternative utilizate de sistemul de fișiere NTFS sunt asocieri de fișiere și directoare invizibile pentru tehnicile clasice de scanare. Numeroase infiltrări încearcă să evite detectarea deghizându-se ca fluxuri de date alternative.

Execută scanări în fundal cu prioritate redusă – fiecare secvență de scanare consumă o anumită cantitate de resurse de sistem. Dacă lucrați cu programe ce consumă multe resurse de sistem, puteți activa scanarea în fundal cu prioritate redusă, economisind astfel resurse pentru aplicațiile dvs.

Înregistrează în log toate obiectele – Secțiunea Jurnal scanare va afișa toate fișierele scanate ca arhive SFX, chiar și pe cele care nu sunt infectate (este posibil ca această opțiune să genereze o cantitate mare de date pentru jurnalul de scanare și să mărească dimensiunea fișierului jurnalului de scanare).

Activare optimizare Smart – Cu optimizarea Smart activată, se utilizează setările optime pentru a asigura cel mai eficient nivel de scanare menținând, simultan, cele mai mari viteze de scanare. Diversele module de protecție efectuează o scanare inteligentă, utilizând diferite metode de scanare și aplicându-le tipurilor specifice de fișiere. Dacă opțiunea Optimizare Smart este dezactivată, la efectuarea unei scanări se aplică numai setările definite de utilizator din nucleul ThreatSense al modulelor particulare.

Păstrare ultimul marcaj temporal – selectați această opțiune pentru a păstra timpul de acces inițial pentru fișierele scanate în loc de actualizarea acestuia (de exemplu, pentru utilizare cu sistemele de copiere de rezervă a datelor).

Limite

Secțiunea Limite vă permite să specificați dimensiunea maximă a obiectelor și nivelurile de arhive imbricate de scanat:

Setări obiect

Dimensiune maximă obiect – definește dimensiunea maximă a obiectelor de scanat. Modul antivirus corespunzător va scana numai obiecte mai mici decât dimensiunea specificată. Această opțiune se va modifica numai de către utilizatorii avansați care pot avea un motiv anumit pentru a exclude obiecte mai mari de la scanare. Valoare implicită: nelimitată.

Timp maxim de scanare pentru obiect (sec.) – Definește valoarea maximă de timp pentru scanarea fișierelor dintr-un obiect container (cum ar fi o arhivă RAR/ZIP sau un e-mail cu mai multe atașări). Această setare nu se aplică pentru fișierele independente. Dacă s-a introdus o valoare definită de utilizator și timpul respectiv s-a scurs, o scanare se va opri cât mai curând posibil, indiferent dacă s-a terminat sau nu scanarea tuturor fișierelor dintr-un obiect container.
În cazul unei arhive cu fișiere mari, scanarea se va opri cel mai devreme după extragere unui fișier din arhivă (de exemplu, atunci când variabila definită de utilizator este 3 secunde, dar extragerea unui fișier durează 5 secunde). Restul fișierelor din arhivă nu vor fi scanate după expirarea acestui timp.
Pentru a limita timpul de scanare, inclusiv arhivele mai mari, utilizați opțiunile **Dimensiune maximă obiect** și **Dimensiune maximă fișier în arhivă** (lucru nerecomandat din cauza riscurilor posibile de securitate).
Valoare implicită: nelimitată.

Setare scanare arhivă

Nivel imbricare arhivă – specifică profunzimea maximă de scanare a arhivei. Valoare implicită: 10.

Dimensiune maximă fișier în arhivă – Această opțiune vă permite să specificați dimensiunea maximă de fișier pentru fișierele cuprinse în arhivele (când sunt extrase) ce trebuie scanate. Valoarea maximă este **3 GB**.

> Nu recomandăm modificarea valorilor implicite; în condiții normale, nu există motive pentru modificarea acestora.

Listă de fișiere excluse de la scanare

Extensiile de fișiere excluse fac parte din parametri ThreatSense. Pentru a configura extensiile de fișiere excluse, faceți clic pe **parametri ThreatSense** în fereastra Setare avansată pentru orice modul care utilizează tehnologia ThreatSense.

O extensie este partea unui nume de fișier separată printr-un punct. Extensia definește tipul și conținutul fișierului. Această secțiune din setarea parametrilor ThreatSense vă permite să definiți tipurile de fișiere de scanat.

> Nu confundați între ele Excluderi de procese, Excluderi HIPS sau Excluderi fișier/folder.

În mod implicit, se scanează toate fișierele. În lista de fișiere excluse de la scanare se poate adăuga orice extensie.

Excluderea fișierelor este uneori necesară dacă scanarea anumitor tipuri de fișiere împiedică funcționarea corectă a programului care utilizează anumite extensii. De exemplu, poate fi recomandabil să excludeți extensiile `.edb`, `.eml` și `.tmp` atunci când folosiți servere Microsoft Exchange.

> Pentru a adăuga o nouă extensie la listă, faceți clic pe **Adăugare**. Tastați extensia în câmpul necompletat (de exemplu, tmp) și faceți clic pe **OK**. Atunci când selectați **Introducere valori multiple**, puteți adăuga mai multe extensii de fișier delimitate prin linie, virgulă sau punct și virgulă (de exemplu, alegeți **Punct și virgulă** din meniul vertical ca separator și tastați `edb;eml;tmp`).
> Puteți folosi simbolul special ? (semnul întrebării). Semnul întrebării reprezintă orice simbol (de exemplu `?db`).

> Pentru a vedea extensia exactă (dacă există) a unui fișier dintr-un sistem de operare Windows, trebuie să debifați opțiunea **Se ascund extensiile pentru tipurile de fișiere cunoscute** din **Panou de control** > **Opțiuni folder** > (fila) **Vizualizare** și aplicați această modificare.

Parametri ThreatSense suplimentari

Pentru a edita aceste setări, navigați la **Setare avansată** (F5) > **Motor de detecție** > **Protecție în timp real pentru sistemul de fișiere** > **Parametri ThreatSense suplimentari**.

Parametri ThreatSense suplimentari pentru fișiere nou create și

modificate

Probabilitatea de infectare în fișiere nou create sau modificate este comparativ mai mare decât în fișiere existente. Din acest motiv, programul verifică aceste fișiere cu parametri de scanare suplimentari. ESET NOD32 Antivirus utilizează euristică avansată, care poate detecta noi amenințări înainte de lansarea actualizării motorului de detecție, în combinație cu metode de scanare bazate pe semnături.

Pe lângă fișierele nou create, se efectuează scanarea și pentru **Arhive SFX** și **Pachete runtime** (fișiere executabile comprimate intern). În mod implicit, arhivele sunt scanate până la nivelul de imbricare 10 și sunt verificate indiferent de dimensiunea lor efectivă. Pentru a modifica setările pentru scanarea arhivelor, debifați opțiunea **Setări implicite pentru scanare arhivă**.

Parametri ThreatSense suplimentari pentru fișierele executate

Euristică avansată la executarea fișierelor – În mod implicit, se utilizează euristica avansată la executarea fișierelor. Vă recomandăm cu insistență să păstrați activate opțiunile Optimizare Smart și ESET LiveGrid® pentru a limita impactul asupra performanțelor sistemului.

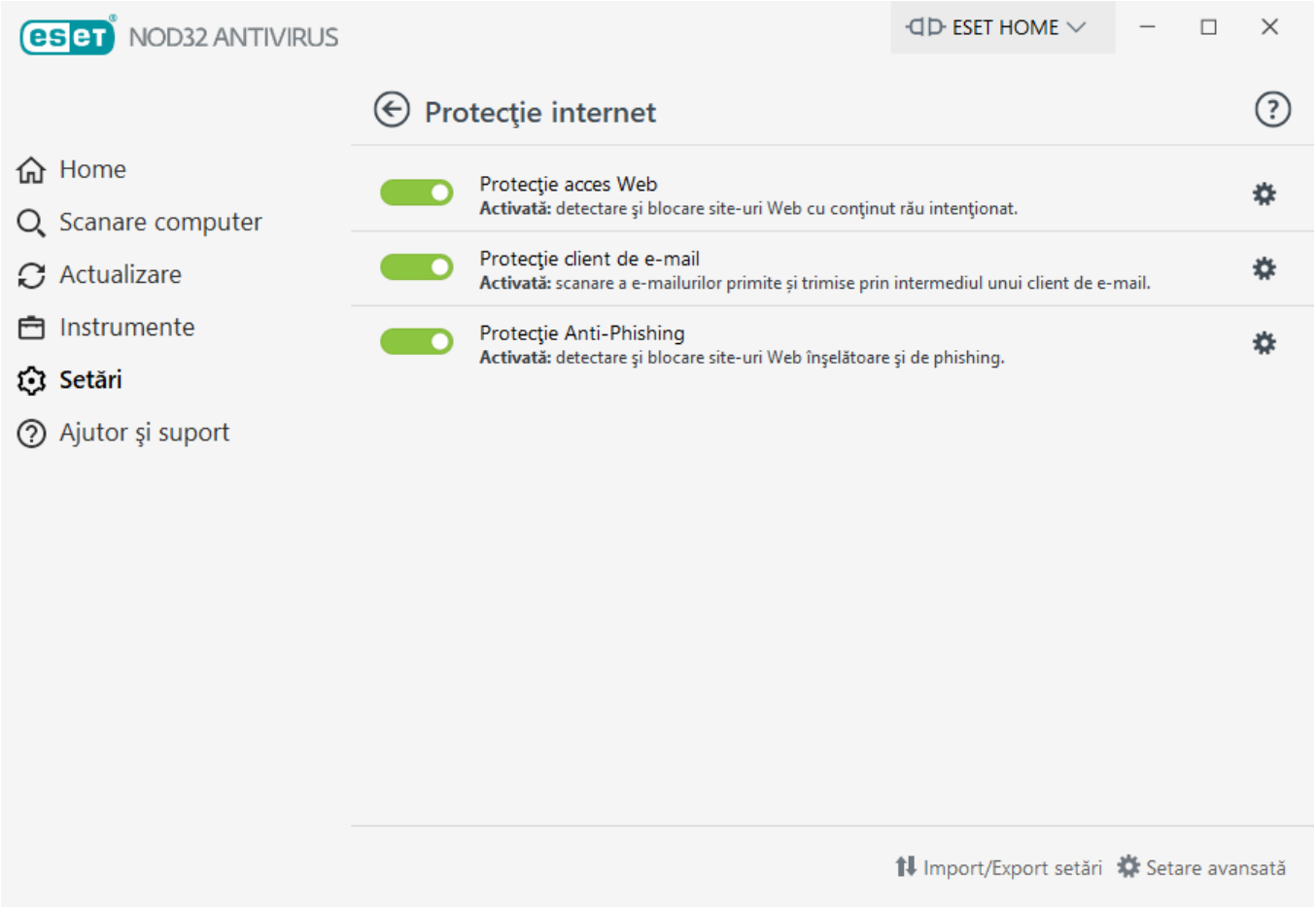
Euristică avansată la executarea fișierelor de pe unități media portabile – Euristica avansată emulează codul într-un mediu virtual și îi evaluează comportamentul înainte ca acesta să se poată executa de pe unitățile media portabile.

Protecție internet

Pentru a configura protecția pentru web și e-mail, faceți clic pe **Protecție internet** în fereastra **Setare**. De aici puteți accesa setări mai detaliate ale programului.

Pentru a pune în pauză sau a dezactiva module de protecție individuale, faceți clic pe pictograma barei cu glisor .

⚠ Dezactivarea modulelor de protecție poate scădea nivelul de protecție pentru computerul dvs.



Faceți clic pe pictograma rotiță pentru a deschide setările pentru web/e-mail/anti-phishing în Setări avansate.

Conectivitatea Internet este o caracteristică standard a computerelor personale. Din păcate, Internetul a devenit mediul principal pentru distribuirea codului dăunător. Din acest motiv, este esențial să țineți cont de setările Protecție acces Web.

Protecție client de email permite controlul comunicărilor prin email primite prin protocoalele POP3(S) și IMAP(S). Utilizând programul insert pentru clientul de email, Microsoft Outlook, ESET NOD32 Antivirus oferă controlul asupra tuturor comunicărilor din clientul de email.

Protecție Anti-Phishing vă permite să blocați paginile Web cunoscute că distribuie conținut de phishing. Vă recomandăm ferm să lăsați componenta Anti-Phishing activată.

Filtrare protocol

Protecția antivirus pentru protocoalele de aplicații este asigurată de motorul de scanare ThreatSense, care integrează fără probleme toate tehnicile avansate de scanare de programe malware. Filtrarea protocolului funcționează automat, indiferent de browserul internet sau clientul de e-mail folosit. Pentru a edita setările criptate (SSL/TLS), accesați **Setare avansată** (F5) > **Web și e-mail** > **SSL/TLS**.

Activare filtrare conținut protocol aplicație – se poate utiliza pentru a dezactiva filtrarea protocolului. Rețineți că multe componente ale produsului ESET NOD32 Antivirus (Protecție acces Web, Protecție protocoale de email, Anti-Phishing, Control parental) depind de această opțiune și nu vor funcționa fără aceasta.

Aplicații excluse – vă permite să excludeți anumite aplicații de la filtrarea protocolului. Opțiune utilă dacă filtrarea protocolului provoacă probleme de incompatibilitate.

Adrese IP excluse – vă permite să excludeți anumite adrese la distanță de la filtrarea protocolului. Opțiune utilă dacă filtrarea protocolului provoacă probleme de incompatibilitate.

Adaugă (de exemplu, *2001:718:1c01:16:214:22ff:fec9:ca5*).

Subrețea – subrețea (un grup de computere) definită de o adresă IP și o mască (de exemplu, *2002:c0a8:6301:1::1/64*).

Exemplu de adrese IP excluse

Adrese IPv4 și mască:

- *192.168.0.10* – adaugă adresa IP a unui anumit computer pentru care trebuie aplicată regula
- *192.168.0.1* la *192.168.0.99* – introduceți prima și ultima adresă pentru a specifica intervalul de adrese IP (pentru mai multe computere) pentru care trebuie aplicată regula.
- Subrețea (un grup de computere) definită de o adresă IP și o mască. De exemplu, *255.255.255.0* este masca de rețea pentru prefixul *192.168.1.0/24*, adică intervalul de adrese de la *192.168.1.1* la 192.168.1.254.

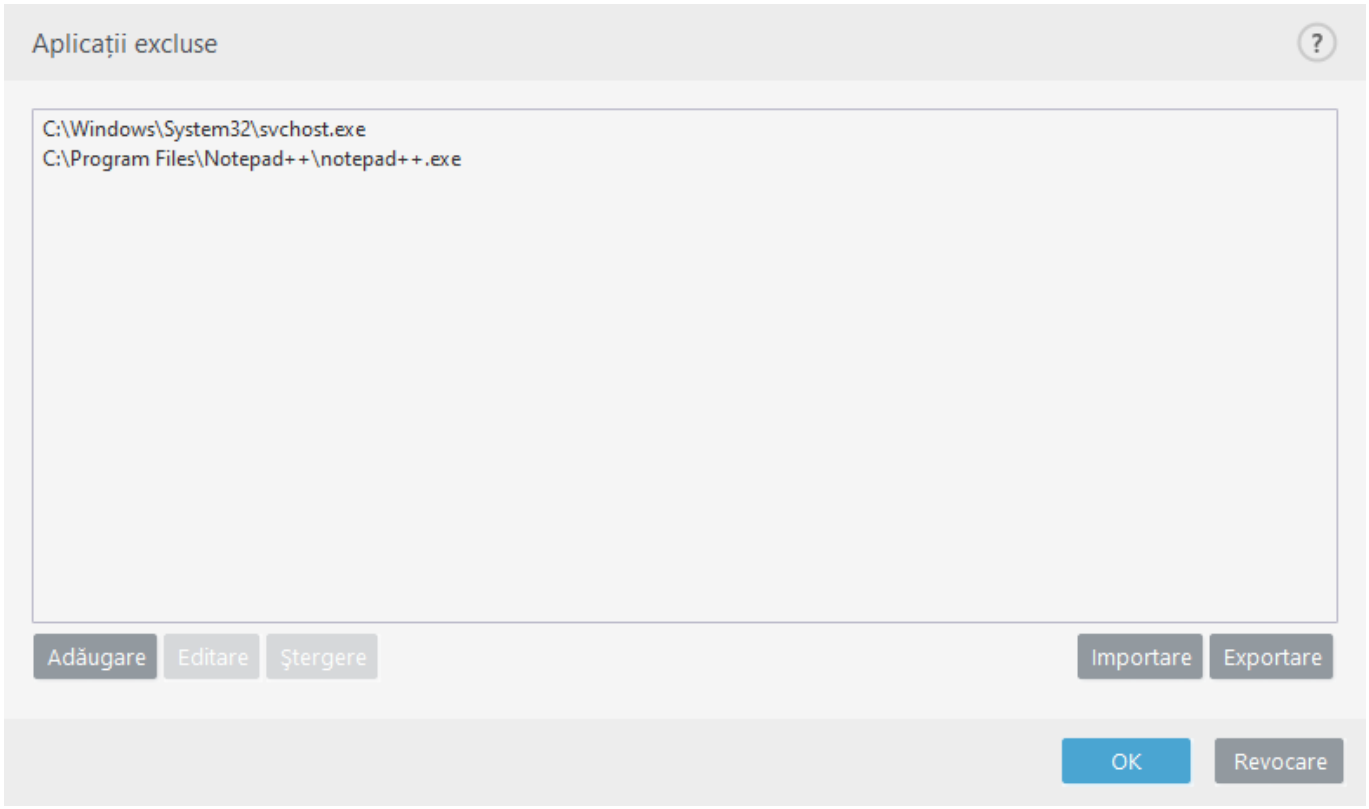
Adrese IPv6 și mască:

- *2001:718:1c01:16:214:22ff:fec9:ca5* – adresa Ipv6 a unui anumit computer pentru care trebuie aplicată regula
- *2002:c0a8:6301:1::1/64* – adresă IPv6 cu lungime prefix de 64 de biți, adică *2002:c0a8:6301:0001:0000:0000:0000:0000 până la 2002:c0a8:6301:0001:ffff:ffff:ffff:ffff*

Aplicații excluse

Pentru a exclude comunicarea aplicațiilor de rețea de la filtrarea conținutului, selectați aplicațiile în listă. Comunicarea prin HTTP/POP3/IMAP a aplicațiilor selectate nu se va verifica pentru amenințări. Vă recomandăm să utilizați această opțiune numai pentru aplicațiile care nu funcționează corect dacă se efectuează verificarea comunicării acestora.

Aici va fi disponibilă, în mod automat, executarea aplicațiilor și serviciilor. Faceți clic pe **Adăugare** pentru a adăuga o aplicație dacă nu este afișată în lista de filtrare a protocolului.



Adrese IP excluse

Înregistrările din listă se vor exclude de la filtrarea conținutului protocolului. Comunicarea prin HTTP/POP3/IMAP de la/la adresele selectate nu vor fi verificate pentru amenințări. Vă recomandăm să utilizați această opțiune numai pentru adresele care sunt cunoscute ca fiind de încredere.

Faceți clic pe **Adăugare** pentru a exclude o adresă IP/un domeniu de adrese/o subrețea a unui punct aflat la distanță care nu este afișat în lista de filtrare a protocolului.

Faceți clic pe **Ștergere** pentru a elimina înregistrările selectate în listă.



Adăugare adresă IPv4

Această opțiune vă permite să adăugați o adresă IP/un interval de adrese/o subrețea pentru un punct la distanță pentru care se aplică o regulă. Versiunea 4 a protocolului Internet este cea mai veche, dar ea este în continuare cea mai des folosită.

Adresă unică – adaugă adresa IP a unui anumit computer pentru care trebuie aplicată regula, (de exemplu *192.168.0.10*).

Interval de adrese – introduceți prima și ultima adresă pentru a specifica intervalul de adrese IP (pentru mai multe computere) pentru care trebuie aplicată regula, de exemplu de la *192.168.0.1* la *192.168.0.99*).

Subrețea – subrețea (un grup de computere) definită de o adresă IP și o mască.

De exemplu, *255.255.255.0* este masca de rețea pentru prefixul *192.168.1.0/24*, adică intervalul de adrese de la *192.168.1.1* la 192.168.1.254.

Adăugare adresă IPv6

Această opțiune vă permite să adăugați o adresă IPv6/o subrețea pentru un punct la distanță pentru care se aplică o regulă. Este cea mai nouă versiune a protocolului Internet și ea va înlocui versiunea mai veche 4.

Adresă unică – adaugă adresa IP a unui anumit computer pentru care trebuie aplicată regula (de exemplu *2001:718:1c01:16:214:22ff:fec9:ca5*).

Subrețea – subrețea (un grup de computere) definită de o adresă IP și o mască (de exemplu: *2002:c0a8:6301:1::1/64*).

SSL/TLS

ESET NOD32 Antivirus poate verifica amenințările din comunicările care utilizează protocolul SSL. Puteți utiliza diferite metode de filtrare pentru a examina comunicările SSL protejate prin certificate de încredere, certificate necunoscute sau certificate excluse de la verificarea comunicărilor SSL protejate.

Activare filtrare protocol SSL/TLS – dacă filtrarea protocolului este dezactivată, programul nu va scana comunicările prin SSL.

modul de filtrare a protocolului SSL/TLS este disponibil în opțiunile următoare:

Mod de filtrare	Descriere
Mod Automat	Modul implicit va scana numai aplicațiile corespunzătoare, cum ar fi browserele Web și clienții de email. Îl puteți anula selectând aplicațiile pentru care vor fi scanate comunicările.
Mod Interactiv	Dacă intrați pe un site nou, protejat prin SSL (cu un certificat necunoscut), se afișează o casetă de dialog de selectare a unei acțiuni. Acest mod vă permite să creați o listă cu certificatele SSL/aplicațiile care vor fi excluse la scanare.

Mod de filtrare	Descriere
Mod Politică	Selectați această opțiune pentru a scana toate comunicările SSL protejate, cu excepția comunicărilor protejate prin certificate excluse la verificare. Dacă se stabilește o comunicare nouă care utilizează un certificat semnat necunoscut, veți fi notificat, iar comunicarea va fi filtrată automat. Dacă accesați un server cu un certificat care nu este de încredere, dar este marcat ca fiind de încredere (este în lista certificatelor de încredere), se permite comunicarea cu serverul, iar conținutul canalului de comunicare se filtrează.

Lista de aplicații filtrate SSL/TLS poate fi folosită pentru a particulariza comportamentul produsului ESET NOD32 Antivirus pentru anumite aplicații.

Lista de certificate cunoscute – vă permite să personalizați comportamentul produsului ESET NOD32 Antivirus pentru anumite certificate SSL.

Excludeți comunicarea cu domeniile de încredere – dacă este activată, comunicarea cu domeniile de încredere nu va fi inclusă în verificări. Gradul de încredere al domeniului este stabilit de lista albă încorporată.

Blochează comunicarea criptată care utilizează protocolul vechi SSL v2 – Comunicarea care utilizează versiunea anterioară a protocolului SSL va fi blocată automat.

Certificat root

Adăugare certificat root la browserele cunoscute – pentru ca în browsere/clienții de e-mail să funcționeze corect comunicările SSL, este esențial ca în lista de certificate root cunoscute (editori) să fie adăugat certificatul root pentru ESET. Dacă activați opțiunea, ESET NOD32 Antivirus va adăuga automat certificatul ESET SSL Filter CA în browserele cunoscute (de exemplu, Opera). Pentru browserele care utilizează depozite de certificări de sistem, certificatul se adaugă automat. De exemplu, Firefox este configurat automat să acorde încredere pentru autoritățile Root din depozitul de certificări de sistem.

Pentru a aplica certificatul browserelor neacceptate, faceți clic pe **Vizualizare certificat** > **Detalii** > **Copiere la fișier** și importați-l manual în browser.

Validitate certificat

Dacă încrederea în certificat nu se poate verifica – În unele cazuri, certificatul unui site web nu se poate verifica utilizând depozitul Trusted Root Certification Authorities (TRCA). Prin urmare, certificatul a fost semnat de cineva (de exemplu, un administrator al unui server web sau o companie mică) și a considera acest certificat ca fiind de încredere nu constituie întotdeauna un risc. Majoritatea companiilor mari (de exemplu, bănci) utilizează un certificat semnat de TRCA. Dacă opțiunea **Întreabă despre valabilitatea certificatului** este selectată (în mod implicit), utilizatorului i se solicită să aleagă o acțiune de efectuat la stabilirea unei comunicări criptate. Puteți selecta **Blocare comunicații care utilizează certificatul** pentru a închide întotdeauna conexiunile criptate către site-uri cu certificate neverificate.

Dacă certificatul este deteriorat - Aceasta înseamnă că certificatul a fost semnat incorect sau este deteriorat. În acest caz, ESET vă recomandă să lăsați selectată opțiunea **Blocare comunicații care utilizează certificatul** selectat. Dacă este selectată opțiunea **Întreabă despre valabilitatea certificatului**, utilizatorului i se solicită să selecteze o acțiune de efectuat atunci când este stabilită comunicarea criptată.

Exemple ilustrate

Următoarele articole din Baza de cunoștințe ESET este posibil să fie disponibile numai în limba engleză:

- Notificări privind certificatele în produsele ESET Windows Home
- Mesajul „Trafic de rețea criptat: Certificatul fără încredere” este afișat atunci când se vizitează pagini web

Certificate

Pentru ca în browser/clienții de email să funcționeze corect comunicările SSL, este esențial ca în lista de certificate root cunoscute (editori) să fie adăugat certificatul root pentru ESET. Opțiunea **Adaugă certificatul root la browserele cunoscute** trebuie să fie activată. Selectați această opțiune pentru a adăuga automat certificatul root ESET în browserele cunoscute (de exemplu, Opera și Firefox). Pentru browserele care utilizează depozitul certificărilor de sistem (de exemplu Internet Explorer), certificatul se adaugă automat. Pentru a aplica certificatul browserelor neacceptate, faceți clic pe **Vizualizare certificat** > **Detalii** > **Copiere la fișier** și importați-l manual în browser.

În unele cazuri, certificatul nu se poate verifica utilizând depozitul Trusted Root Certification Authorities (de exemplu VeriSign). Aceasta înseamnă că certificatul este autosemnat de către cineva (de exemplu un administrator al unui server Web sau o companie mică) și considerarea acestui certificat ca fiind de încredere nu constituie întotdeauna un risc. Majoritatea companiilor mari (de exemplu, bănci) utilizează un certificat semnat de TRCA.

Dacă opțiunea **Întreabă despre valabilitatea certificatului** este selectată (în mod implicit), utilizatorului i se va solicita să selecteze o acțiune de efectuat la stabilirea unei comunicări criptate. Se va afișa un dialog de selectare a acțiunii, unde puteți decide să marcați certificatul ca fiind de încredere sau exclus. Dacă certificatul nu este prezent în lista TRCA, fereastra este de culoare roșie. Dacă certificatul este prezent în lista TRCA, fereastra este de culoare verde.

Puteți selecta **Blochează comunicarea care utilizează certificatul** pentru a se termina întotdeauna o conexiune criptată la site-ul care utilizează certificatul neverificat.

Dacă certificatul este nevalid sau alterat, înseamnă că acesta a expirat sau a fost autosemnat incorect. În acest caz, vă recomandăm să blocați comunicarea care utilizează certificatul.

Trafic de rețea criptat

Dacă sistemul dvs. este configurat să utilizeze scanarea protocolului SSL, se va afișa o fereastră de dialog de solicitare a alegerii unei acțiuni în următoarele două situații:

În primul rând, dacă un site web utilizează un certificat neverificabil sau nevalid, iar ESET NOD32 Antivirus este configurat să întrebe utilizatorul în astfel de cazuri (în mod implicit Da pentru certificate neverificabile și Nu pentru certificate nevalide), o casetă de dialog vă va întreba dacă doriți **permiterea** sau **blocarea** conexiunii. În cazul în care certificatul nu se află în depozitul Trusted Root Certification Authorities store (TRCA), acesta este considerat ca nefiind de încredere.

În al doilea rând, dacă opțiunea **Mod filtrare protocol SSL** este setată la **Mod interactiv**, o casetă de dialog pentru fiecare site Web vă va întreba dacă doriți **scanarea** sau **ignorarea** traficului. Unele aplicații verifică dacă traficul lor SSL este modificat sau inspectat de cineva; într-un astfel de caz, ESET NOD32 Antivirus trebuie să **ignore** traficul respectiv pentru a menține aplicația funcțională.

Exemple ilustrate

Următoarele articole din Baza de cunoștințe ESET este posibil să fie disponibile numai în limba engleză:

- Notificări privind certificatele în produsele ESET Windows Home
- Mesajul „Trafic de rețea criptat: Certificatul fără încredere” este afișat atunci când se vizitează pagini web

În ambele situații, utilizatorul poate alege memorarea acțiunii selectate. Acțiunile salvate se stochează în Lista de certificate cunoscute.

Lista de certificate cunoscute

Lista de certificate cunoscute poate fi utilizată pentru particularizarea comportamentului produsului ESET NOD32 Antivirus pentru anumite certificate SSL și pentru memorarea acțiunilor alese dacă este selectat **modul Interactiv** în **modul de filtrare a protocolului SSL/TLS**. Lista poate fi vizualizată și editată în **Setări avansate** (F5) > **Web și email** > **SSL/TLS** > **Lista de certificate cunoscute**.

Fereastra **Lista de certificate cunoscute** are următoarea structură:

Coloane

Nume – numele certificatului.

Emitent certificat – numele creatorului certificatului.

Subiect certificat – acest câmp identifică entitatea asociată cu cheia publică stocată în câmpul Subiect cheie publică.

Acces – selectați **Permitere** sau **Blocare** ca **Acțiune acces** pentru permiterea/blocarea comunicațiilor securizate de acest certificat, indiferent de gradul de încredere. Selectați **Auto** pentru a permite certificate de încredere și a fi întrebat pentru cele care nu sunt de încredere. Selectați **Întreabă** pentru a se solicita întotdeauna utilizatorului specificarea acțiunii de efectuat.

Scanare– selectați **Scanare** sau **Ignorare** ca **Acțiune scanare** pentru a se scana sau a ignora comunicațiile securizate de acest certificat. Selectați **Auto** pentru a se efectua scanare în modul Automat și a se solicita acțiunea în modul Interactiv. Selectați **Întreabă** pentru a se solicita întotdeauna utilizatorului specificarea acțiunii de efectuat.

Elemente de control

Adăugare – adăugați un certificat nou și modificați setările acestuia privind opțiunile de accesare și scanare.

Editare – selectați certificatul pe care doriți să îl configurați și faceți clic pe **Editare**.

Ștergere – selectați certificatul pe care doriți să îl ștergeți și faceți clic pe **Eliminare**.

OK/Revocare – faceți clic pe **OK** dacă doriți să salvați modificările sau pe **Revocare** dacă doriți să ieșiți fără salvare.

Listă de aplicații filtrate SSL/TLS

Opțiunea **Listă de aplicații filtrate SSL/TLS** poate fi utilizată pentru particularizarea comportamentului produsului ESET NOD32 Antivirus pentru anumite aplicații și pentru memorarea acțiunilor alese dacă **Mod filtrare protocol SSL/TLS** este setat la **Mod Interactiv**. Lista poate fi vizualizată și editată în **Setare avansată** (F5) > **Web și e-mail** > **SSL/TLS** > **Listă de aplicații filtrate SSL/TLS**.

Fereastra **Listă de aplicații filtrate SSL/TLS** are următoarea structură:

Coloane

Aplicație – Alegeți un fișier executabil din arborele directoarelor, faceți clic pe opțiunea **...** sau introduceți manual calea.

Acțiune de scanare – Selectați **Scanare** sau **Ignorare** pentru a scana sau ignora comunicarea. Selectați **Auto** pentru a se efectua scanare în modul Automat și a se solicita acțiunea în modul Interactiv. Selectați **Întreabă** pentru a se solicita întotdeauna utilizatorului specificarea acțiunii de efectuat.

Elemente de control

Adăugare – adăugați aplicația filtrată.

Editare – selectați aplicația pe care doriți s-o configurați și faceți clic pe **Editare**.

Eliminare – selectați aplicația pe care doriți s-o ștergeți și faceți clic pe **Eliminare**.

Import/Export – Importați aplicații dintr-un fișier sau salvați lista curentă de aplicații într-un fișier.

OK/Revocare – faceți clic pe **OK** dacă doriți să salvați modificările sau pe **Revocare** dacă doriți să ieșiți fără salvare.

Protecție client email

Consultați Integrarea ESET NOD32 Antivirus cu clientul de e-mail pentru a configura integrarea.

Setările de client email se găsesc în **Configurare avansată** (F5) > **Web și email** > **Protecție client de email** > **Clienți de email**.

Clienți de email

Activare protecție e-mail de către inserturile clientului – Atunci când această opțiune este dezactivată, protecția mesajelor de e-mail de către inserturile clientului este dezactivată.

Mesaje email de scanat

Selectați e-mailurile de scanat:

- **Mesaje e-mail primite**
- **Mesaje e-mail trimise**

- **Citire mesaje e-mail**
- **E-mail modificat**

> Vă recomandăm să păstrați activată opțiunea **Activare protecție e-mail de către inserturile clientului**. Chiar dacă integrarea nu este activată sau nu funcționează, comunicarea prin e-mail este protejată în continuare de funcția Filtrare protocol (pentru IMAP/IMAPS și POP3/POP3S).

Acțiune de efectuat pentru mesajele email infectate

Nicio acțiune – în cazul activării, programul va identifica atașamentele infectate, dar nu va lua nicio acțiune pentru email-uri.

Ștergere mesaj e-mail – programul va notifica utilizatorul despre infiltrări și va șterge mesajul.

Mutare mesaj e-mail în directorul Elemente șterse – mesajele de email infectate vor fi mutate automat în directorul Elemente șterse.

Mutare mesaj e-mail în directorul (acțiune implicită) – e-mailurile infectate vor fi mutate automat în directorul specificat.

Director – specificați directorul particularizat unde doriți să mutați mesajele email infectate atunci când sunt detectate.

Integrare client email

Integrarea ESET NOD32 Antivirus cu clienții dvs. de e-mail sporește nivelul protecției active împotriva codului dăunător în mesajele de email. În cazul în care clientul dvs. de email este acceptat, integrarea poate fi activată în ESET NOD32 Antivirus. Atunci când produsul este integrat în clientul de email, bara de instrumente ESET NOD32 Antivirus este introdusă direct în clientul de e-mail, asigurând o protecție mai eficientă a mesajelor de email. Setările de integrare se găsesc în **Configurare avansată** (F5) > **Web și email** > **Protecție client de email** > **Integrare client e-mail**.

Clienții de email acceptați în prezent sunt Microsoft Outlook, Outlook Express, Windows Mail și Windows Live Mail. Pentru aceste programe, componenta Protecția e-mail funcționează ca un plugin. Avantajul principal al insertului constă în faptul că este independent de protocolul utilizat. Când clientul de email primește un mesaj criptat, acesta este decriptat și trimis către scannerul de viruși. Pentru lista completă cu clienții de email acceptați și versiunile acestora, consultați următorul articol din Baza de cunoștințe ESET.

Dezactivați opțiunile **Optimizare a administrării atașamentelor** și **Procesare avansată client de e-mail** dacă observați o încetinire a sistemului la recuperarea e-mailurilor.

Bara de instrumente Microsoft Outlook

Protecția Microsoft Outlook funcționează ca un modul insert. După instalarea produsului ESET NOD32 Antivirus, această bară de instrumente care conține opțiunile de protecție antivirus/ se adaugă la Microsoft Outlook:

ESET NOD32 Antivirus – Faceți dublu clic pe pictogramă pentru a deschide fereastra principală a ESET NOD32 Antivirus.

Rescanare mesaje – Vă permite să lansați manual verificarea mesajelor de email. Puteți specifica mesaje care vor fi verificate și puteți activa rescanarea pentru email primit. Pentru informații suplimentare, consultați Protecție client de email.

Setare scanner – Afișează opțiunile de setare pentru protecția clientului de email.

Bară de instrumente Outlook Express și Windows Mail

Protecția pentru Outlook Express și Windows Mail funcționează ca un modul insert. După instalarea produsului ESET NOD32 Antivirus, această bară de instrumente care conține opțiunile de protecție antivirus/ se adaugă la Outlook Express sau Windows Mail:

ESET NOD32 Antivirus – Faceți dublu clic pe pictogramă pentru a deschide fereastra principală a ESET NOD32 Antivirus.

Rescanare mesaje – Vă permite să lansați manual verificarea mesajelor de email. Puteți specifica mesaje care vor fi verificate și puteți activa rescanarea pentru email primit. Pentru informații suplimentare, consultați Protecție client de email.

Setare scanner – Afișează opțiunile de setare pentru protecția clientului de email.

Interfață utilizator

Personalizare aspect – Se poate modifica aspectul barei de instrumente pentru clientul de email. Deselectați opțiunea pentru a personaliza aspectul independent de parametrii programului de email.

Afișare text – Afișează descrieri pentru pictograme.

Text la dreapta – Descrierile opțiunii sunt mutate din partea de jos în partea dreaptă a pictogramelor.

Pictograme mari – Afișează pictograme mari pentru opțiunile de meniu.

Dialog de confirmare

Această notificare verifică dacă utilizatorul dorește într-adevăr să efectueze acțiunea selectată, aceasta ar trebui să elimine posibilele greșeli.

Pe de altă parte, dialogul oferă și posibilitatea de a dezactiva confirmările.

Rescanare mesaje

Bara de instrumente ESET NOD32 Antivirus integrată în clienții de email permite utilizatorilor să specifice câteva opțiuni pentru verificarea email-ului. Opțiunea **Rescanare mesaje** oferă două moduri de scanare:

Toate mesajele din directorul curent – Scanează mesaje din directorul curent afișat.

Numai mesaje selectate – Scanează numai mesajele marcate de utilizator.

Caseta de selectare **Scanează din nou mesajele deja scanate** oferă utilizatorului opțiunea de a executa o altă

scanare a mesajelor scanate înainte.

Protocoale de email

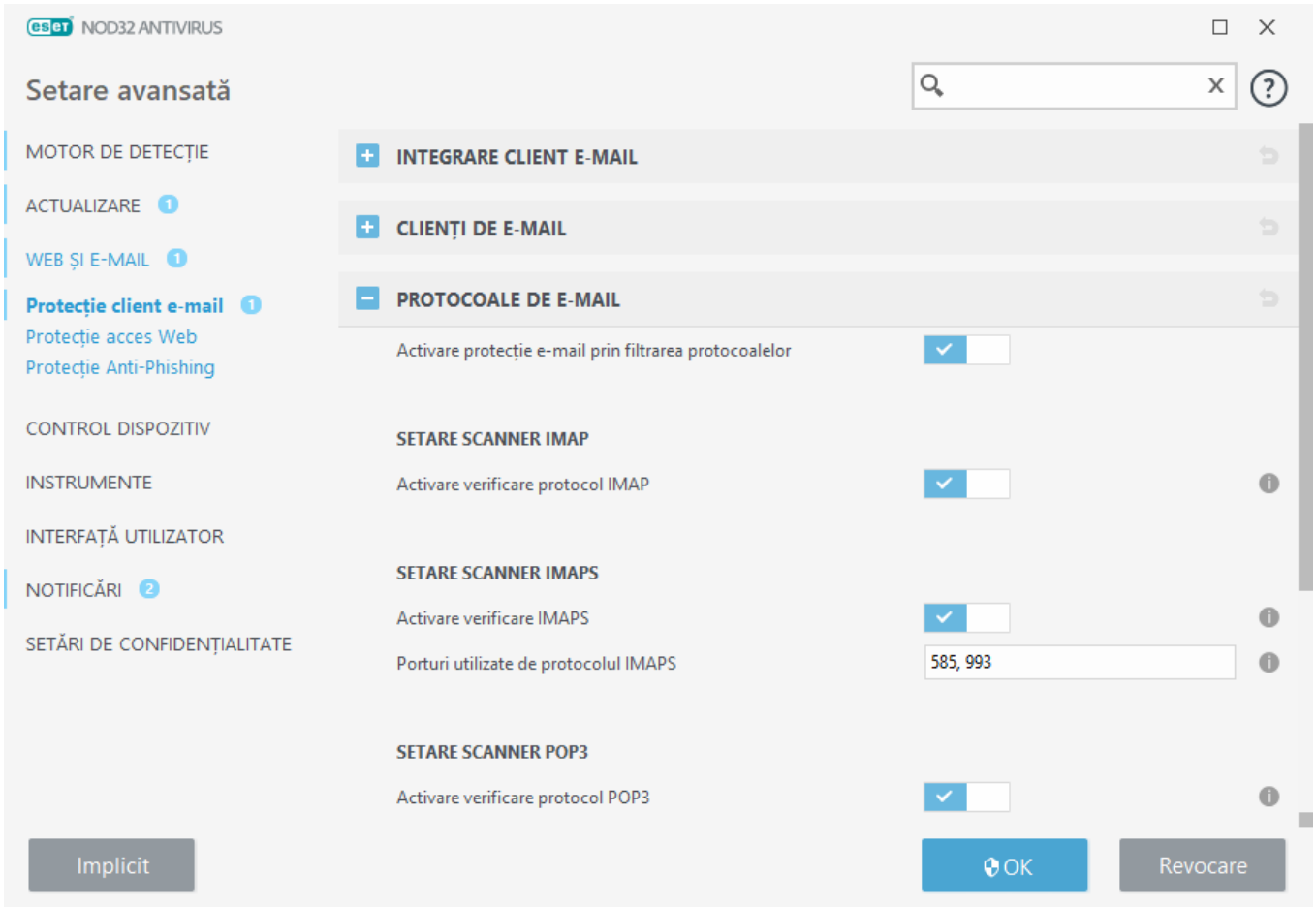
Protocoalele IMAP și POP3 sunt cele mai utilizate pentru comunicarea prin e-mail într-o aplicație client de e-mail. Internet Message Access Protocol (IMAP) este un alt protocol Internet pentru recuperarea mesajelor de e-mail. IMAP are unele avantaje față de POP3, de exemplu, mai mulți clienți se pot conecta simultan la aceeași cutie poștală și pot să mențină informații despre starea mesajelor, cum ar fi dacă mesajul a fost sau nu citit, șters sau dacă s-a răspuns sau nu la el. Modulul de protecție care furnizează acest control este inițiat automat la pornirea sistemului și apoi rămâne activ în memorie.

ESET NOD32 Antivirus asigură protecție pentru aceste protocoale indiferent de clientul de e-mail utilizat și fără a necesita reconfigurarea clientului de e-mail. În mod implicit, se scanează toată comunicarea prin protocoalele POP3 și IMAP, indiferent care sunt porturile POP3/IMAP implicite.
Protocolul IMAP nu este scanat. Însă comunicarea cu serverul Microsoft Exchange poate fi scanată de modulul de integrare în clienți de e-mail cum ar fi Microsoft Outlook.

Vă recomandăm să păstrați activată opțiunea **Activare protecție e-mail prin filtrarea protocoalelor**. Pentru a configura verificarea protocoalelor IMAP/IMAPS și POP3/POP3S, accesați **Setare avansată** > **Web și e-mail** > **Protecție client e-mail** > **Protocoale de e-mail**.

ESET NOD32 Antivirus acceptă și scanarea protocoalelor IMAPS (prin porturile 585, 993) și POP3S (prin portul 995), care utilizează un canal criptat pentru transferarea informațiilor între server și client. ESET NOD32 Antivirus controlează comunicarea utilizând protocoalele SSL (Secure Socket Layer) și TLS (Transport Layer Security). Programul va scana numai traficul de la porturile definite în **Porturi utilizate de protocolul IMAPS/POP3S**, indiferent de versiunea sistemului de operare. Puteți adăuga și alte porturi de comunicare, dacă este necesar. Numerele de porturi trebuie să fie delimitate printr-o virgulă.

Comunicările criptate vor fi scanate în mod implicit. Pentru a vizualiza configurarea scanerului, deschideți Setare avansată > **Web și e-mail** > **SSL/TLS**..



Filtru POP3, POP3S

Protocolul POP3 este cel mai răspândit protocol utilizat pentru a primi comunicări prin email într-o aplicație de client email. ESET NOD32 Antivirus asigură protecția acestui protocol indiferent de clientul de email utilizat.

Modulul de protecție care furnizează acest control este inițiat automat la pornirea sistemului și apoi rămâne activ în memorie. Pentru ca modulul să funcționeze corect, asigurați-vă că acesta este activat – verificarea protocolului POP3 se efectuează automat, fără a necesita reconfigurarea clientului de email. În mod implicit, sunt scanate toate comunicările prin portul 110, dar se mai pot adăuga și alte porturi de comunicare, dacă este necesar. Numerele mai multor porturi trebuie separate printr-o virgulă.

Comunicările criptate vor fi scanate în mod implicit. Pentru a vizualiza configurarea scanerului, deschideți Setare avansată > **Web și e-mail** > SSL/TLS..

În această secțiune puteți configura verificarea protocoalelor POP3 și POP3S.

Activare verificare protocol POP3 – dacă se activează, se monitorizează pentru cod dăunător tot traficul prin POP3.

Porturi utilizate de protocolul POP3 – o listă de porturi utilizată de protocolul POP3 (110 în mod implicit).

ESET NOD32 Antivirus acceptă și verificarea protocolului POP3S. Acest tip de comunicare utilizează un canal criptat pentru a transfera informațiile între server și client. ESET NOD32 Antivirus efectuează verificarea comunicărilor utilizând metodele de criptare SSL (Secure Socket Layer) și TLS (Transport Layer Security).

Nu utiliza verificarea POP3S – comunicația criptată nu va fi verificată.

Utilizează verificarea protocolului POP3S pentru porturile selectate – selectați această opțiune pentru a permite verificarea POP3S numai pentru porturile definite în **Porturi utilizate de protocolul POP3S**.

Porturi utilizate de protocolul POP3S – o listă de porturi POP3S de verificat (implicit: 995).

Etichete e-mail

Opțiunile acestei funcționalități sunt disponibile prin **Setări avansate** > **Web și email** > **Protecție client email** > **Alerte și notificări**.

După verificarea unui e-mail, la mesaj poate fi adăugată o notificare cu rezultatul scanării. Puteți opta pentru opțiunea **Adaugă mesaje etichetă la mesajele e-mail primite și citite** sau **Adaugă mesaje etichetă la mesaje e-mail trimise**. Rețineți că, în cazuri foarte rare, este posibil ca mesajele etichetă să nu fie incluse în mesajele HTML problematice sau dacă mesajele sunt falsificate de malware. Mesajele etichetă pot fi adăugate la mesajele e-mail primite și citite, la mesajele e-mail trimise sau la ambele. Sunt disponibile următoarele opțiuni:

- **Niciodată** – nu se vor adăuga mesaje etichetă.
- **Atunci când se produce o detectare** – vor fi marcate ca verificate numai mesajele ce conțin software dăunător (opțiunea implicită).
- **Pentru toate e-mailurile, în momentul scanării** – programul va adăuga mesaje la toate mesajele e-mail scanate.

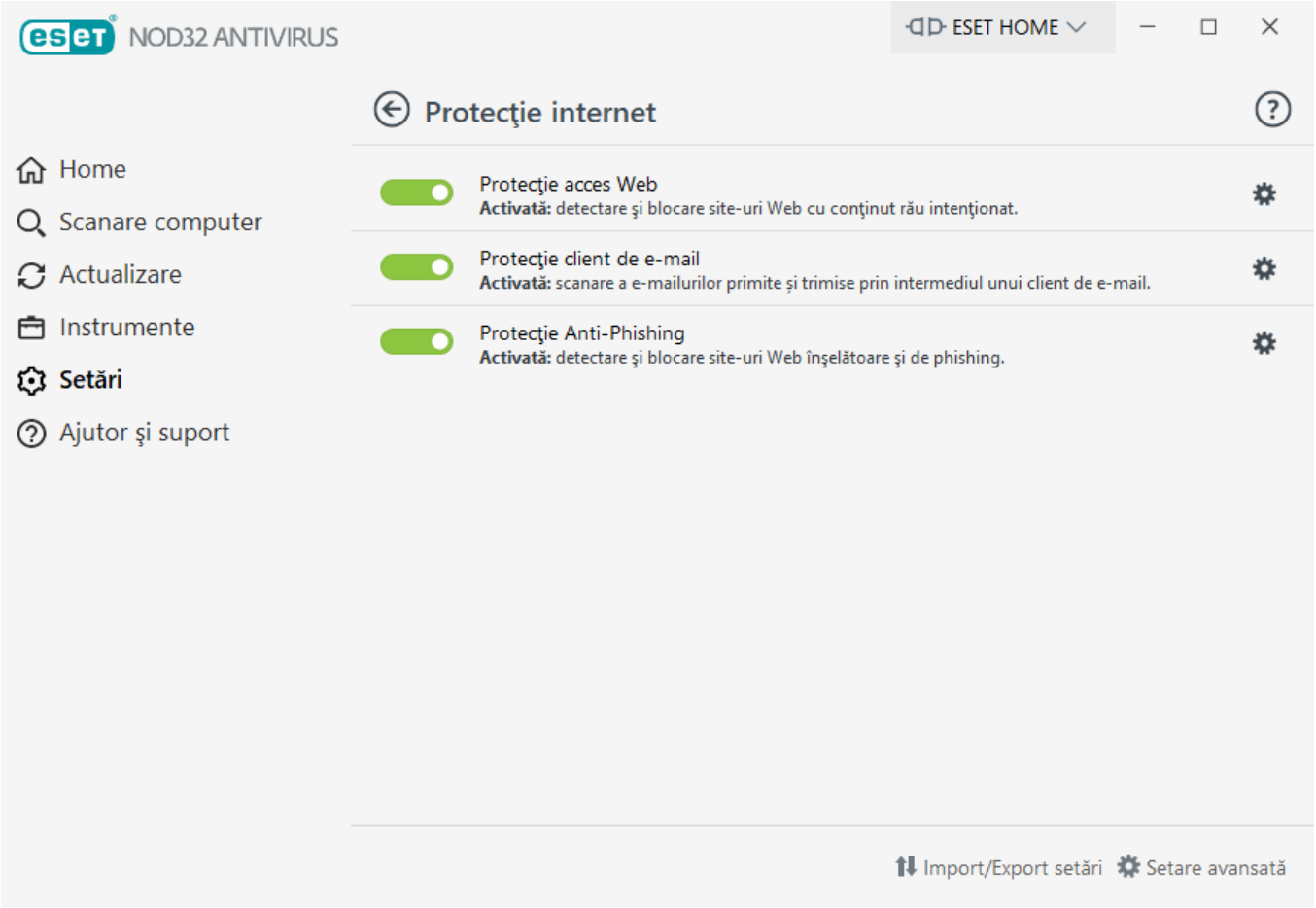
Text de adăugat la subiectul mesajelor e-mail detectate – Editați acest șablon dacă doriți să modificați formatului prefixului de subiect pentru un mesaj e-mail infectat. Această funcție va înlocui subiectul de mesaj „Salut” cu o valoare în formatul următor: „[detecție %DETECTIONNAME%] Salut”. Variabila %DETECTIONNAME% reprezintă amenințarea detectată.

Protecție acces Web

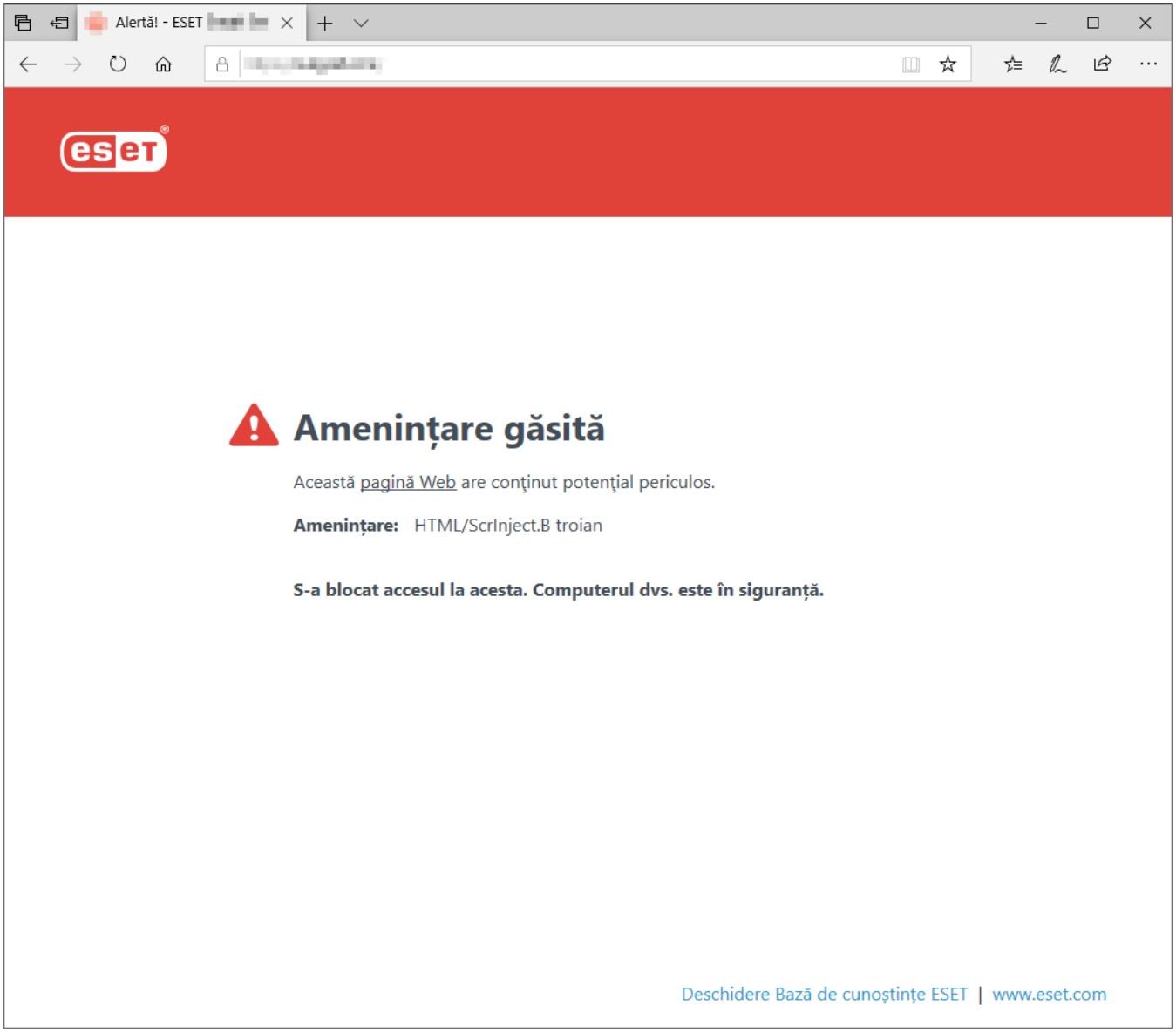
Conectivitatea Internet este o caracteristică standard într-un computer personal. Din păcate, a devenit și mediul principal pentru transferul codului dăunător. Protecția accesului la Web funcționează prin monitorizarea comunicării dintre browserele Web și serverele la distanță și este conformă cu regulile HTTP (Hypertext Transfer Protocol) și HTTPS (comunicare criptată).

Accesul la paginile Web cunoscute că includ conținut dăunător este blocat înainte de descărcarea conținutului. Toate celelalte pagini Web sunt scanate de motorul de scanare ThreatSense atunci când sunt încărcate și sunt blocate dacă se detectează conținut dăunător. Protecția la acces Web oferă două niveluri de protecție – blocarea după lista neagră și blocarea după conținut.

Vă recomandăm insistent să activați opțiunea Protecție acces Web. Această opțiune se poate accesa în fereastra principală a programului > **Setare** > **Protecție Internet** > **Protecție acces Web**.



Componente Protecție acces web va afișa mesajul următor în browser atunci când este blocat site-ul web:



Instrucțiuni ilustrate

Următoarele articole din Baza de cunoștințe ESET este posibil să fie disponibile numai în limba engleză:

- Excluderea unui site web sigur, astfel încât acesta să nu fie blocat de componenta Protecție acces web
- Blocarea unui site web utilizând ESET NOD32 Antivirus

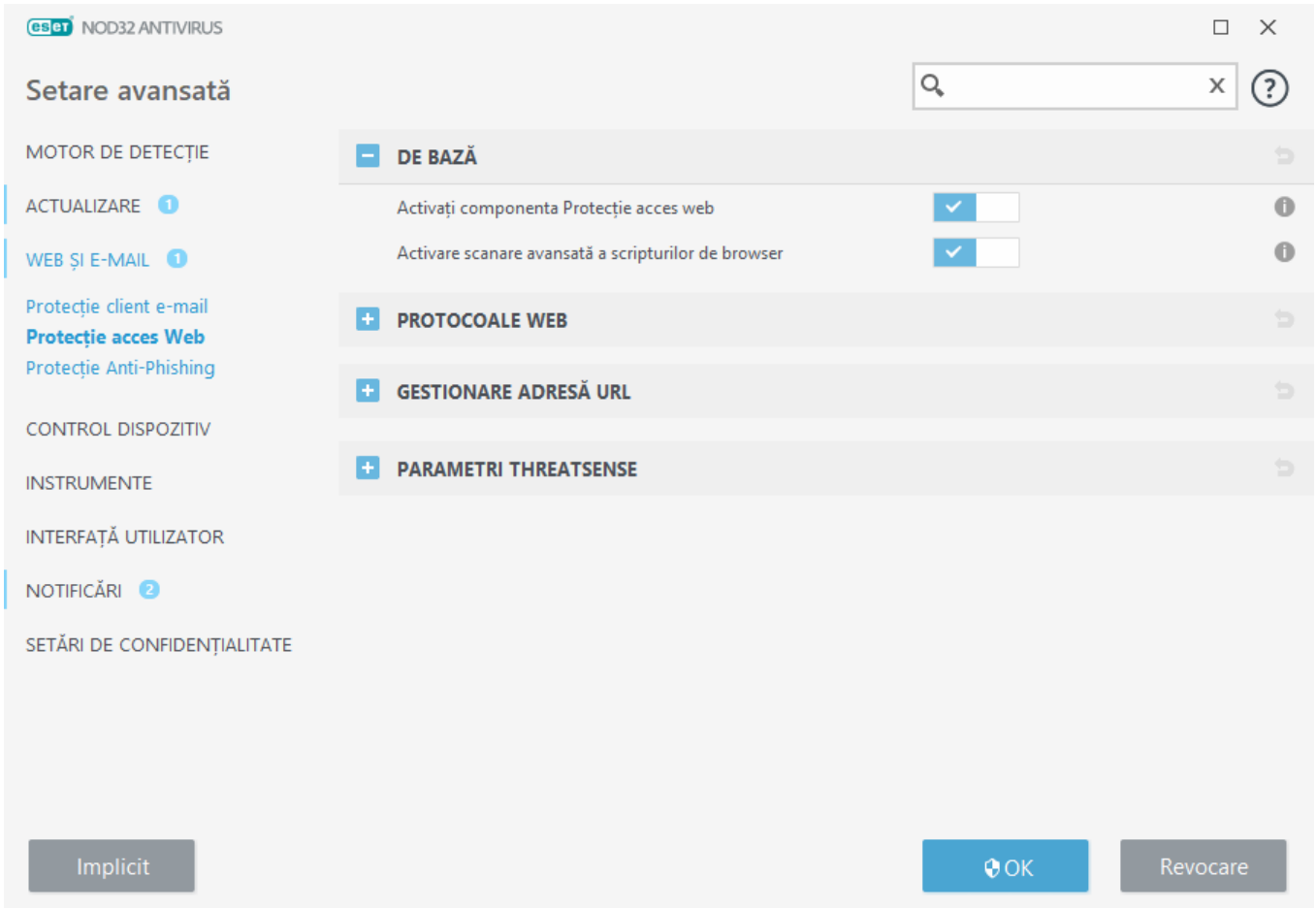
În **Setări avansate** (F5) > **Web și email** > **Protecție acces Web** sunt disponibile următoarele opțiuni:

De bază – pentru a activa sau a dezactiva această caracteristică în Setare avansată.

Protocoale web – vă permite să configurați monitorizarea acestor protocoale standard care sunt utilizate de majoritatea browserelor Internet.

Gestionare adrese URL – vă permite să specificați adresele URL care vor fi blocate, permise sau excluse de la verificare.

Parametri ThreatSense – setare avansată a scanării de viruși – vă permite să configurați setări precum tipurile de obiecte de scanat (email-uri, arhive etc.), metode de detectare pentru protecția accesului Web etc.



Setare avansată pentru Protecție acces web

În **Setări avansate** (F5) > **Web și e-mail** > **Protecție acces web** > **De bază** sunt disponibile următoarele opțiuni:

Activare Protecție acces web – atunci când această opțiune este dezactivată, nu se vor executa componentele protecție acces web și protecție anti-phishing. Această opțiune este disponibilă numai atunci când este activată filtrarea protocoalelor SSL/TLS.

Activare scanare avansată a scripturilor de browser – atunci când această opțiune este activată, toate programele JavaScript executate de browserele web vor fi verificate de motorul de detecție.

Vă recomandăm cu insistență să lăsați activată opțiunea Protecție acces Web.

Protocoale Web

În mod implicit, ESET NOD32 Antivirus este configurat să monitorizeze protocolul HTTP utilizat de majoritatea browserelor Internet.

Setare scaner HTTP

Traficul HTTP este monitorizat întotdeauna pentru toate porturile și pentru toate aplicațiile.

Setare scaner HTTPS

ESET NOD32 Antivirus acceptă, de asemenea, verificarea protocolului HTTPS. Comunicația HTTPS utilizează un canal criptat pentru a transfera informațiile între server și client. ESET NOD32 Antivirus efectuează verificarea comunicației utilizând protocoalele SSL (Secure Socket Layer) și TLS (Transport Layer Security). Programul va scana numai traficul de la porturile (443, 0-65535) definite în **Porturi utilizate de protocolul HTTPS** indiferent de versiunea sistemului de operare.

Comunicările criptate vor fi scanate în mod implicit. Pentru a vizualiza configurarea scanerului, deschideți Setare avansată > **Web și e-mail** > **SSL/TLS**..

Gestionare adresă URL

Secțiunea de gestionare a adreselor URL vă permite să specificați adresele HTTP care vor fi blocate, permise sau excluse de la scanarea conținutului.

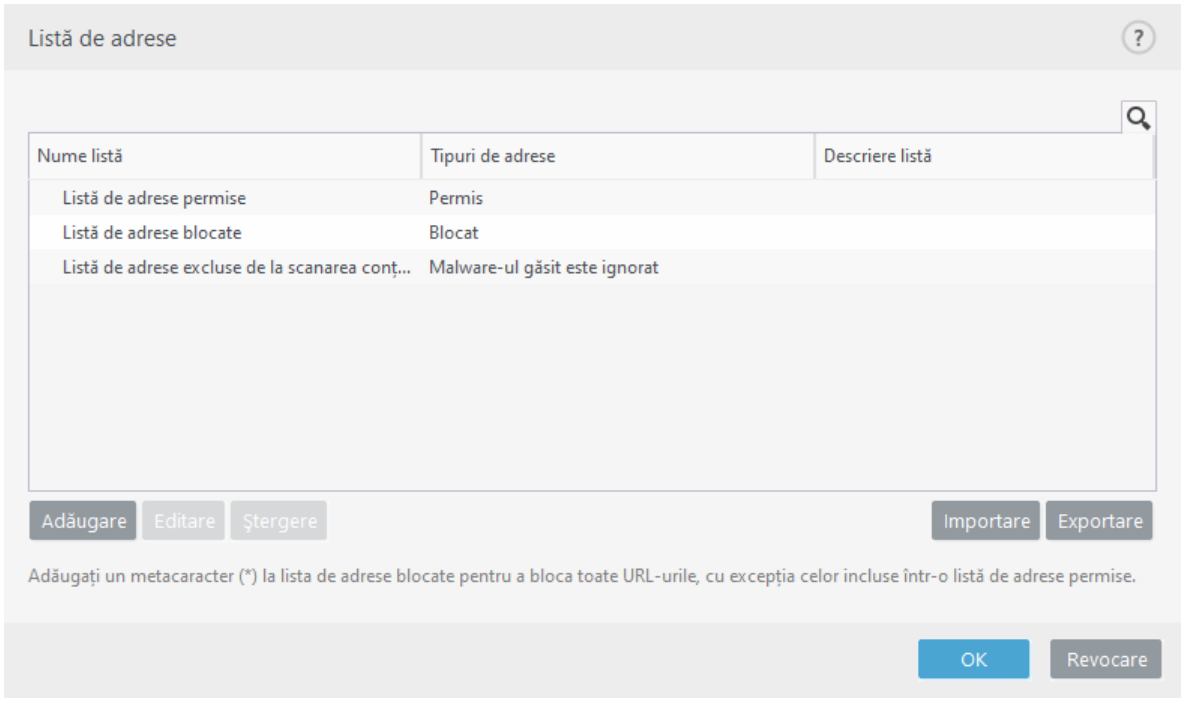
Dacă, pe lângă paginile Web HTTP, doriți să fie filtrate și adresele HTTPS, trebuie să bifați opțiunea Activare filtrare protocol SSL/TLS. În caz contrar, vor fi adăugate numai domeniile site-urilor HTTPS pe care le-ați vizitat, însă nu vor fi adăugat URL-urile complete.

Site-urile web din **Lista de adrese blocate** nu vor fi accesibile decât dacă sunt incluse și în **Lista de adrese permise**. Site-urile web din **Listă de adrese excluse de la scanarea conținutului** nu sunt scanate pentru cod dăunător atunci când sunt accesate.

Dacă doriți să blocați toate adresele HTTP, cu excepția adreselor prezente în **Lista de adrese permise** activă, adăugați * la **Lista de adrese blocate** activă.

Simbolurile speciale * (asterisc) și ? (semnul întrebării) pot fi utilizate în liste. Asteriscul înlocuiește orice șir de caractere, iar semnul de întrebare înlocuiește orice simbol. Se va acorda o atenție specială la specificarea adreselor excluse, deoarece lista trebuie să conțină numai adresele de încredere și sigure. În mod similar, este necesar să vă asigurați că simbolurile * și ? sunt utilizate corect în listă. Consultați Adăugare adresă HTTP/mască domeniu pentru a afla cum puteți selecta în siguranță un întreg domeniu, inclusiv subdomeniile sale. Pentru a activa o listă, selectați **Listă activă**. Dacă doriți să primiți o notificare la introducerea unei adrese din lista curentă, selectați **Notificare la aplicare**.

> **Domenii de încredere**
> Adresele nu vor fi filtrate dacă setarea **Web și e-mail** > **SSL/TLS** > **Excludeți comunicarea cu domeniile de încredere** este activată, iar domeniul este considerat de încredere.



Elemente de control

Adăugare – creează o listă nouă în plus față de cele predefinite. Acest lucru poate fi util dacă doriți să separați logic diferite grupuri de adrese. De exemplu, o listă de adrese blocate poate conține adrese dintr-o listă neagră externă publică, iar o a doua listă poate conține propria dvs. listă neagră, ceea ce simplifică actualizarea listei externe cu păstrarea intactă a listei proprii.

Editare – modifică liste existente. Utilizați această opțiune pentru a adăuga sau elimina adrese.

Ștergere – șterge listele existente. Opțiunea este disponibilă numai pentru liste create cu opțiunea **Adăugare**, nu și pentru listele implicite.

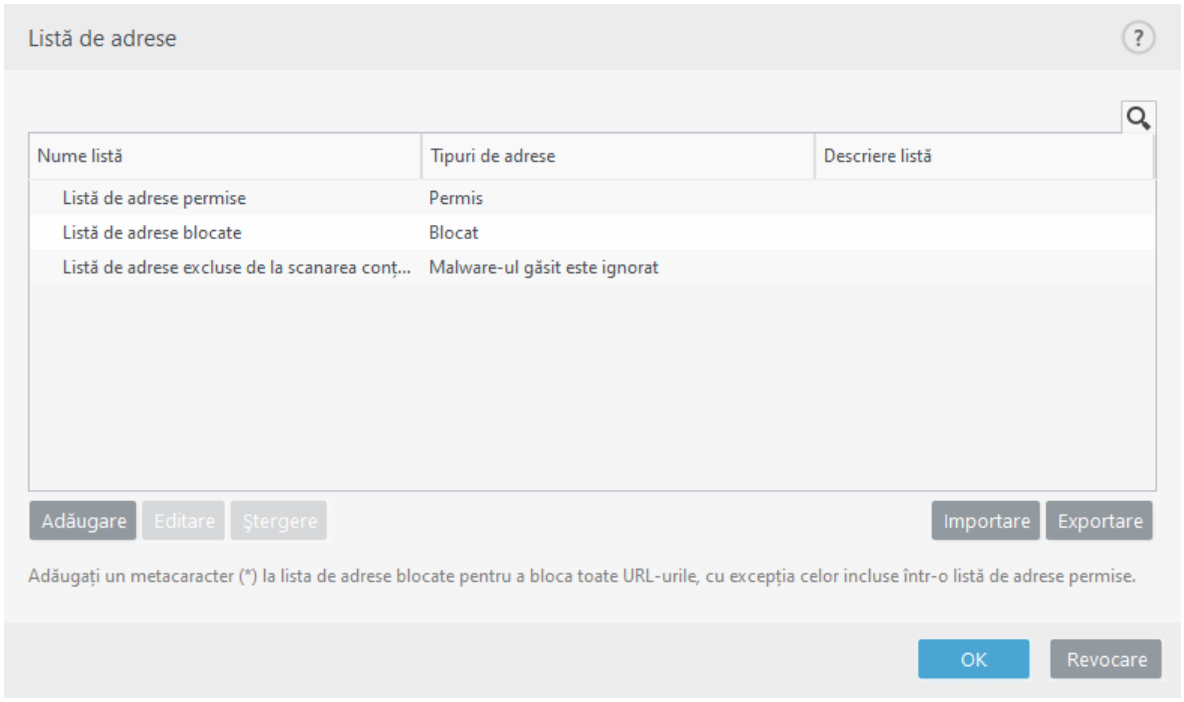
Listă de adrese URL

Această secțiune vă permite să specificați liste de adrese HTTP care vor fi blocate, permise sau excluse de la verificare.

În mod implicit, sunt disponibile următoarele trei liste:

- **Listă de adrese excluse de la scanarea conținutului** – adresele adăugate în această listă nu vor fi verificate pentru a detecta cod rău intenționat.
- **Listă de adrese permise** – Dacă este activată opțiunea Permite accesul numai la adresele HTTP din lista de adrese permise și lista de adrese blocate conține * (potrivire cu orice), utilizatorul va avea permisiunea să acceseze numai adresele specificate în această listă. Adresele din această listă sunt permise chiar dacă sunt incluse în lista de adrese blocate.
- **Listă de adrese blocate** – utilizatorul nu va avea permisiunea să acceseze adresele specificate în această listă decât dacă acestea sunt prezente și în lista de adrese permise.

Faceți clic pe **Adăugare** pentru a crea o listă nouă. Pentru a șterge listele selectate, faceți clic pe **Ștergere**.



Instrucțiuni ilustrate

Următoarele articole din Baza de cunoștințe ESET este posibil să fie disponibile numai în limba engleză:

- Excluderea unui site web sigur, astfel încât acesta să nu fie blocat de componenta Protecție acces web
- Blocarea unui site web folosind produse ESET Windows Home

Pentru mai multe informații, consultați Gestionare adrese URL.

Crearea unei liste noi de adrese URL

Această secțiune vă permite să specificați lista de adrese/măști URL care vor fi blocate, permise sau excluse de la verificare.

Dacă creați o listă nouă, sunt valabile pentru configurare opțiunile următoare:

Tip listă de adrese – sunt disponibile aceste tipuri de listă:

- **Exclus de la verificare** – adresele adăugate în listă nu se vor verifica de cod dăunător.
- **Blocate** - utilizatorul nu va avea permisiunea să acceseze adresele specificate în această listă.
- **Permise** – dacă este activată opțiunea Permite accesul numai la adresele HTTP din lista de adrese permise și lista de adrese blocate conține * (potrivire cu orice), utilizatorul va avea permisiunea să acceseze numai adresele specificate în această listă. Adresele din această listă sunt permise chiar dacă sunt prezente în lista de adrese blocate.

Nume listă – Specificați numele listei. Acest câmp va fi inactiv când editați una dintre cele trei liste predefinite.

Descriere listă – introduceți o descriere scurtă a listei (opțional). Va fi inactiv când editați una dintre cele trei liste predefinite.

Pentru a activa o listă, selectați **Listă activă** lângă lista respectivă. Dacă doriți să primiți o notificare atunci când se utilizează o anumită listă pentru evaluarea unui site HTTP vizitat, selectați **Notificare la aplicare**. De exemplu, se

va emite o notificare dacă un site Web este blocat sau permis, deoarece este inclus în lista adreselor blocate sau permise. Notificarea va conține numele listei care include site-ul Web specificat.

Elemente de control

Adăugare – adăugați a adresă URL nouă la listă (introduceți mai multe valori cu separator).

Editare – modifică adresa existentă în listă. Posibil numai pentru adresele create cu **Adăugare**.

Eliminare – șterge adresele existente în listă. Posibil numai pentru adresele create cu **Adăugare**.

Import – importați un fișier cu adrese URL (valori separate pe câte un rând, de exemplu *.txt utilizând codificarea UTF-8).

Cum se adaugă o mască URL

Consultați instrucțiunile din acest dialog înainte de a introduce adresa/masca de domeniu dorită.

ESET NOD32 Antivirus permite utilizatorului să blocheze accesul la site-uri Web specificate și să împiedice browser-ul Internet să le afișeze conținutul. Mai mult, permite utilizatorului să specifice adrese care trebuie excluse de la verificare. Dacă numele complet al serverului la distanță nu este cunoscut sau utilizatorul dorește să specifice un întreg grup de servere la distanță, puteți folosi așa numitele măști pentru a identifica un astfel de grup. Măștile includ simbolurile „?” și „*”:

- folosiți ? pentru a înlocui un simbol
- folosiți * pentru a înlocui un șir text.

De exemplu *.c?m se aplică tuturor adreselor pentru care ultima parte începe cu litera c, care se termină cu litera m și care conțin un simbol necunoscut între acestea (.com, .cam etc.)

Secvența inițială „*.” este tratată special atunci când este folosită la începutul unui nume de domeniu. Metacaracterul * nu caută în acest caz potriviri pentru caracterul bară oblică („/”). Aceasta pentru a preveni evitarea măștii, de exemplu, masca **.domain.com* nu va fi corespunde *http://anydomain.com/anypath#.domain.com* (such suffix can be appended to any URL without affecting the download). În al doilea rând, „*.” caută și corespondențe pentru orice șir necompletat în acest caz special. Aceasta pentru a permite găsirea corespondenței pentru domeniul complet, inclusiv orice subdomenii, folosind o singură mască. De exemplu, masca **.domain.com* va returna și corespondențele *http://domain.com*. Utilizarea **domain.com* nu este corectă, deoarece va returna și corespondențele *http://anotherdomain.com*.

Protecție Anti-Phishing

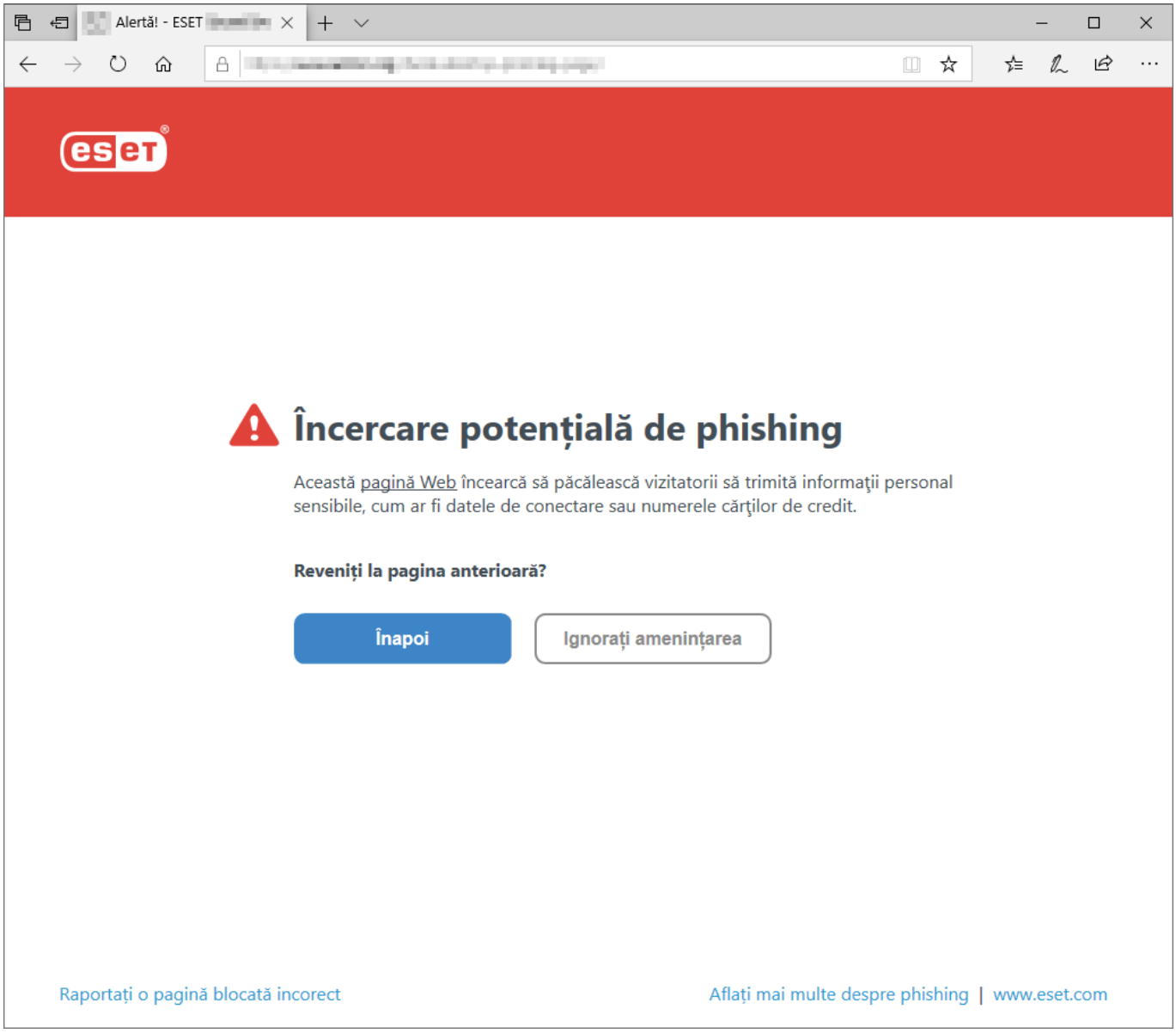
Termenul phishing (înşelătorie) defineşte o activitate infracțională care foloseşte tehnici de inginerie socială (manipularea utilizatorilor pentru a obține informații confidențiale). Phishing – utilizat adesea pentru a obține acces la date sensibile, cum ar fi numere de cont bancar, coduri PIN etc. Citiți detalii despre această activitate în glosar. ESET NOD32 Antivirus include protecție împotriva phishing-ului, care blochează paginile Web cunoscute că distribuie astfel de conținut.

Vă recomandăm insistent să activați modulul Anti-Phishing în ESET NOD32 Antivirus. Pentru aceasta, deschideți **Setări avansate** (F5) și navigați la **Web și email** > **Protecție Anti-Phishing**.

Citiți articolul din baza de cunoștințe ESET pentru mai multe informații despre protecția Anti-Phishing în ESET NOD32 Antivirus.

Accesarea unui site Web înșelător

Atunci când accesați un site Web recunoscut ca fiind de phishing, se afișează dialogul următor în browserul Web. Dacă doriți în continuare să accesați site-ul Web, faceți clic pe **Ignorare amenințare** (nerecomandat).



Site-urile Web potențial înșelătoare trecute în lista albă vor expira în mod implicit după câteva ore. Pentru a permite permanent un site Web, utilizați instrumentul Gestionare adrese URL. În **Setări avansate** (F5) > **Web și email** > **Protecție acces Web** > **Gestionare adrese URL** > **Listă de adrese** > **Editare** adăugați site-ul Web pe care doriți să-l editați la listă.

Raportarea unui site înșelător

Legătura **Raportare** vă permite să raportați un site Web de phishing/dăunător pentru a fi analizat de ESET.

Înainte de a trimite un site Web la ESET, asigurați-vă că îndeplinește unul sau mai multe dintre următoarele criterii:
- Site-ul Web nu este detectat deloc.
- Site-ul Web este detectat în mod incorect ca fiind o amenințare. În acest caz, puteți să Raportați o pagină blocată incorect.

Alternativ, puteți trimite site-ul Web prin email. Trimiteți mesajul de email la samples@eset.com. Nu uitați să utilizați un subiect descriptiv și să includeți cât mai multe informații posibil despre site-ul Web (de exemplu, site-ul Web care v-a direcționat aici, cum ați auzit despre acest site Web etc.).

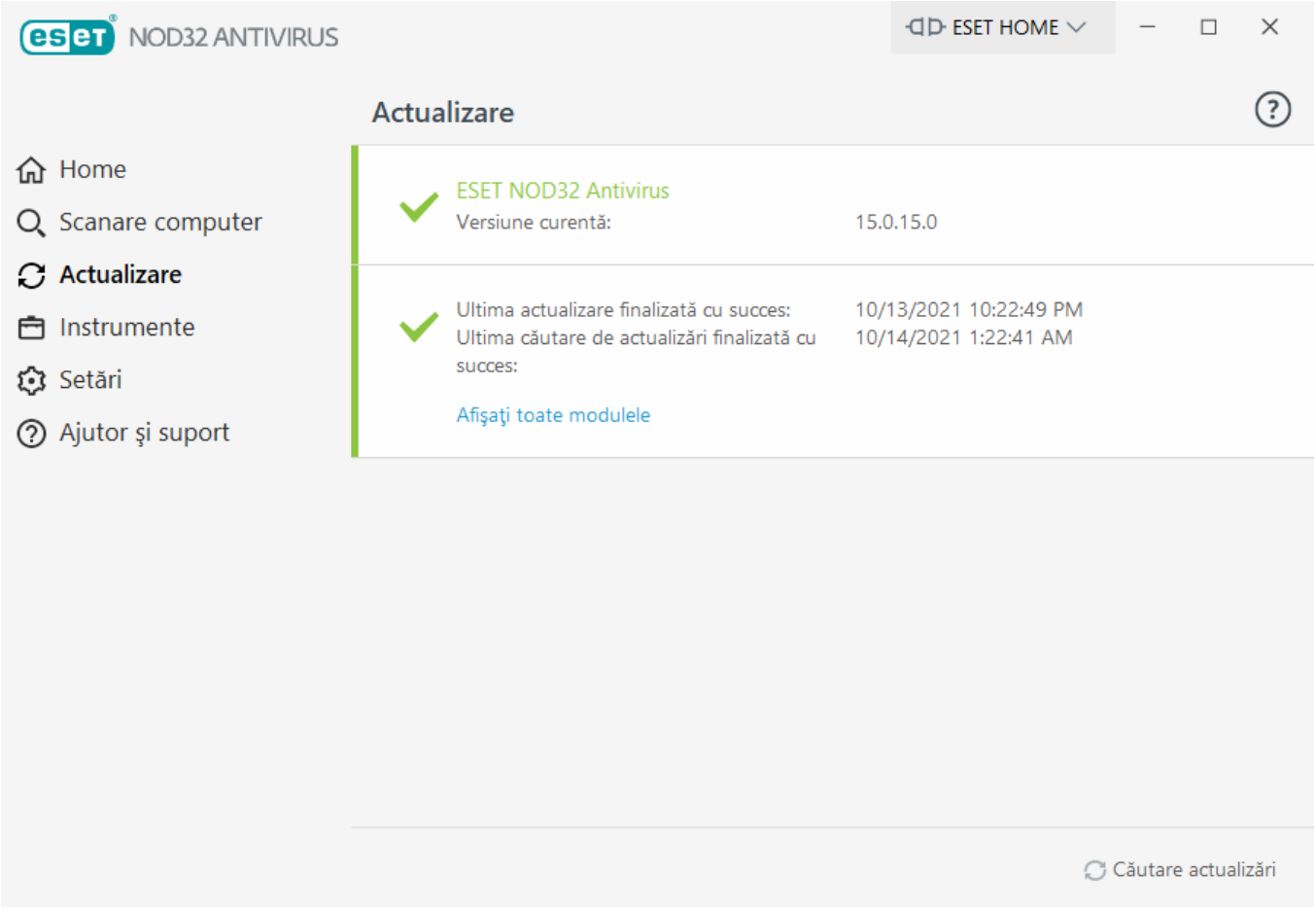
Actualizare program

Actualizarea regulată a produsului ESET NOD32 Antivirus este cea mai bună metodă de a asigura nivelul maxim de securitate pe computerul dvs. Modulul Actualizare asigură că atât modulele de program, cât și componentele sistemului sunt întotdeauna actualizate.

Cu clic pe **Actualizare** în fereastra principală a meniului, puteți vizualiza starea curentă a actualizării, inclusiv data și ora ultimei actualizări reușite și dacă este necesară o actualizare.

Pe lângă actualizările automate, puteți face clic pe **Căutare actualizări** pentru a declanșa o actualizare manuală. Actualizarea regulată a modulelor și componentelor programului este un aspect important pentru menținerea protecției complete împotriva codurilor dăunătoare. Acordați atenție configurării și funcționării modulelor produsului. Trebuie să activați produsul utilizând cheia de licență pentru a primi actualizări. Dacă nu ați făcut acest lucru în timpul instalării, trebuie să introduceți cheia de licență pentru a activa produsul și a accesa serverele de actualizare ESET.

Ați primit cheia de licență într-un e-mail de la ESET după achiziționarea produsului ESET NOD32 Antivirus.



Versiune curentă – arată numărul versiunii curente a produsului pe care l-ați instalat.

Ultima actualizare realizată cu succes – arată data ultimei actualizări realizată cu succes. Dacă nu vedeți o dată recentă, este posibil ca modulele produsului să nu fie actualizate.

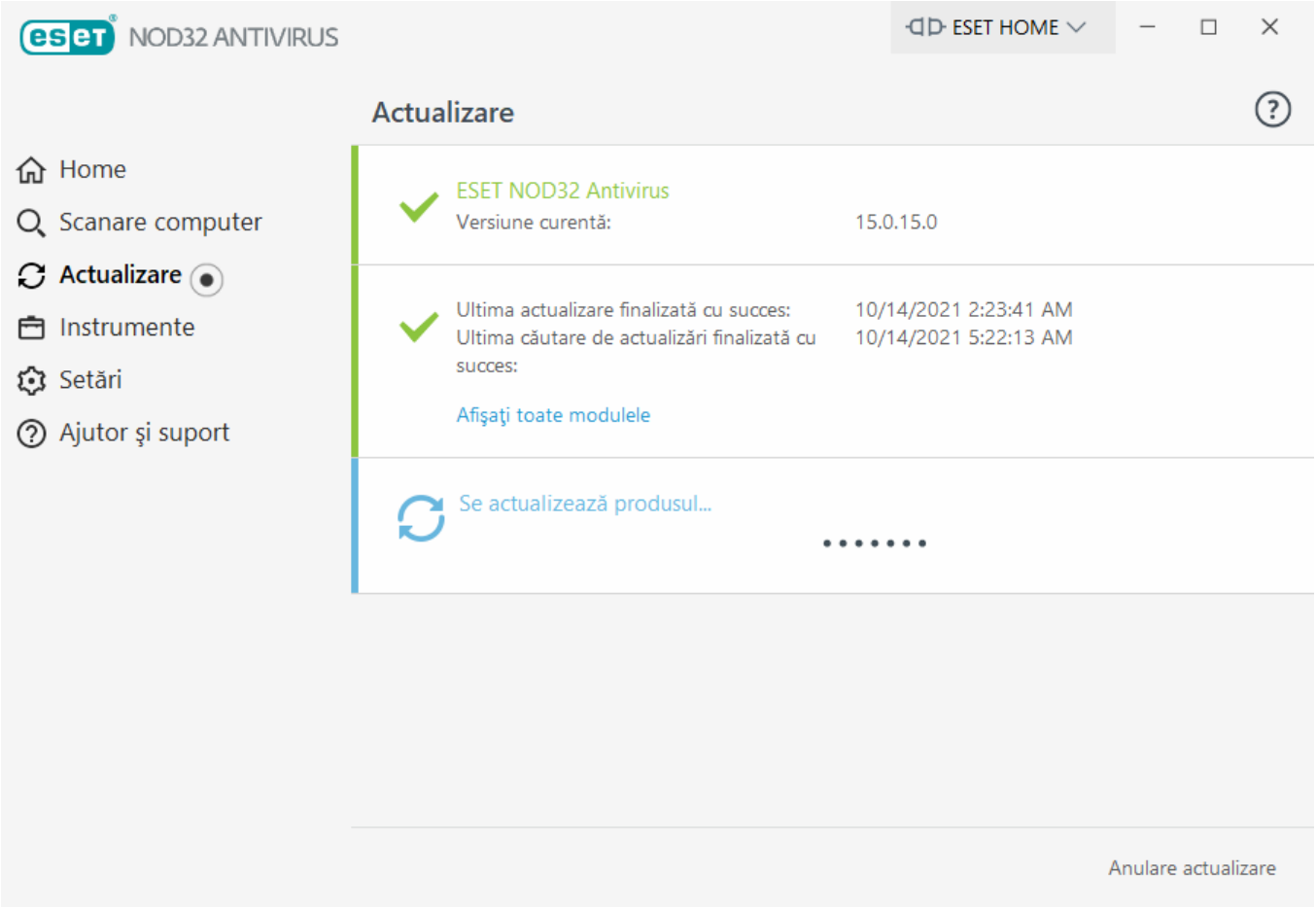
Ultima căutare a actualizărilor realizată cu succes – arată data ultimei căutări de actualizări realizată cu succes.

Afișați toate modulele – arată despre lista modulelor de program instalate.

Faceți clic pe **Căutare actualizări** pentru a detecta cea mai recentă versiune ESET NOD32 Antivirus disponibilă.

Proces de actualizare

După ce faceți clic pe **Căutare actualizări**, începe descărcarea. Sunt afișate o bară de progres pentru descărcare și timpul rămas pentru descărcare. Pentru a întrerupe actualizarea, faceți clic pe **Anulare actualizare**.



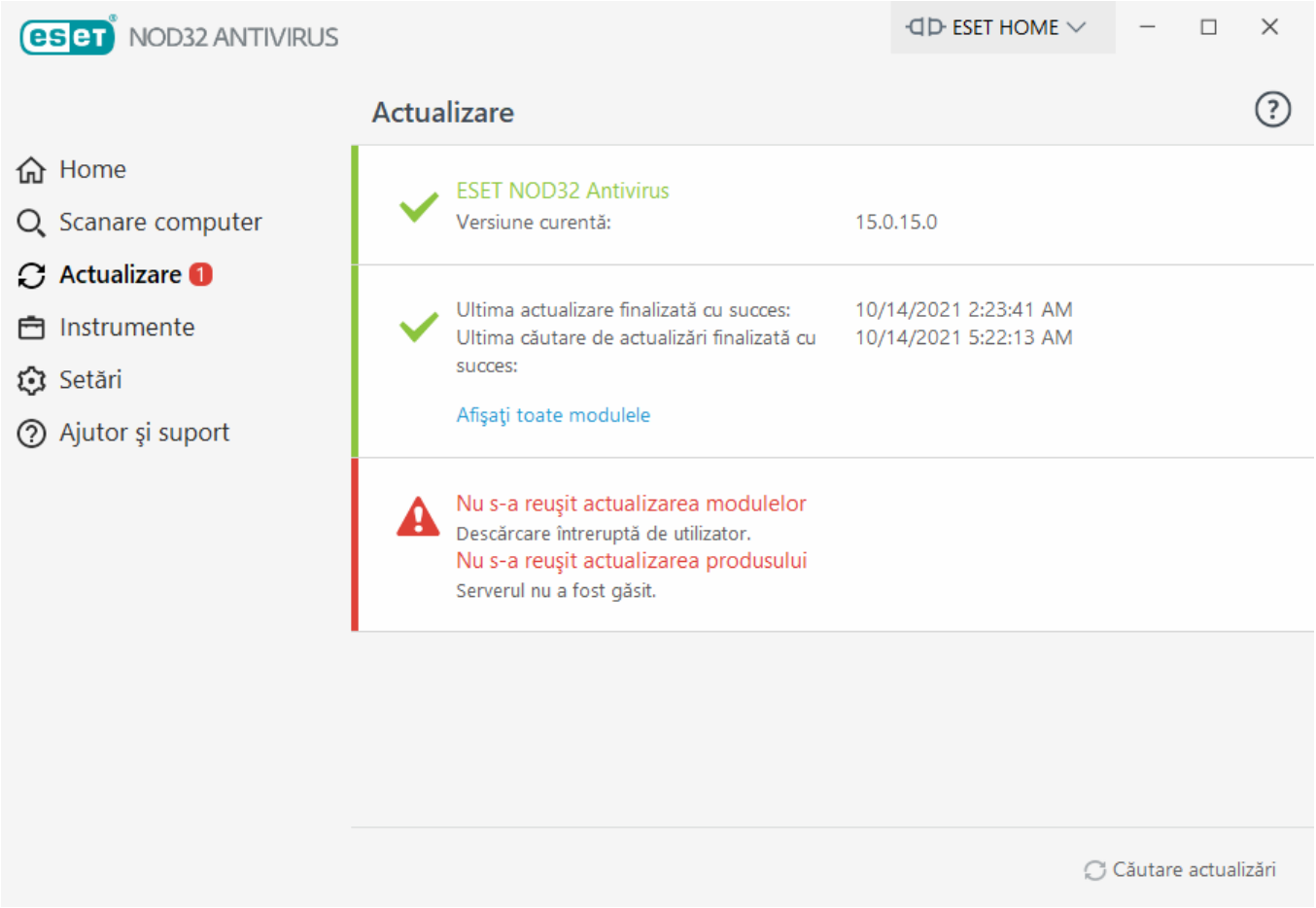
În condiții normale, veți vedea o bifă verde în fereastra **Actualizare** care indică faptul că programul este actualizat. Dacă lucrurile nu vedeți bifa verde, programul nu este actualizat și este mai vulnerabil la infectare. Actualizați modulele programului cât mai curând posibil.

Actualizare eșuată

Dacă primiți un mesaj de informare cu privire la actualizări eșuate ale modulelor, acesta poate fi cauzat de următoarele probleme:

1. **Licență nevalidă** – Licența utilizată pentru activare nu este validă sau a expirat. În fereastra principală a programului, faceți clic pe **Ajutor și suport** > **Schimbare licență** și introduceți o cheie de licență nouă.

2. **Eroare la descărcarea fișierelor de actualizare** – această notificare poate avea drept cauză setări de conexiune la Internet incorecte. Vă recomandăm să verificați conexiunea la Internet (deschizând un site Web la întâmplare în browserul Web). Dacă site-ul Web nu se deschide, probabil nu s-a stabilit conexiunea la Internet sau există probleme de conectivitate cu computerul. Contactați furnizorul de servicii Internet (ISP) dacă nu aveți o conexiune activă la Internet.



Vă recomandăm să reporniți computerul după realizarea cu succes a unei actualizări a ESET NOD32 Antivirus la o versiune de produs mai nouă, pentru a vă asigura că toate modulele programului au fost actualizate corect. Nu este necesară repornirea computerului după actualizările obișnuite ale modulelor.

Pentru mai multe informații, consultați Depanarea mesajului „Nu s-a reușit actualizarea modulelor”.

Setare actualizare

Opțiunile pentru setarea actualizării sunt disponibile în structura **Setări avansate** (F5) la **Actualizare** > **De bază**. Această secțiune specifică informațiile despre sursa actualizării, cum ar fi serverele de actualizare utilizate și datele de autentificare pentru aceste servere.

De bază

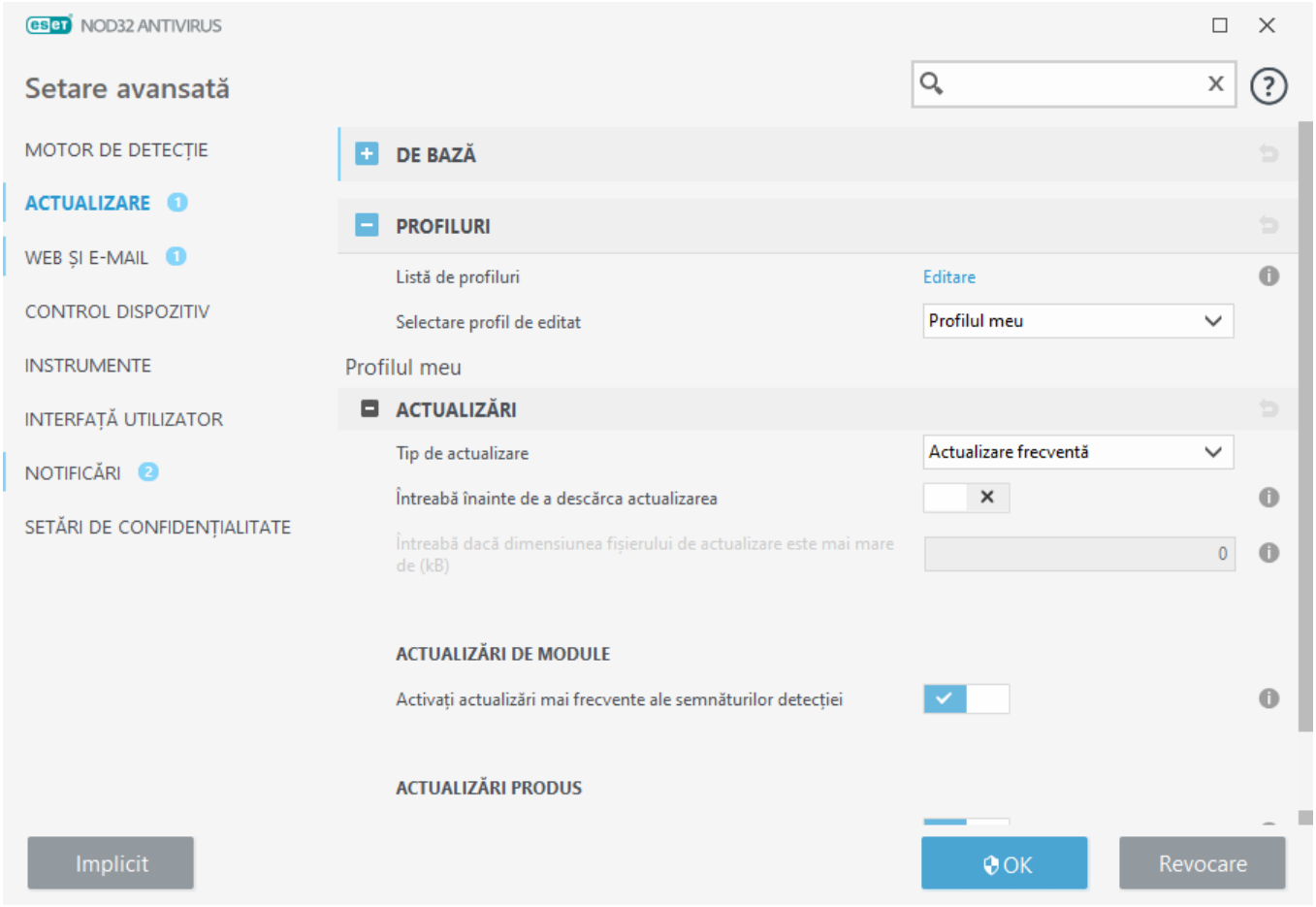
Profilul de actualizare utilizat în uz (cu excepția cazului în care ați configurat unul în mod explicit în **Setări avansate** > **Firewall** > **Rețele cunoscute**) este afișat în meniul vertical **Selectare profil implicit de actualizare**.

Pentru a crea un profil nou, consultați secțiunea Profiluri de actualizare.

Dacă aveți probleme atunci când încercați să descărcați actualizări ale motorului de detecție sau ale modulelor, faceți clic pe **Golire** pentru a goli fișiere/memoria cache de actualizări temporare.

Revenire la versiunea anterioară a modulului

Dacă aveți suspiciunea că o actualizare nouă a motorului de detectare și/sau a modulelor de program este instabilă sau deteriorată, puteți reveni la versiunea anterioară și dezactiva actualizările pentru o perioadă de timp stabilită.



Pentru ca acestea să fie descărcate corect, este esențial să completați corect toți parametrii de actualizare. Dacă utilizați un paravan de protecție, asigurați-vă că programul ESET are permisiunea de a comunica prin Internet (de exemplu, comunicare HTTP).

Profiluri

Se pot crea profiluri de actualizare pentru diverse configurații și sarcini de actualizare. Crearea de profiluri de actualizare este utilă în special pentru utilizatorii mobili, care necesită profiluri alternative pentru proprietățile conexiunii Internet care se modifică în mod de regulat.

Meniul vertical **Selectare profil de editat** afișează profilul selectat curent, valoarea implicită fiind **Profilul meu**. Pentru a crea un profil nou, faceți clic pe **Editare** lângă **Listă de profiluri**, introduceți propriul dvs. **Nume de profil**, apoi faceți clic pe **Adăugare**.

Actualizări

În mod implicit, opțiunea **Tip de actualizare** este setată la **Actualizare regulată** pentru a se asigura descărcarea automată a fișierelor de actualizare de pe serverul ESET cu cel mai redus trafic de rețea. Actualizările versiunii de încercare (opțiunea **Actualizare versiune de încercare**) au trecut printr-o testare internă completă și vor fi disponibile pentru publicul larg în curând. Activându-le, veți avea acces la cele mai recente metode de detectare și

corecții. Însă ele pot să nu fie întotdeauna stabile și NU trebuie folosite pe servere și stații de lucru care necesită disponibilitate și stabilitate maxime.

Întreabă înainte de a descărca actualizarea – Programul va afișa o notificare în care puteți confirma sau refuza descărcarea fișierelor actualizării.

Întreabă dacă dimensiunea fișierului de actualizare este mai mare de (kB) – Programul va afișa un dialog de confirmare dacă dimensiunea fișierului de actualizare este mai mare decât valoarea specificată. Dacă dimensiunea fișierului de actualizare este setată la 0 kB, programul va afișa întotdeauna un dialog de confirmare.

Dezactivare notificare privind actualizări efectuate cu succes – se dezactivează notificarea din bara de sistem din colțul din colțul din dreapta jos al ecranului. Este util să selectați această opțiune dacă se execută o aplicație sau un joc pe ecran complet. Rețineți că modul pentru jocuri va dezactiva toate notificările.

Actualizări modul

Activați actualizări mai frecvente ale semnăturilor de detecție – Semnăturile de detecție vor fi activate la intervale mai scurte. Dezactivarea acestei setări poate afecta negativ rata de detecție.

Actualizări produs

Actualizări ale funcționalităților aplicației – Instalați automat versiuni noi de ESET NOD32 Antivirus.

Opțiuni de conectare

Pentru a utiliza un server proxy pentru a descărca actualizările, consultați secțiunea Opțiuni de conectare.

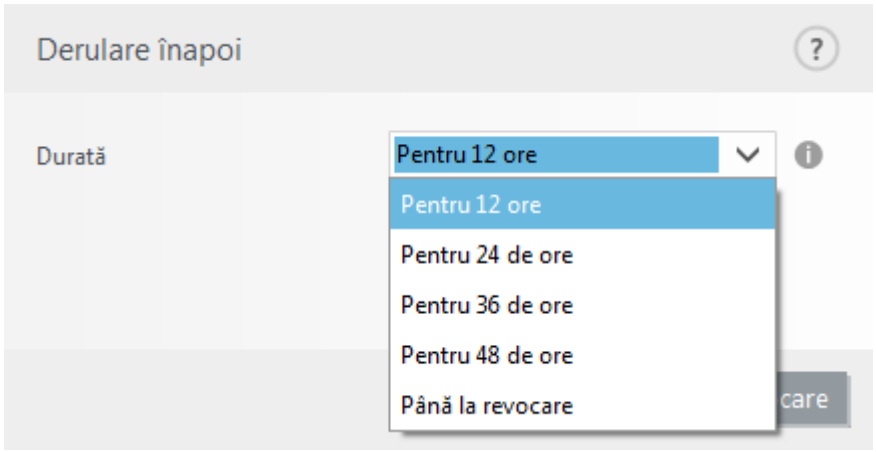
Derularea înapoi a actualizărilor

Dacă suspectați că o actualizare nouă a motorului de detecție sau a modulelor de program este instabilă sau deteriorată, puteți reveni la versiunea anterioară și puteți dezactiva temporar actualizările. Alternativ, puteți activa actualizările dezactivate anterior dacă le-ați amânat pentru o perioadă nedefinită.

ESET NOD32 Antivirus înregistrează instantanee ale motorului de detecție și modulelor de program care pot fi utilizate cu caracteristica Derulare înapoi. Pentru a crea instantanee ale bazei de date de viruși, păstrați activată opțiunea **Creați instantanee cu modulele**. Când opțiunea **Creați instantanee cu modulele** este activată, primul instantaneu este creat în timpul primei actualizări. Următorul este creat după 48 de ore. Câmpul **Număr de instantanee stocate local** definește numărul de instantanee ale motorului de detecție stocate.

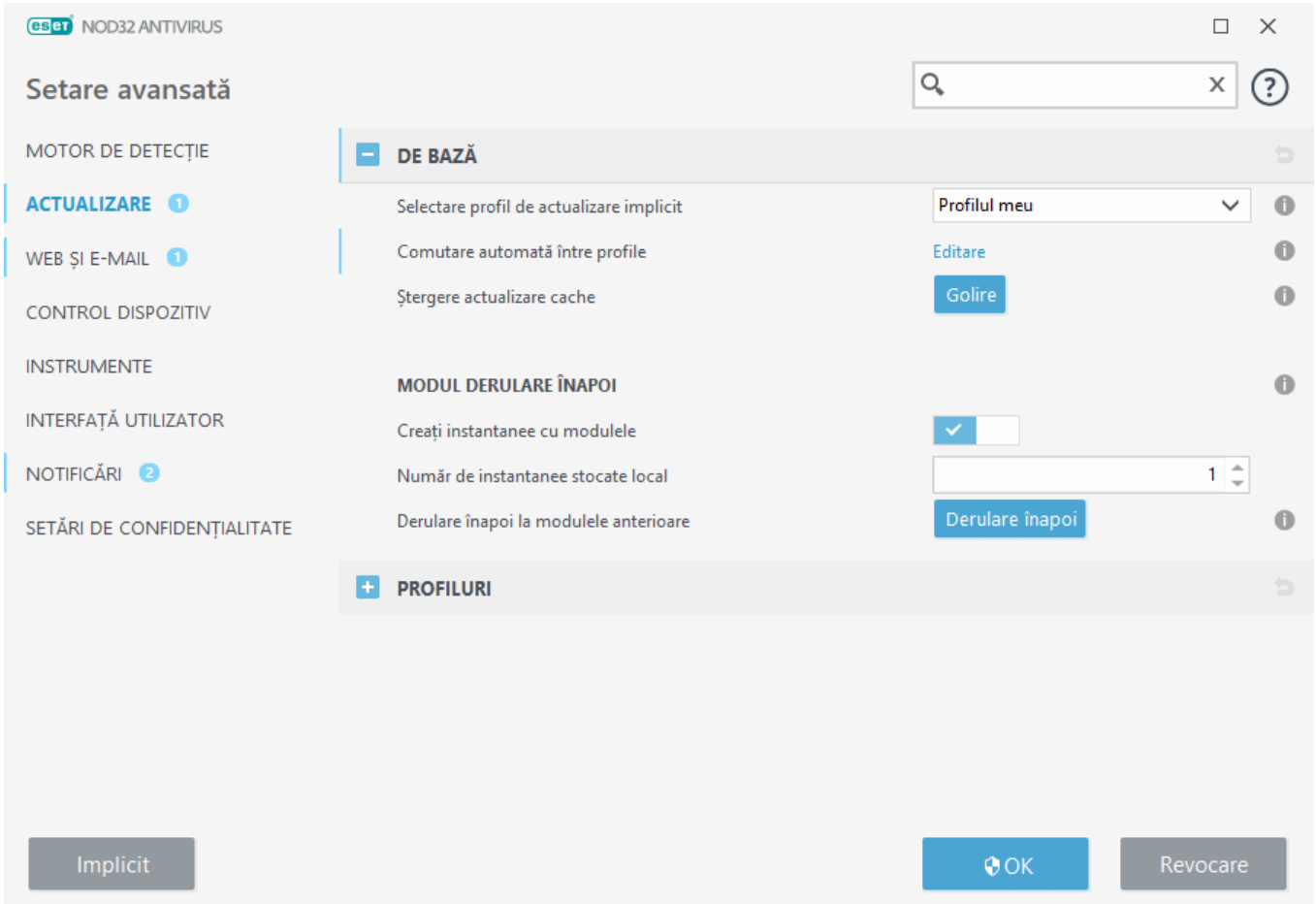
> Când se atinge numărul maxim de instantanee (de exemplu, trei), cel mai vechi instantaneu este înlocuit cu un instantaneu nou la fiecare 48 de ore. ESET NOD32 Antivirus derulează înapoi motorul de detecție și versiunile de actualizări pentru modulele de program la cel mai vechi instantaneu.

Dacă faceți clic pe **Derulare înapoi** (**Setări avansate** (F5) > **Actualizare** > **De bază**), trebuie să selectați un interval de timp din meniul vertical **Durată**, care reprezintă perioada de timp cât vor fi trecute în pauză actualizările motorului de detecție și ale modulelor de program.



Selectați **Până la revocare** pentru a amâna pe termen nedefinit actualizările regulate până când restabiliți manual funcția de actualizare. Deoarece reprezintă un risc potențial pentru securitate, ESET nu vă recomandă să selectați această opțiune.

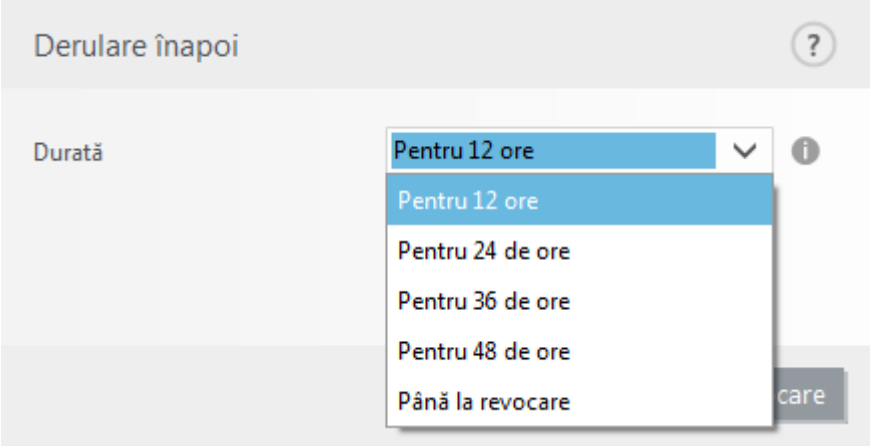
Dacă se efectuează derularea înapoi, butonul **Derulare înapoi** devine **Permitere actualizări**. Nu se va permit actualizări pentru perioada selectată în meniul vertical **Actualizări suspendate**. Versiunea motorului de detecție revine la cea mai veche disponibilă și stocată ca instantaneu în sistemul de fișiere al computerului local.



Să presupunem că 22700 este cel mai recent număr de versiune a motorului de detecție, iar 22698 și 22696 sunt stocate ca instantanee ale motorului de detecție. Versiunea 22697 nu este disponibilă. În acest exemplu, computerul a fost oprit în timpul actualizării 22697 și o actualizare mai recentă a fost pusă la dispoziție înainte de descărcarea 22697. Dacă valoarea din câmpul **Număr de instantanee stocate local** este doi și faceți clic pe **Derulare înapoi**, motorul de detecție (inclusiv modulele de program) este restaurat la versiunea cu numărul 22696. Acest proces poate dura ceva timp. Verificați dacă versiunea motorului de detecție a scăzut în ecranul Actualizare.

Interval de timp pentru derulare înapoi

Dacă faceți clic pe **Derulare înapoi** (**Setări avansate** (F5) > **Actualizare** > **De bază**), trebuie să selectați un interval de timp din meniul vertical **Durată**, care reprezintă perioada de timp cât vor fi trecute în pauză actualizările motorului de detecție și ale modulelor de program.



Selectați **Până la revocare** pentru a amâna pe termen nedefinit actualizările regulate până când restabiliți manual funcția de actualizare. Deoarece reprezintă un risc potențial pentru securitate, ESET nu vă recomandă să selectați această opțiune.

Actualizări produs

Secțiunea **Actualizări produs** vă permite să instalați în mod automat actualizări noi de funcționalități, atunci când ele sunt disponibile.

Actualizările funcționalităților aplicației aduc funcționalități noi sau le modifică pe cele care există deja din versiunile anterioare. Se pot efectua automat, fără intervenția utilizatorului, sau puteți alege să primiți o notificare. După ce s-a instalat o actualizare a funcționalității aplicației, poate fi necesară o repornire a computerului.

Actualizări ale funcționalităților aplicației – Când această opțiune este activată, actualizările funcționalităților aplicației se vor efectua automat.

Opțiuni de conectare

Pentru a accesa opțiunile de setare a serverului proxy pentru un anumit profil de actualizare, faceți clic pe **Actualizare** din structura de tip arbore **Setări avansate** (F5) și apoi faceți clic pe **Profiluri** > **Actualizări** > **Opțiuni de conectare**. Faceți clic pe meniul vertical **Mod proxy** și selectați una dintre următoarele trei opțiuni:

- Nu utiliza server proxy
- Conectare printr-un server proxy
- Utilizează setări globale server proxy

Selectați opțiunea **Utilizare setări globale server proxy** pentru a utiliza opțiunile de configurare a serverului proxy deja specificate în ramura **Instrumente** > **Server proxy** din structura arborelui de configurare avansată.

Selectați **Nu utiliza server proxy** pentru a specifica faptul că nu se utilizează niciun server proxy pentru a actualiza ESET NOD32 Antivirus.

Opțiunea **Conectare printr-un server proxy** se selectează dacă:

- Un alt server proxy față de cel definit în **Instrumente** > **Server proxy** este utilizat pentru a actualiza ESET NOD32 Antivirus. În această configurație, informațiile pentru noul server proxy trebuie specificate în adresa pentru **Server proxy**, **Portul** de comunicare (3128 implicit) și **Nume utilizator** și **Parolă** pentru serverul proxy, dacă sunt necesare.

- Setările serverului proxy nu sunt setate global, dar ESET NOD32 Antivirus se va conecta la un server proxy pentru actualizări.
- Computerul este conectat la Internet printr-un server proxy. Setările sunt preluate din Internet Explorer în timpul instalării programului, dar dacă sunt modificate (de exemplu, dacă schimbați furnizorul de servicii Internet), verificați dacă setările de server proxy listate în această fereastră sunt corecte. În caz contrar, programul nu se va putea conecta la serverele de actualizare.

Setarea implicită pentru serverul proxy este **Utilizează setări globale server proxy**.

Utilizați conexiunea directă dacă serverul proxy nu este disponibil – serverul proxy va fi ocolit în timpul actualizării dacă nu se poate stabili conexiunea cu acesta.

> Câmpurile **Nume utilizator** și **Parolă** din această secțiune sunt specifice serverului proxy. Completați aceste câmpuri doar dacă numele de utilizator și parola sunt necesare pentru a accesa serverul proxy. Aceste câmpuri trebuie completate numai dacă știți că aveți nevoie de o parolă pentru acces la internet printr-un server proxy.

Cum se creează sarcini de actualizare

Actualizările pot fi declanșate manual cu clic pe **Căutare actualizări** din fereastra principală afișată după ce ați făcut clic pe **Actualizare** în meniul principal.

De asemenea, actualizările pot fi executate ca sarcini planificate. Pentru a configura o sarcină planificată, faceți clic pe **Instrumente** > **Orar**. În mod implicit, în ESET NOD32 Antivirus sunt activate următoarele sarcini:

- **Actualizare automată periodică**
- **Actualizare automată după conexiune dial-up**
- **Actualizare automată după conectare utilizator**

Fiecare sarcină de actualizare poate fi modificată astfel încât să satisfacă cerințele dvs. În afară de sarcinile de

actualizare implicite, puteți crea sarcini de actualizare noi cu o configurație definită de utilizator. Pentru detalii suplimentare despre crearea și configurarea sarcinilor de actualizare, consultați secțiunea Orar.

Fereastră de dialog – Este necesară repornirea

Este necesară o repornire a computerului după actualizarea ESET NOD32 Antivirus la o nouă versiune. Publicăm noi versiuni de ESET NOD32 Antivirus pentru a implementa îmbunătățiri sau a remedia probleme pe care actualizările automate ale modulelor de program nu le pot rezolva.

Noua versiune de ESET NOD32 Antivirus poate fi instalată automat, pe baza setărilor de actualizare a programului, sau manual, descărcând și instalând o versiune mai nouă față de cea anterioară.

Faceți clic pe **Repornire acum** pentru a reporni computerul. Dacă intenționați să reporniți computerul mai târziu, faceți clic pe **Amintește-mi mai târziu**. Ulterior, puteți reporni manual computerul din secțiunea **Acasă**, în fereastra principală a programului.

Instrumente

Meniul **Instrumente** cuprinde module care ajută la simplificarea administrării programului și oferă opțiuni suplimentare pentru utilizatorii avansați.

Consultați Instrumente din ESET NOD32 Antivirus pentru mai multe informații.

Instrumente în ESET NOD32 Antivirus

Meniul **Instrumente** cuprinde module care ajută la simplificarea administrării programului și oferă opțiuni suplimentare pentru utilizatorii avansați.

Acest meniu cuprinde următoarele instrumente:

 Fișiere log

 Raport de securitate

 Procese care se execută (dacă ESET LiveGrid® s-a activat în ESET NOD32 Antivirus)

 ESET SysInspector

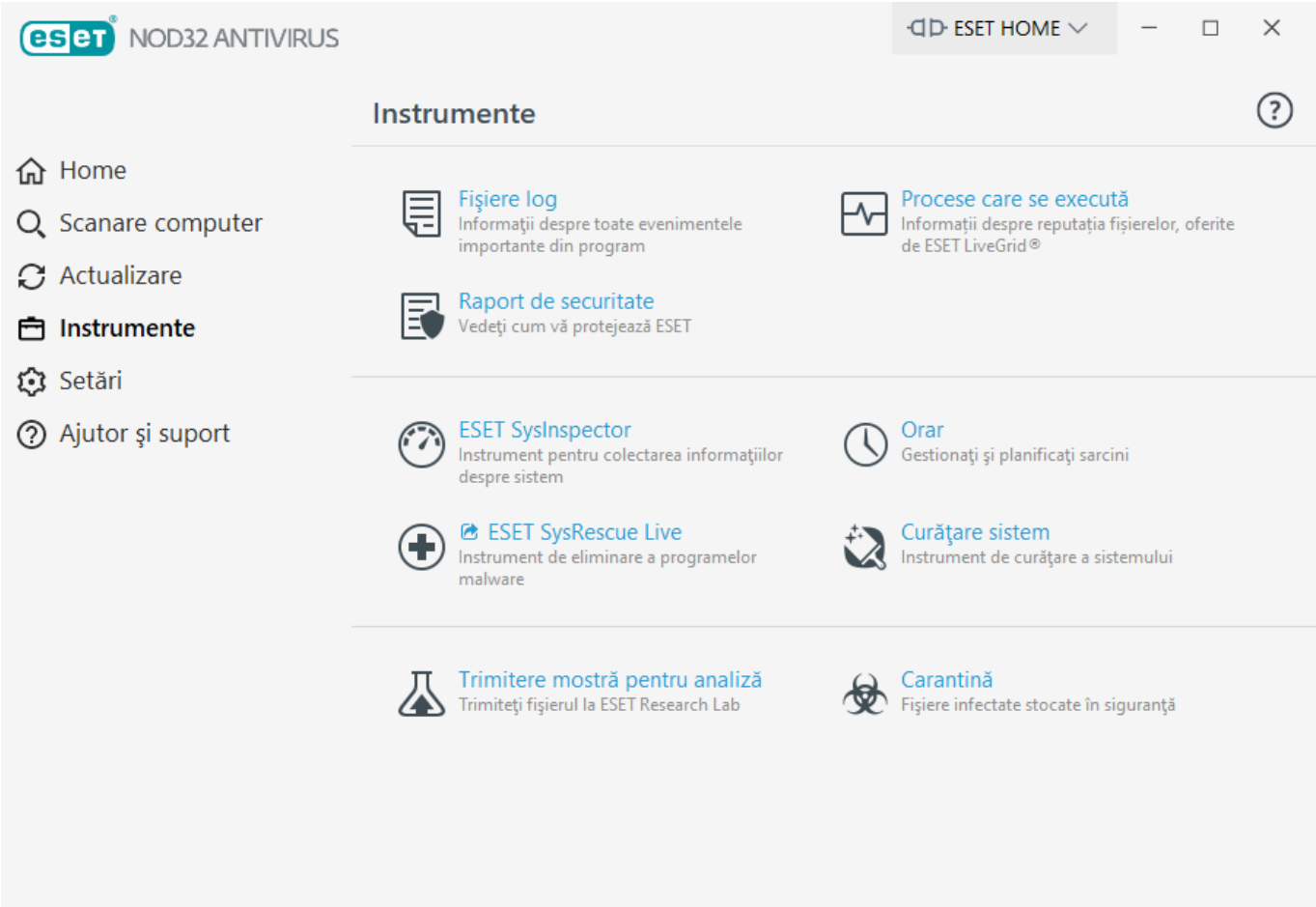
 ESET SysRescue Live – Vă redirecționează către pagina ESET SysRescue Live, unde puteți descărca imaginea CD/DVD pentru ESET SysRescue Live .iso.

 Orar

 Curățare sistem – vă ajută să restaurați computerul la o stare utilizabilă după curățarea amenințării.

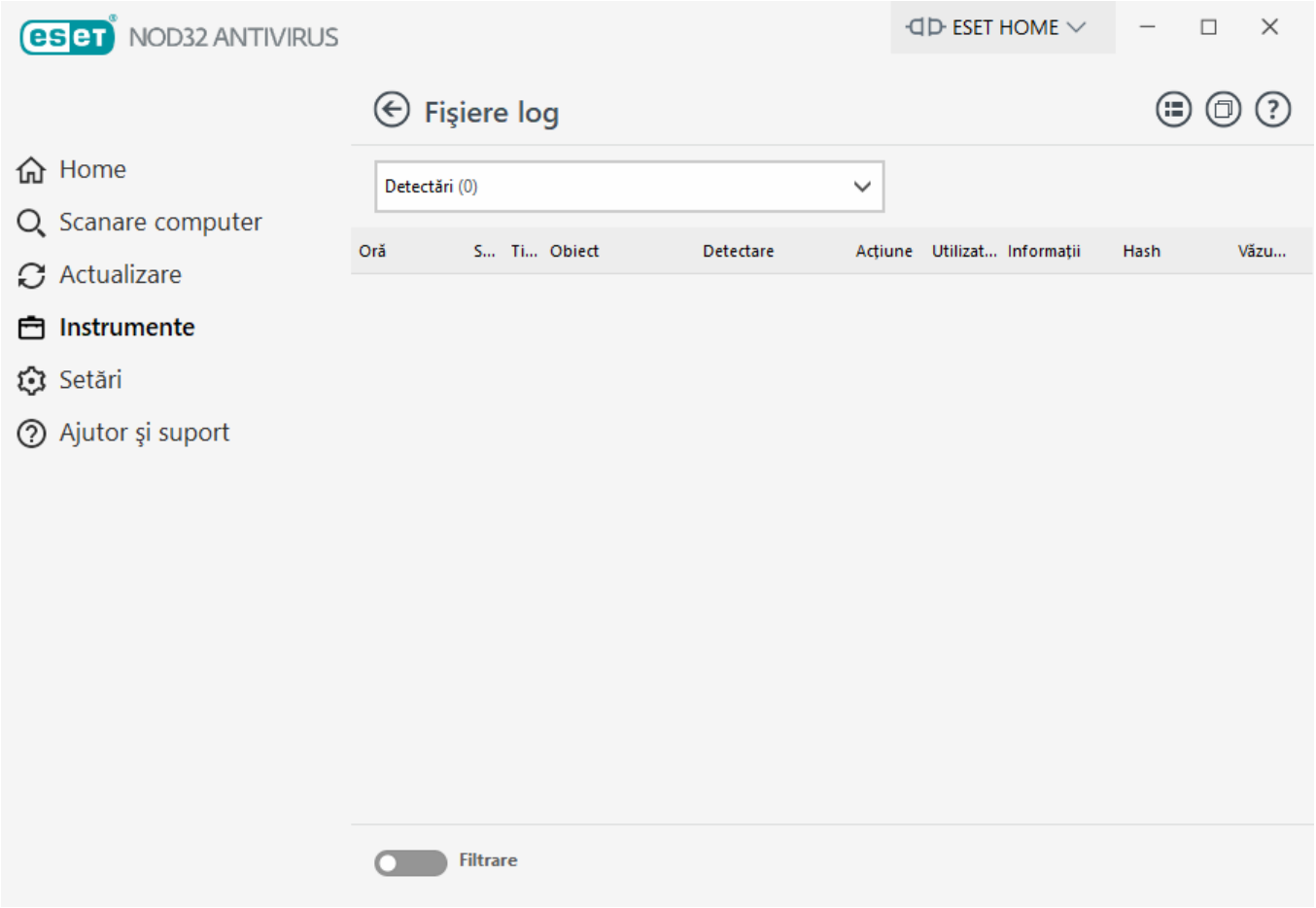
Trimitere mostră pentru analiză – Vă permite să trimiteți Laboratorului de cercetare ESET spre analiză un fișier suspect (este posibil ca această opțiune să nu fie disponibil, în funcție de configurația dvs. ESET LiveGrid®.

Carantină



Fișiere log

Fișierele log conțin informații despre evenimentele de program importante care au avut loc și oferă o prezentare generală a amenințărilor detectate. Scrierea în log reprezintă o parte esențială pentru analiza sistemului, detectarea amenințărilor și pentru depanare. Scrierea în log se efectuează activ în fundal, fără interacțiunea utilizatorului. Informațiile se înregistrează în funcție de setările curente de scriere în log. Se pot vizualiza mesajele text și fișierele log direct din ESET NOD32 Antivirus și se pot arhiva fișiere log.



Fișierele log se pot accesa din fereastra principală a meniului făcând clic pe **Instrumente** > **Fișiere log**. Selectați tipul de log dorit în meniul vertical **Log**. Sunt disponibile următoarele loguri:

- **Detectări** – Acest log oferă informații detaliate despre detectările și infiltrările detectate de ESET NOD32 Antivirus. Informațiile din log includ momentul detectării, tipul de scaner, tipul de obiect, numele detectării, locația, acțiunea efectuată, numele utilizatorului conectat în momentul în care s-a detectat infiltrarea, codul hash și prima apariție. Faceți clic dublu pe orice înregistrare din log pentru a afișa detaliile acesteia într-o fereastră separată. Infiltrările necurățate sunt marcate întotdeauna cu text roșu pe fondal roșu deschis. Aplicațiile potențial nesigure necurățate sunt marcate cu text galben pe fundal alb.

- **Evenimente** – Toate acțiunile importante efectuate de ESET NOD32 Antivirus sunt înregistrare în logul evenimentelor. Logul evenimentelor conține informații despre evenimente și erori care au apărut în program. Acesta este conceput pentru administratorii de sistem și utilizatori pentru a rezolva problemele. Adesea, informațiile găsite aici vă pot ajuta la găsirea unei probleme a programului.

- **Scanare computer** – În această fereastră se afișează rezultatele tuturor scanărilor anterioare. Fiecare rând corespunde unei singure scanarea de computer. Faceți dublu clic pe orice înregistrare pentru a vizualiza detaliile scanării selectate.

- **HIPS** – Conține înregistrări ale regulilor HIPS specifice care au fost marcate pentru înregistrare. Protocolul prezintă aplicația care a declanșat operațiunea, rezultatul (dacă regula a fost permisă sau interzisă) și numele regulii.

- **Site-uri Web filtrate** – Această listă este utilă dacă doriți să vizualizați o listă cu site-urile Web blocate de componenta Protecție acces Web. Fiecare log include ora, adresa URL, utilizatorul și aplicația care a creat o conexiune la un anumit site Web.

- **Control dispozitiv** – Conține înregistrări despre unitățile media portabile sau dispozitivele conectate la computer. În log se vor înregistra numai dispozitivele cu respectivele reguli asociate componentei Control dispozitiv. Dacă regula nu se aplică unui dispozitiv conectat, nu se va crea o înregistrare în log pentru respectivul dispozitiv conectat. De asemenea, aici puteți vedea detalii precum tipul dispozitivului, numărul de serie, numele distribuitorului și dimensiunea suportului (dacă este disponibilă).

Selectați conținutul oricărui log și apăsați pe **CTRL + C** pentru a-l copia în clipboard. Țineți apăsate tastele **CTRL** sau **SHIFT** pentru a selecta mai multe intrări.

Faceți clic pe **Filtrare** pentru a se deschide fereastra Filtrare log, unde puteți defini criteriile de filtrare.

Faceți clic dreapta pe o anumită înregistrare pentru a deschide meniul contextual. În meniul contextual sunt disponibile opțiunile următoare:

- **Afișare** – Arată informații mai detaliate despre logul selectat într-o fereastră nouă.
- **Filtrare înregistrări de același tip** – După activarea acestui filtru, veți vedea numai înregistrările de același tip (diagnostice, avertismente etc).
- **Filtrare** – După ce faceți clic pe această opțiune, fereastra Filtrare Log vă va permite să definiți criterii de filtrare pentru intrări de log specifice.
- **Activare filtru** – Activează setările de filtrare.
- **Dezactivare filtru** – Golește toate setările de filtrare (conform descrierii de mai sus).
- **Copiere/Copiere tot** – Copiază informațiile despre înregistrările selectate în fereastră.
- **Ștergere/Ștergere tot** – Șterge înregistrările selectate sau toate înregistrările afișate. Această acțiune necesită privilegii de administrator.
- **ExportExportare toate** – Exportă informații despre înregistrările selectate sau despre toate înregistrările, în format XML.
- **Găsire/Găsire următor/Găsire anterior** – După ce faceți clic pe această opțiune, puteți defini criterii de filtrare pentru intrări specifice folosind fereastra Filtrare Log.
- **Descriere detectare** – Deschide Enciclopedia amenințărilor ESET, care conține informații detaliate despre pericolele și simptomele infiltrării înregistrate.
- **Creare excludere** – Creați o excludere nouă de la detectare folosind un expert (opțiunea nu este disponibilă pentru detectările de malware).

Filtrare Log

Faceți clic pe **Filtrare** în **Instrumente** > **Fișiere log** pentru a defini criteriile de filtrare.

Caracteristica de filtrare a fișierelor log vă va ajuta să găsiți informațiile pe care le căutați, în special atunci când există multe înregistrări. Aceasta vă permite să restrângeți numărul de înregistrări log returnate atunci când, de exemplu, căutați un anumit tip de eveniment, o anumită stare sau o anumită perioadă. Puteți filtra înregistrările log specificând anumite opțiuni de căutare și numai înregistrările relevante (potrivit opțiunilor de căutare) vor fi afișate în fereastra Fișiere log.

Tastați cuvântul cheie pe care îl căutați în câmpul **Găsire text**. Utilizați meniul vertical **Căutare în coloane** pentru a vă rafina căutarea. Alegeți una sau mai multe înregistrări în meniul vertical **Tipuri de log pentru înregistrare**. Definiți **Perioada de timp** pentru care doriți afișarea rezultatelor. Puteți folosi și alte opțiuni de căutare, cum ar fi **Potrivire numai cuvinte întregi** sau **Diferențiere litere mari și mici**.

Găsire text

Tastați un șir (un cuvânt sau o parte dintr-un cuvânt). Vor fi afișate numai înregistrările care conțin șirul respectiv. Iar alte înregistrări vor fi omise.

Căutare în coloane

Selectați ce coloane vor fi luate în calcul la căutare. Puteți verifica una sau mai multe coloane care să fie folosite pentru căutare.

Tipuri de înregistrare

Alegeți unul sau mai multe tipuri de înregistrări log în meniul vertical:

- **Diagnostic** – înregistrează informațiile necesare pentru reglajul fin al programului și toate înregistrările de mai sus.
- **Informativ** – înregistrează mesajele informative, inclusiv mesajele privind actualizarea cu succes plus toate înregistrările de mai sus.
- **Avertismente** – înregistrează erori critice și mesaje de avertisment.
- **Erori** – se vor înregistra erori precum „Eroare la descărcarea fișierului” și erorile critice.
- **Critice** – înregistrează numai erorile critice (erori la pornirea protecției antivirus

Perioadă de timp

Definiți perioada de timp pentru afișarea rezultatelor.

- **Nespecificat** (implicit) - Nu se caută în intervalul de timp, se caută în întregul log.
- **Ultima zi**
- **Ultima săptămână**
- **Ultima lună**
- **Perioadă de timp** - Puteți specifica o perioadă de timp exactă (De la: și Până la:) pentru a filtra numai înregistrările din perioada de timp specificată.

Potrivire numai cuvinte întregi

Folosiți această casetă de selectare dacă doriți să căutați cuvinte întregi, pentru rezultate mai precise.

Diferențiere litere mari și mici

Activați această opțiune dacă pentru dvs. este important să utilizați litere majuscule sau minuscule la filtrare.

După ce ați configurat opțiunile pentru filtrare/căutare, faceți clic pe **OK** pentru a afișa înregistrările log filtrate sau pe **Găsire** pentru a începe căutarea. Fișiere log sunt căutate de sus în jos, începând cu poziția curentă (înregistrarea evidențiată în prezent). Căutarea se oprește atunci când prima înregistrare care corespunde este găsită. Apăsați pe **F3** pentru a căuta următoarea înregistrare sau faceți clic dreapta și selectați **Găsire** pentru a rafina opțiunile de căutare.

Configurația de scriere în log

Configurația ESET NOD32 Antivirus de scriere în log este accesibilă în fereastra meniului principal. Faceți clic pe **Setare** > **Setări avansate** > **Instrumente** > **Fișiere log**. Secțiunea loguri este utilizată pentru a defini modul de gestionare a logurilor. Programul șterge automat logurile vechi pentru a economisi spațiu pe hard disk. Puteți specifica următoarele opțiuni pentru fișiere log:

Detalii minime la scriere în log – specifică nivelul minim de detalii pentru evenimentele de înregistrat.

- **Diagnostic** – înregistrează informațiile necesare pentru reglajul fin al programului și toate înregistrările de mai sus.
- **Informativ** – înregistrează mesajele informative, inclusiv mesajele privind actualizarea cu succes plus toate înregistrările de mai sus.
- **Avertismente** – înregistrează erori critice și mesaje de avertisment.
- **Erori** – se vor înregistra erori precum „Eroare la descărcarea fișierului” și erorile critice.
- **Critice** – înregistrează numai erorile critice (erori la pornirea protecției antivirusetc...).

Vor fi înregistrate toate conexiunile blocate atunci când selectați nivelul de detalii Diagnostic.

Înregistrările din log mai vechi decât numărul de zile specificat în câmpul **Șterge automat înregistrările mai vechi de (zile)** vor fi șterse automat.

Optimizează automat fișierele de log – dacă se selectează, fișierele log se vor defragmenta automat dacă procentajul este mai mare decât valoarea specificată în câmpul **Dacă numărul de înregistrări nefolosite depășește (%)**.

Faceți clic pe **Optimizare** pentru a începe defragmentarea fișierelor log. În timpul acestui proces se vor șterge din log toate înregistrările necompletate, îmbunătățind astfel performanța și viteza procesării logurilor. Această îmbunătățire se poate observa mai ales dacă logurile conțin un număr mare de înregistrări.

Opțiunea **Activare protocol text** permite stocarea logurilor în alt format de fișier, separat de Fișiere log:

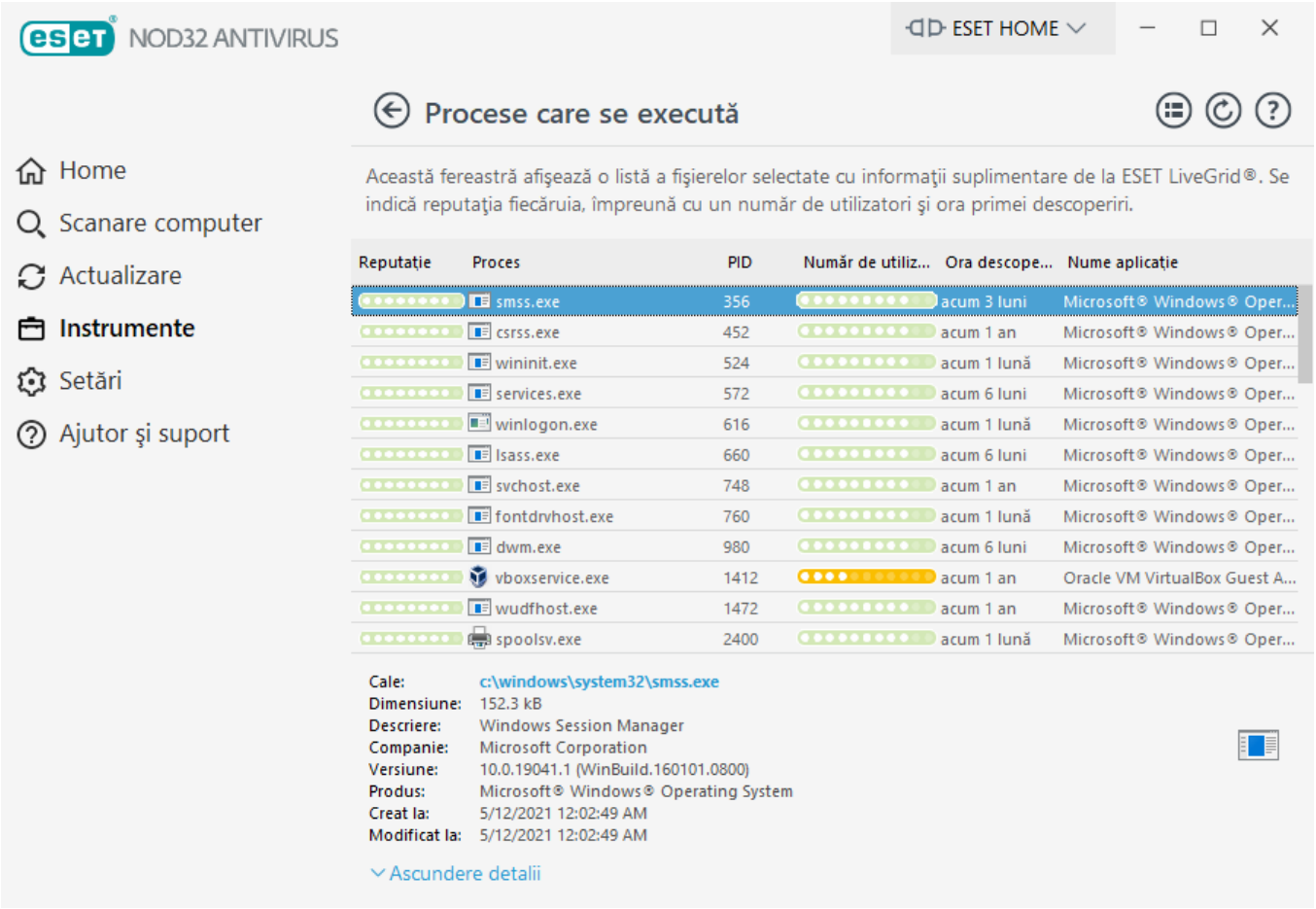
- **Director de destinație** – directorul în care vor fi stocate fișierele log (se aplică numai pentru Text/CSV). Fiecare secțiune de log are propriul său fișier cu nume de fișier predefinit (de exemplu, virlog.txt pentru secțiunea **Detectări** a fișierelor log dacă utilizați pentru stocarea logurilor formatul de fișiere cu text simplu).
- **Tip** – dacă selectați formatul de fișier **Text**, logurile vor fi stocate într-un fișier text; datele vor fi separate prin caractere de tabulare. Același lucru se aplică formatului de fișier **CSV** cu separare prin virgule. Dacă selectați **Eveniment**, logurile vor fi stocate în Windows Event Log (vizualizabil cu Event Viewer din Control Panel), nu într-un fișier.

• **Ștergere toate fișierele log** – șterge toate logurile selectate curent în meniul vertical **Tip**. Se va afișa o notificare despre ștergerea cu succes a logurilor.

Pentru a se rezolva problemele mai rapid, este posibil ca ESET să vă solicite să furnizați loguri de pe computerul dvs. ESET Log Collector facilitează colectarea informațiilor necesare. Pentru mai multe informații despre ESET Log Collector, consultați articolul din baza de cunoștințe ESET.

Procese în execuție

Procesele în execuție afișează programele sau procesele care se execută pe computer și informează ESET imediat și permanent despre infiltrările noi. ESET NOD32 Antivirus oferă informații detaliate despre procesele care se execută pentru a proteja utilizatorii cu tehnologia ESET LiveGrid®.



Reputație – În majoritatea cazurilor, ESET NOD32 Antivirus, utilizând tehnologia ESET LiveGrid®, atribuie niveluri de risc obiectelor (fișiere, procese, chei de registry etc.) utilizând o serie de reguli euristice care examinează caracteristicile tuturor obiectelor și cuantifică posibilitatea acestora de înregistrare a unor activități dăunătoare. În funcție de această euristică, se atribuie un nivel de risc obiectelor între 1 – Fin (verde) și 9 – Riscant (roșu).

Proces – Numele imaginii programului sau procesului care se execută în mod curent pe computer. De asemenea, puteți utiliza Managerul de activități din Windows pentru a vizualiza toate procesele care în execuție pe computer. Pentru a deschide aplicația Manager de activități, faceți clic dreapta pe o zonă liberă din bara de activități și apoi faceți clic pe **Manager de activități** sau apăsați pe **Ctrl**+**Shift**+**Esc** pe tastatură.

Aplicațiile cunoscute marcate drept Sigur (verde) sunt foarte sigure (în lista albă) și se vor exclude la scanare, pentru a îmbunătăți performanțele.

PID – numărul de identificare a procesului poate fi utilizat drept parametru în diverse acțiuni ale funcțiilor, cum ar fi ajustarea priorității procesului.

Număr de utilizatori – Numărul de utilizatori care utilizează o anumită aplicație. Aceste informații sunt culese de tehnologia ESET LiveGrid®.

Ora descoperirii – Perioada de timp de când tehnologia ESET LiveGrid® a descoperit aplicația.

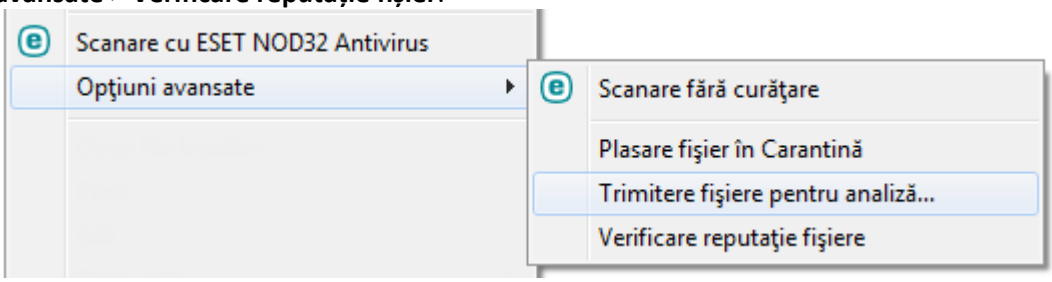
O aplicație marcată drept Necunoscut (portocaliu) nu este neapărat software rău intenționat. În general, este o aplicație nouă. Dacă nu sunteți sigur în privința fișierului, puteți remite fișierul pentru analiză la laboratorul de cercetare de la ESET. Dacă fișierul se dovedește o aplicație rău intenționată, detectarea sa va fi adăugată la una dintre actualizările ulterioare.

Nume aplicație – Numele unui program sau proces.

Faceți clic pe o aplicație pentru a afișa următoarele detalii ale aplicației respective:

- **Cale** – locația unei aplicații de pe computer.
- **Dimensiune** – dimensiunea fișierului în KO (kiloocteți) sau MO (megaocteți).
- **Descriere** – caracteristicile fișierului în funcție de descrierea de la sistemul de operare.
- **Companie** – numele vânzătorului sau al procesului aplicației.
- **Versiune** – informații de la editorul aplicației.
- **Produs** – numele aplicației și/sau denumirea comercială.
- **Creat la/Modificat la** – data și ora creării (modificării).

De asemenea, puteți verifica reputația fișierelor care nu acționează drept programe/procese în execuție. Pentru aceasta, faceți clic dreapta pe acestea într-un program de explorare a fișierelor și selectați **Opțiuni avansate** > **Verificare reputație fișier**.



Raport de securitate

Această funcție vă oferă o prezentare generală a statisticilor pentru următoarele categorii:

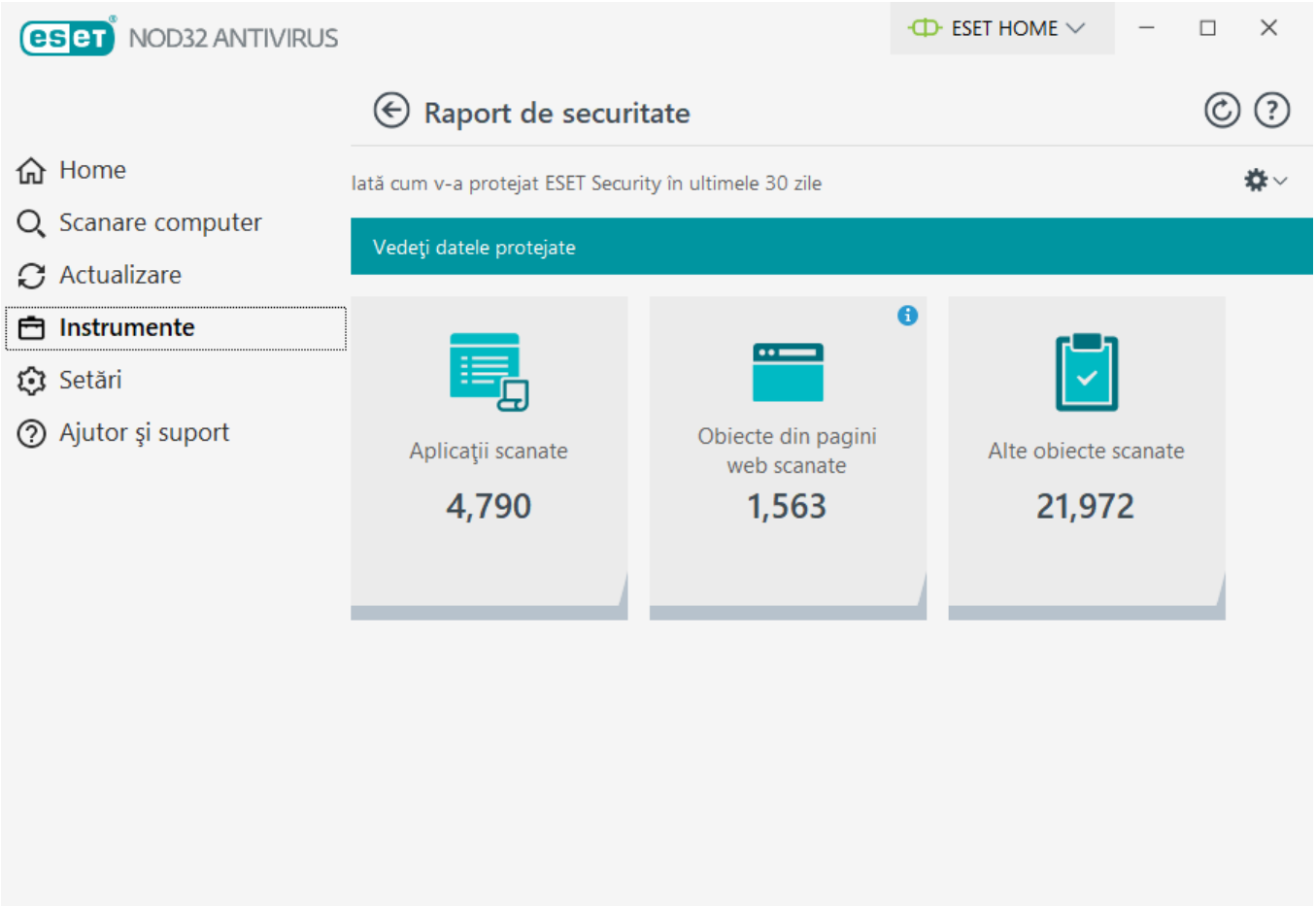
- **Pagini Web blocate** – Afișează numărul de pagini web blocate (adrese URL adăugate în lista neagră pentru PUA, phishing, router, IP sau certificat spart).
- **Obiecte e-mail infectate detectate** – Afișează numărul de obiecte e-mail infectate care au fost detectate.
- **Aplicații potențial nedorite detectate** – Afișează numărul de aplicații potențial nedorite (PUA).

- **Documente verificate** – Afișează numărul de obiecte scanate ale documentelor.
- **Aplicații scanate** – Afișează numărul de obiecte executabile scanate.
- **Alte obiecte verificate** – Afișează numărul celorlalte obiecte scanate.
- **Obiecte din pagini web scanate** – Afișează numărul de obiecte scanate ale paginilor web.
- **Obiecte e-mail scanate** – Afișează numărul de obiecte e-mail scanate.

Ordinea acestor categorii se bazează pe valoarea numerică, de la cea mai înaltă la cea mai mică. Categoriile cu valori zero nu sunt afișate. Faceți clic pe **Afișați mai** mult pentru a extinde și a afișa categorii ascunse.

După activarea funcției, aceasta nu mai este afișată drept nefuncțională în raportul de securitate.

Faceți clic pe rotița dințată din colțul din dreapta sus pentru a **activa sau a dezactiva notificările privind raportul de securitate** sau pentru a selecta dacă doriți să afișați datele pentru ultimele 30 de zile sau din momentul activării produsului. Dacă ESET NOD32 Antivirus a fost instalat de mai puțin de 30 de zile, se poate selecta doar numărul de zile de la instalare. Perioada de 30 de zile este setată în mod implicit.



Opțiunea **Resetare date** va șterge toate statisticile și va elimina datele existente pentru raportul de securitate. Această acțiune trebuie confirmată, cu excepția cazului în care debifați opțiunea **Întreabă înainte de a reinițializa statistici** în **Setări avansate** > **Notificări** > **Mesaje de confirmare** > **Mesaje de confirmare** > **Editare**.

ESET SysInspector

ESET SysInspector este o aplicație care inspectează complet computerul, adună informații detaliate despre componentele sistemului, cum ar fi driverele și aplicațiile, conexiunile de rețea sau înregistrările importante din registry, și evaluează nivelul de risc al fiecărei componente. Aceste informații pot ajuta la determinarea cauzei comportamentului suspect al sistemului, care poate fi provocat de o incompatibilitate software sau hardware ori de o infecție malware. Pentru a afla cum să utilizați ESET SysInspector, consultați Ajutorul online ESET SysInspector.

Fereastra ESET SysInspector afișează următoarele informații despre jurnale:

- **Oră** – Ora creării logului.
- **Comentariu** – Un comentariu scurt.
- **Utilizator** – Numele utilizatorului care a creat logul.
- **Stare** – Starea creării logului.

Sunt disponibile următoarele acțiuni:

- **Afișare** – Deschide jurnalul selectat în ESET SysInspector. De asemenea, puteți să faceți clic dreapta pe un fișier log și să selectați **Afișare** din meniul contextual.
- **Comparare** – compară două loguri existente.
- **Creează** – Creează un log nou. Așteptați până când se generează ESET SysInspector (cu starea **Creat**) înainte de a încerca să accesați jurnalul.
- **Ștergere** – Elimină din listă logurile selectate.

Următoarele elemente sunt disponibile din meniul contextual atunci când s-au selectat unul sau mai multe fișiere log:

- **Afișare** – Deschide logul selectat în ESET SysInspector (aceeași funcție ca și clic dreapta pe un log).
- **Comparare** – compară două loguri existente.
- **Creează** – Creează un log nou. Așteptați până când se generează ESET SysInspector (cu starea **Creat**) înainte de a încerca să accesați jurnalul.
- **Ștergere** – Elimină din listă logurile selectate.
- **Ștergere tot** – Șterge toate logurile.
- **Exportare** – Exportă logul într-un fișier .xml sau .xml arhivat. Jurnalul este exportat în C:\ProgramData\ESET\ESET Security\SysInspector.

Orar

Orarul gestionează și lansează sarcini planificate cu configurații și proprietăți predefinite.

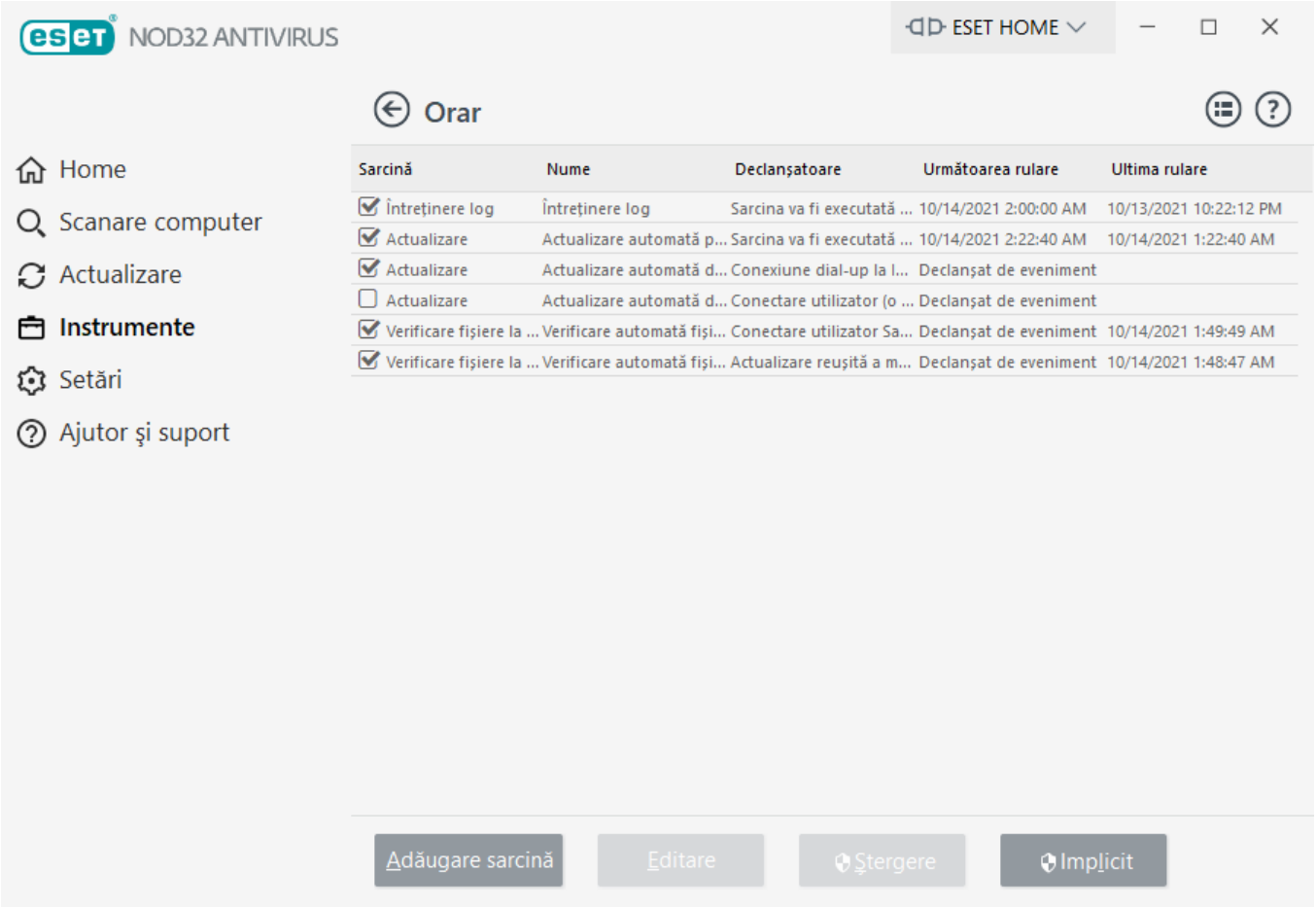
Orarul se poate accesa din fereastra principală a programului ESET NOD32 Antivirus, făcând clic pe **Instrumente** > **Orar**. **Orarul** conține o listă cu toate sarcinile programate și proprietățile de configurare, cum ar fi datele predefinite, ora și profilul de scanare utilizat.

Orarul are rolul de a programa următoarele sarcini: actualizare module, sarcină de scanare, verificare fișier la pornirea sistemului și întreținere fișiere de log. Puteți adăuga sau șterge sarcini direct din fereastra principală Orar (faceți clic pe **Adăugare sarcină** sau pe **Ștergere** în partea de jos). Puteți readuce lista sarcinilor programate la valorile implicite și puteți șterge toate modificările făcând pe **Implicit**. Faceți clic dreapta oriunde în fereastra Orar pentru a executa următoarele acțiuni: afișare informații detaliate, executare imediată sarcină, adăugare sarcină nouă și ștergere sarcină existentă. Utilizați casetele de selectare de la începutul fiecărei înregistrări pentru a activa/dezactiva sarcinile.

În mod implicit, în **Orar** se afișează următoarele sarcini programate:

- **Întreținere log**
- **Actualizare automată periodică**
- **Actualizare automată după conexiune dial-up**
- **Actualizare automată după conectare utilizator**
- **Verificare fișiere cu pornire automată** (după conectarea utilizatorului)
- **Verificare fișiere cu pornire automată** (după actualizare cu succes a motorului de detecție)

Pentru a edita configurația unei sarcini programate existente (atât implicită, cât și definită de utilizator), faceți clic dreapta pe sarcină și faceți clic pe **Editare** sau selectați sarcina pe care doriți să o modificați și faceți clic pe **Editare**.



Adăugare sarcină nouă

1. Faceți clic pe **Adăugare sarcină** în partea de jos a ferestrei.

2. Introduceți numele sarcinii.

3. Selectați sarcina dorită din meniul vertical:

   • **Rulare aplicație externă** – Programează executarea unei aplicații externe.

   • **Mentenanță log** - Fișierele log conțin și resturi din înregistrările șterse. Această sarcină optimizează regulat înregistrările din fișierele log pentru a funcționa mai eficient.

   • **Verificare fișier la pornire sistem** – Verifică fișierele cărora li se permite executarea la pornirea sistemului sau la conectare.

   • **Creați un instantaneu cu starea computerului** – Creează un instantaneu ESET SysInspector al computerului - adună informații detaliate despre componentele sistemului (de exemplu, drivere, aplicații) și evaluează nivelul de risc al fiecărei componente.

   • **Scanare computer la cerere** – se efectuează o scanare a fișierelor și a directoarelor de pe calculator.

   • **Actualizare** – planifică o sarcină Actualizare prin actualizarea modulelor.

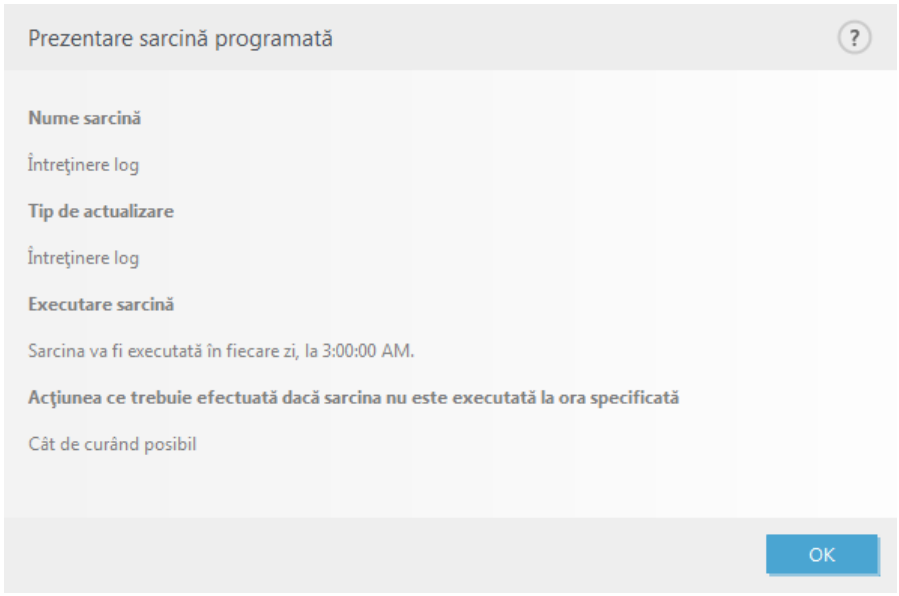
4. Faceți clic pe bara cu glisor de lângă opțiunea **Activat** pentru a activa sarcina (puteți face acest lucru ulterior bifând/debifând caseta de selectare din lista de sarcini planificate), faceți clic pe **Următorul** și selectați una dintre opțiunile de temporizare:

- **O dată** – Sarcina va fi executată la data și la ora predefinite.
- **Repetat** – Sarcina se va executa la intervalul de timp specificat.
- **Zilnic** – Sarcina se va executa repetat zilnic, la ora stabilită.
- **Săptămânal** – Sarcina se va executa în ziua și la ora selectate.
- **Declanșată de eveniment** – Sarcina se va executa la un eveniment specificat.

5. Selectați **Omitere sarcină când computerul funcționează pe baterie** pentru a minimiza utilizarea resurselor sistemului când un laptop funcționează alimentat de la baterie. Activitatea va fi executată la data și ora specificate în câmpurile **Executare sarcină**. Dacă sarcina nu s-a putut executa la ora predefinită, puteți specifica momentul când se va executa din nou:

- **La următoarea oră planificată**
- **Cât de curând posibil**
- **Imediat, dacă timpul de la ultima executare depășește (ore)** – Reprezintă timpul scurs de la prima executare omisă a sarcinii. Dacă acest timp este depășit, sarcina se va executa imediat. Setați ora folosind cadranul de mai jos.

Pentru a vizualiza sarcina planificată, faceți clic dreapta și apoi clic pe **Afișare detalii sarcină**.



Opțiuni pentru Scanare planificată

În această fereastră, puteți specifica opțiuni avansate pentru o activitate programată de scanare a computerului.

Pentru a rula o scanare fără nicio acțiune de curățare, faceți clic pe **Setări avansate** și selectați **Scanare fără curățare**. Istoricul scanării este salvat în jurnalul de scanare.

Dacă selectați **Ignorare excluderi**, fișierele cu extensiile excluse anterior de la scanare vor fi scanate, fără excepție.

Puteți seta o acțiune de efectuat automat după terminarea unei scanări utilizând meniul vertical:

- **Nicio acțiune** – nu se efectuează nicio acțiune după terminarea unei scanări.
- **Închidere** – computerul se închide după terminarea unei scanări.
- **Repornire** – se închid toate programele deschise și se repornește computerul după terminarea unei scanări.
- **Repornire dacă este necesar** - computerul repornește numai dacă acest lucru este necesar pentru a finaliza curățarea amenințărilor detectate.
- **Repornire forțată** – Forțează închiderea tuturor programelor deschise, fără a aștepta interacțiunea cu utilizatorul, și repornește computerul după terminarea unei scanări.
- **Repornire forțată, dacă este necesară** - computerul repornește numai dacă acest lucru este necesar pentru a finaliza curățarea amenințărilor detectate.
- **Repaus** – se salvează sesiunea dvs. și se plasează computerul într-o stare cu alimentare redusă pentru a se putea relua rapid lucrul.
- **Hibernare** – se ia tot ce se execută în memoria RAM și se mută într-un fișier special de pe unitatea de stocare fixă. Computerul se închide, însă, la următoarea pornire, va reveni în starea sa anterioară.

Acțiunile **Veghe** sau **Hibernare** sunt disponibile, în funcție de setările pentru „Alimentare și repaus” ale sistemului de operare sau de funcționalitățile computerului/laptopului. Rețineți că un computer aflat în starea de veghe este în continuare în funcțiune. Computerul continuă să execute funcții de bază și să utilizeze electricitate atunci când funcționează alimentat de la baterie. Pentru a menține durata de viață a bateriei, de exemplu, atunci când părăsiți biroul, vă recomandăm să utilizați opțiunea Hibernare.

Selectați **Scanarea nu poate fi revocată** pentru ca utilizatorii fără privilegii să nu poată opri acțiunile efectuate după scanare.

Selectați opțiunea **Utilizatorul poate întrerupe scanarea timp de (min)** dacă doriți să permiteți utilizatorilor cu drepturi limitate să pună în pauză scanarea computerului pentru o perioadă de timp specificată.

Consultați și Progres scanare.

Prezentare sarcină programată

Această fereastră de dialog afișează informații detaliate despre sarcina planificată selectată atunci când faceți dublu clic pe o sarcină particularizată sau faceți clic dreapta pe o sarcină Orar particularizată și faceți clic pe **Afișare detalii sarcină**.

Detalii sarcină

Tastați **Nume sarcină**, selectați una dintre opțiunile pentru **Tip de activitate**, apoi faceți clic pe **Următorul**:

- **Rulare aplicație externă** – Programează executarea unei aplicații externe.
- **Mentenanță log** - Fișierele log conțin și resturi din înregistrările șterse. Această sarcină optimizează regulat înregistrările din fișierele log pentru a funcționa mai eficient.

- **Verificare fișier la pornire sistem** – Verifică fișierele cărora li se permite executarea la pornirea sistemului sau la conectare.

- **Creați un instantaneu cu starea computerului** – Creează un instantaneu ESET SysInspector al computerului - adună informații detaliate despre componentele sistemului (de exemplu, drivere, aplicații) și evaluează nivelul de risc al fiecărei componente.

- **Scanare computer la cerere** – se efectuează o scanare a fișierelor și a directoarelor de pe calculator.

- **Actualizare** – planifică o sarcină Actualizare prin actualizarea modulelor.

Program sarcină

Sarcina se va executa în mod repetat la intervalul de timp specificat. Selectați una dintre opțiunile de temporizare:

- **O dată** – sarcina va fi executată o singură dată, la data și la ora predefinite.

- **Repetat** – sarcina se va executa la intervalul specificat (în ore).

- **Zilnic** – sarcina se va executa zilnic, la ora stabilită.

- **Săptămânal** – sarcina se va executa o dată sau de mai multe ori pe săptămână, în zilele și la orele selectate.

- **Declanșată de eveniment** – sarcina se va executa după un eveniment specificat.

Omitere sarcină când computerul funcționează pe baterie – o sarcină nu va porni atunci când computerul dvs. funcționează alimentat de la baterie la momentul când ar trebui să se execute sarcina. Acest lucru se aplică și pentru computerele care funcționează pe UPS.

Program sarcină – O dată

Executare sarcină – sarcina specificată va fi executată numai o singură dată la data și ora specificate.

Program sarcină – Zilnic

Sarcina se va executa zilnic, la ora stabilită.

Program sarcină – Săptămânal

Sarcina va rula în mod repetat în fiecare săptămână, în zilele și la orele selectate.

Program sarcină – Declanșat de eveniment

Sarcina va fi declanșată de unul din următoarele evenimente:

- **La fiecare pornire a computerului**

- **Zilnic, la prima pornire a computerului**
- **Conexiune dial-up la Internet/VPN**
- **Actualizare reușită a modulelor**
- **Actualizare reușită a produsului**
- **Conectare utilizator**
- **Detectare amenințare**

La programarea unei sarcini declanșate de un eveniment, puteți specifica intervalul minim între două finalizări ale sarcinii. De exemplu, în cazul în care vă conectați la computer de câteva ori pe zi, alegeți 24 de ore pentru executarea sarcinii numai la prima conectare din zi și apoi pentru ziua următoare.

Sarcină omisă

O sarcină poate fi omisă în cazul în care computerul funcționează pe baterie sau este oprit. Selectați când trebuie executată sarcina omisă cu una dintre aceste opțiuni, apoi faceți clic pe **Următorul**:

- **La următoarea oră planificată** – Sarcina se va executa dacă computerul este pornit la următoarea oră planificată.
- **Cât mai curând posibil** – Sarcina se va executa atunci când computerul este pornit.
- **Imediat, dacă timpul de la ultima rulare programată depășește (ore)** – Reprezintă timpul scurs de la prima executare omisă a sarcinii. Dacă acest timp este depășit, sarcina se va executa imediat.

Imediat, dacă timpul de la ultima rulare programată depășește (ore) – exemple

O sarcină drept exemplu este setată să ruleze în mod repetat la fiecare oră. Opțiunea **Imediat, dacă timpul de la ultima rulare programată depășește (ore)** este selectată și timpul depășit este setat la două ore. Sarcina se execută la ora 13:00, iar când este terminată, computerul intră în starea de veghe:

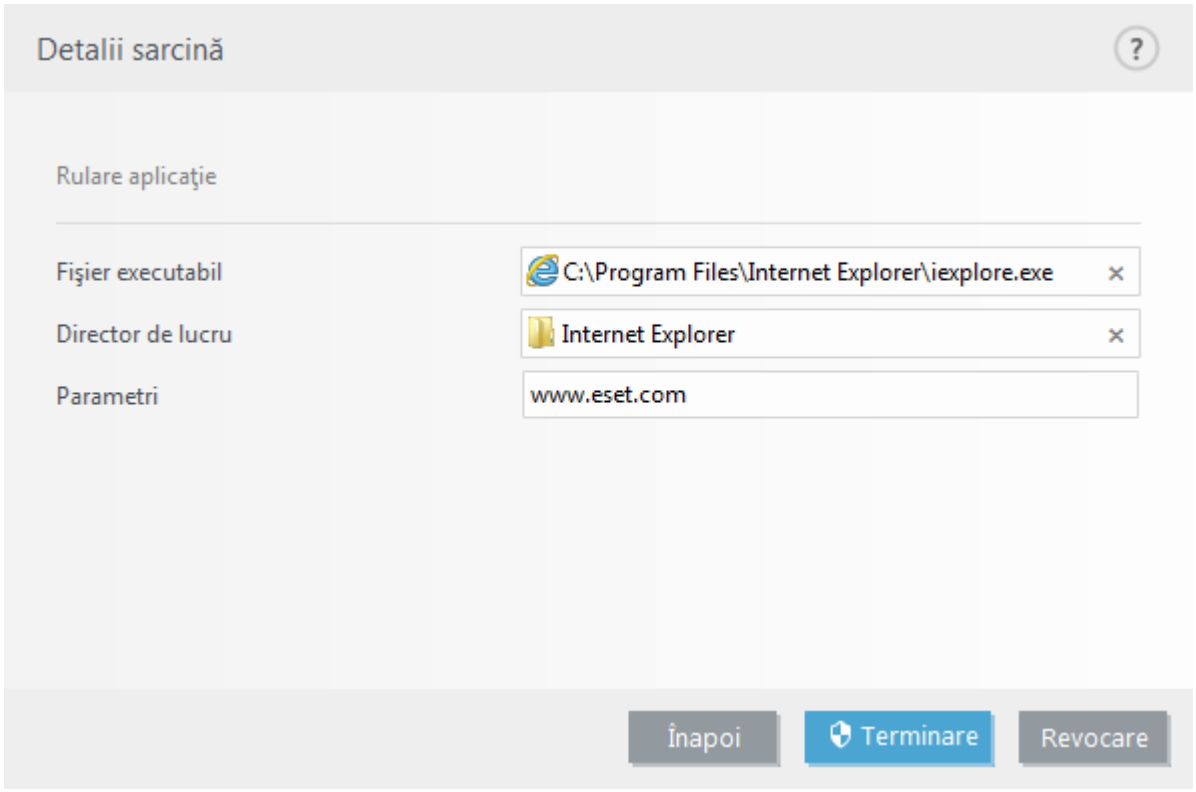
- Computerul se trezește la ora 15:30. Prima executare omisă a sarcinii a fost la ora 14:00. Au trecut doar 1,5 ore de la ora 14:00, astfel că sarcina se va executa la ora 16:00.
- Computerul se trezește la ora 16:30. Prima executare omisă a sarcinii a fost la ora 14:00. Au trecut două ore și jumătate de la ora 14:00, astfel că sarcina se va executa imediat.

Detalii activitate – Actualizare

Dacă doriți să actualizați programul de la două servere de actualizare, trebuie să creați două profile de actualizare diferite. Dacă primul nu reușește să descarce fișierele de actualizare, programul trece automat la cel alternativ. Acest lucru este adecvat, de exemplu, pentru notebook-uri care, în general, se actualizează de la un server de actualizare din rețeaua locală, dar deținătorii acestora se conectează adesea la Internet utilizând alte rețele. Deci, dacă primul profil nu reușește, al doilea va descărca automat fișierele de actualizare de la serverele de actualizare ESET.

Detalii activitate – Rulare aplicație

Această sarcină programează executarea unei aplicații externe.



Fișier executabil – Alegeți un fișier executabil din arborele directoarelor, faceți clic pe opțiunea **...** sau introduceți manual calea.

Director de lucru – Definește directorul de lucru al aplicației externe. Toate fișierele temporare ale **Fișierului executabil** se vor crea în acest director.

Parametri – Parametrii linie de comandă pentru aplicație (opțional).

Faceți clic pe **Terminare** pentru a aplica sarcina.

Curățare sistem

Curățare sistem este un instrument care vă ajută să restaurați computerul la o stare utilizabilă după curățarea amenințării. Programele malware pot dezactiva utilitare precum Editor de registry, Manager de activități sau Actualizări Windows. Instrumentul Curățare sistem restabilește valorile implicite pentru sistemul în cauză, cu un singur clic.

Instrumentul Curățare sistem raportează problemele pentru cinci categorii de setări:

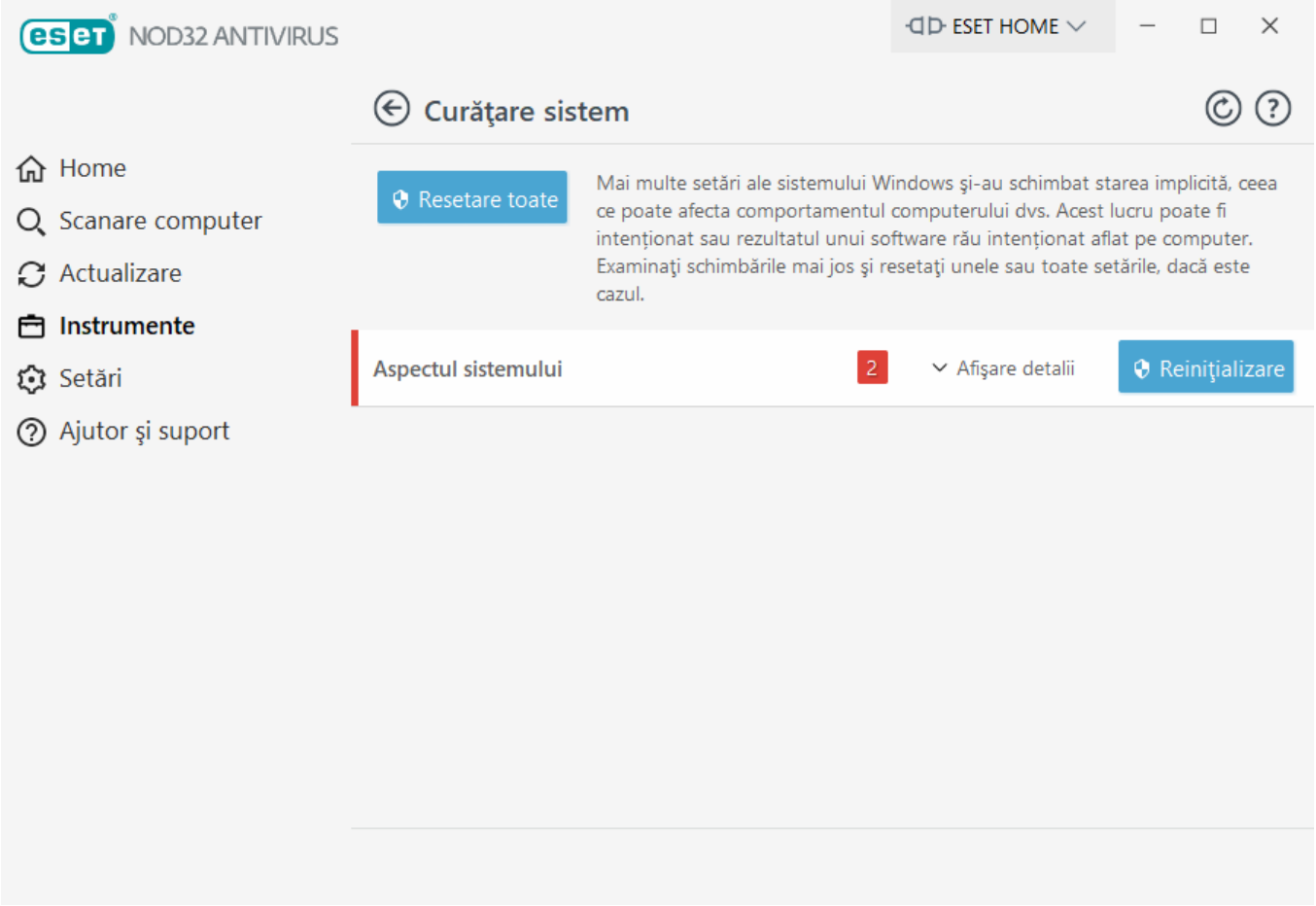
- **Setări de securitate**: modificări ale setărilor care pot crește vulnerabilitatea computerului dvs., cum ar fi Actualizările Windows
- **Setări de sistem**: modificări ale setărilor de sistem care pot genera o schimbare a comportamentului computerului dvs., cum ar fi asocierile de fișiere

- **Aspect sistem**: setări care schimbă modul în care arată sistemul, cum ar fi tapetul desktopului
- **Caracteristici dezactivate**: caracteristici și aplicații importante care pot fi dezactivate
- **Restaurarea sistemului Windows**: setări pentru caracteristica de restaurare a sistemului Windows, care vă permite să readuceți sistemul la o stare anterioară

Curățarea sistemului poate fi solicitată:

- atunci când este găsită o amenințare
- atunci când un utilizator face clic pe **Resetare**

Puteți să examinați modificările și, dacă este cazul, să resetați setări.



Numai un utilizator cu drepturi de administrator poate efectua acțiuni în instrumentul Curățare sistem.

ESET SysRescue Live

ESET SysRescue Live este un utilitar gratuit care vă permite să creați un CD/DVD sau o unitate USB de încărcare de urgență. Puteți să încărcați un computer infectat de pe mediul de încărcare de urgență pentru a scana după malware și a curăța fișierele infectate.

Principalul avantaj al utilitarului ESET SysRescue Live constă în faptul că se execută independent de sistemul de operare gazdă, dar are acces direct la disc și la sistemul de fișiere. Astfel este posibilă eliminarea unor amenințări care, în condiții normale de funcționare, nu ar putea fi șterse (de exemplu, atunci când sistemul de operare se

execută etc.).

- Ajutor online pentru ESET SysRescue Live

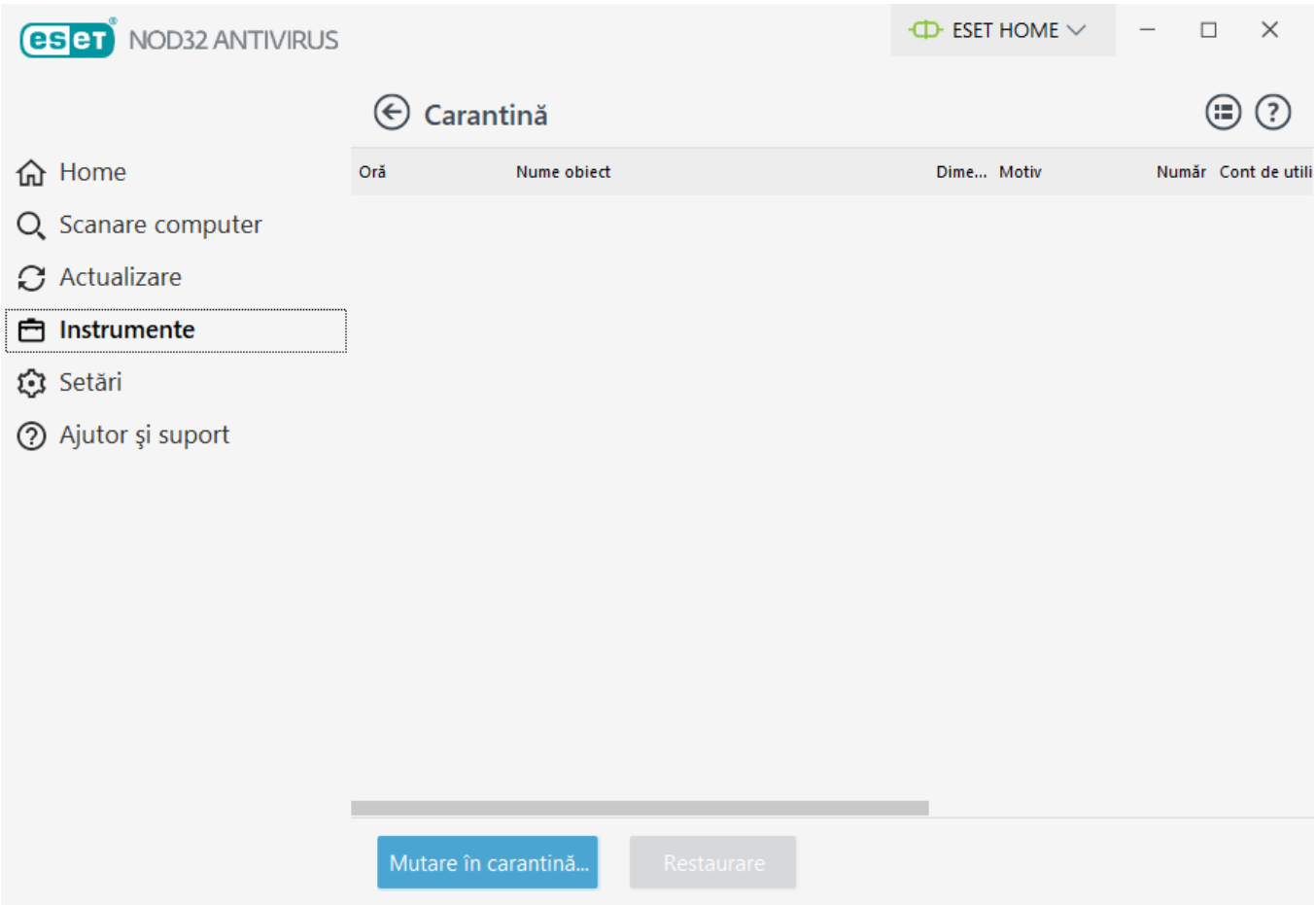
Carantină

Funcția principală a carantinei este stocarea în siguranță a obiectelor raportate (cum ar fi malware, fișiere infectate sau aplicații potențial nedorite).

Puteți accesa Carantina din fereastra principală a programului ESET NOD32 Antivirus, făcând clic pe **Instrumente** > **Carantină**.

Fișierele stocate în folderul Carantină pot fi vizualizate într-un tabel care afișează:

- data și ora introducerii în carantină;
- calea către locația inițială a fișierului;
- dimensiunea fișierului în octeți;
- motiv (de exemplu, obiect adăugat de utilizator),
- și un număr de detectări (de exemplu, detectări dublate ale aceluiași fișier sau dacă este vorba despre o arhivă care conține mai multe infiltrări).



Plasare fișiere în carantină

ESET NOD32 Antivirus plasează automat în carantină fișierele șterse (dacă nu ați revocat această opțiune în fereastra de alertă).

Și alte fișiere ar trebui să fie plasate în carantină atunci când:

a.nu pot fi curățate,

b.nu este sigur sau recomandabil să le ștergeți,

c.sunt detectate în mod fals de către ESET NOD32 Antivirus

d.sau dacă un fișier se comportă suspect, dar nu este detectat de scaner.

Pentru a plasa în carantină un fișier, aveți mai multe opțiuni:

a.Utilizați funcția de glisare și fixare pentru a plasa manual un fișier în carantină, deplasând indicatorul mouse-ului în zona marcată, ținând apăsat și apoi eliberând butonul mouse-ului. După aceea, aplicația este mutată în fundal.

b.Faceți clic dreapta pe fișier > faceți clic pe **Opțiuni avansate** > **Plasare fişier în Carantină**.

c.Faceți clic pe **Mutare în carantină** în fereastra **Carantină**.

d.Meniul contextual poate fi folosit și în acest scop; faceți clic dreapta în fereastra **Carantină** și selectați **Carantină**.

Restaurare din Carantină

Fișierele aflate în carantină pot fi și restaurate în locația lor inițială:

• Utilizați în acest scop caracteristica **Restaurare**, disponibilă în meniul contextual atunci când faceți dreapta pe un anumit fișier din Carantină.

• Dacă un fișier este marcat ca o aplicație potențial nedorită, opțiunea **Restaurare și excludere de la scanare** este activată. Consultați și Excluderi.

• Meniul contextual oferă și o opțiune **Restaurare la**, care vă permite să restaurați un fișier într-o altă locație decât cea din care a fost șters.

• Funcționalitatea de restaurare nu este disponibilă în unele cazuri, de exemplu, pentru fișierele amplasate pe o partiție de rețea doar în citire.

Ștergerea din Carantină

Faceți clic dreapta pe un anumit element și selectați **Ștergere din carantină** sau selectați elementul pe care doriți să-l ștergeți și apăsați pe tasta **Delete** de pe tastatură. De asemenea, puteți să selectați mai multe elemente și să le ștergeți împreună. Elementele șterse vor fi eliminate permanent de pe dispozitiv și din carantină.

Trimiterea unui fișier din Carantină

Dacă ați plasat în carantină un fișier suspect care nu a fost detectat de program sau dacă un fișier a fost detectat ca infectat în mod incorect (de exemplu, prin analiza euristică a codului) și ulterior a fost plasat în carantină, trimiteți laboratorului de cercetare ESET mostra spre analiză. Pentru a trimite un fișier, faceți clic dreapta pe fișier și selectați **Trimitere spre analiză** în meniul contextual.

Descriere detectare

Faceți clic dreapta pe un element și faceți clic pe **Descriere detectare** pentru a deschide Enciclopedia amenințărilor ESET, care conține informații detaliate despre pericolele și simptomele infiltrării înregistrate.

> **Instrucțiuni ilustrate**
>
> Următoarele articole din Baza de cunoștințe ESET este posibil să fie disponibile numai în limba engleză:
>
> - Restaurați un fișier plasat în carantină în ESET NOD32 Antivirus
> - Ștergeți un fișier plasat în carantină în ESET NOD32 Antivirus
> - Produsul meu ESET m-a notificat cu privire la o detectare – ce trebuie să fac?

Nu s-a reușit plasarea în carantină

Motivele pentru care anumite fișiere nu pot fi mutate în Carantină sunt următoarele:

- **Nu aveți permisiuni de citire** – nu puteți vizualiza conținutul unui fișier.
- **Nu aveți permisiunile de scriere** – nu puteți modifica conținutul fișierului, adică fie să adăugați conținut nou, fie să ștergeți conținut existent.
- **Fișierul pe care încercați să-l mutați în Carantină este prea mare** - trebuie să reduceți dimensiunea fișierului.

Când primiți mesajul de eroare „Nu s-a reușit plasarea în carantină”, faceți clic pe **Mai multe informații**. Apare fereastra „Listă de erori carantină” și veți vedea numele fișierului și motivul pentru care fișierul nu poate fi mutat în Carantină.

Server proxy

În rețelele LAN mari, comunicația între computer și Internet poate fi mediată de un server proxy. Utilizându-se această configurație, trebuie definite următoarele setări. În caz contrar, programul nu va reuși să se actualizeze automat. În ESET NOD32 Antivirus, setarea serverului proxy este disponibilă în două secțiuni diferite din arborele Setări avansate.

În primul rând, setările de server proxy pot fi configurate în **Setare avansată** din **Instrumente** > **Server proxy**. Specificarea serverului proxy la acest nivel definește setările globale de server proxy pentru toate aplicațiile ESET NOD32 Antivirus. Parametrii de aici vor fi utilizați de toate modulele care necesită conectare la Internet.

Pentru a specifica setările de server proxy pentru acest nivel, selectați **Utilizare server proxy** și introduceți adresa serverului proxy în câmpul **Server proxy** împreună cu numărul de **port** al serverului proxy.

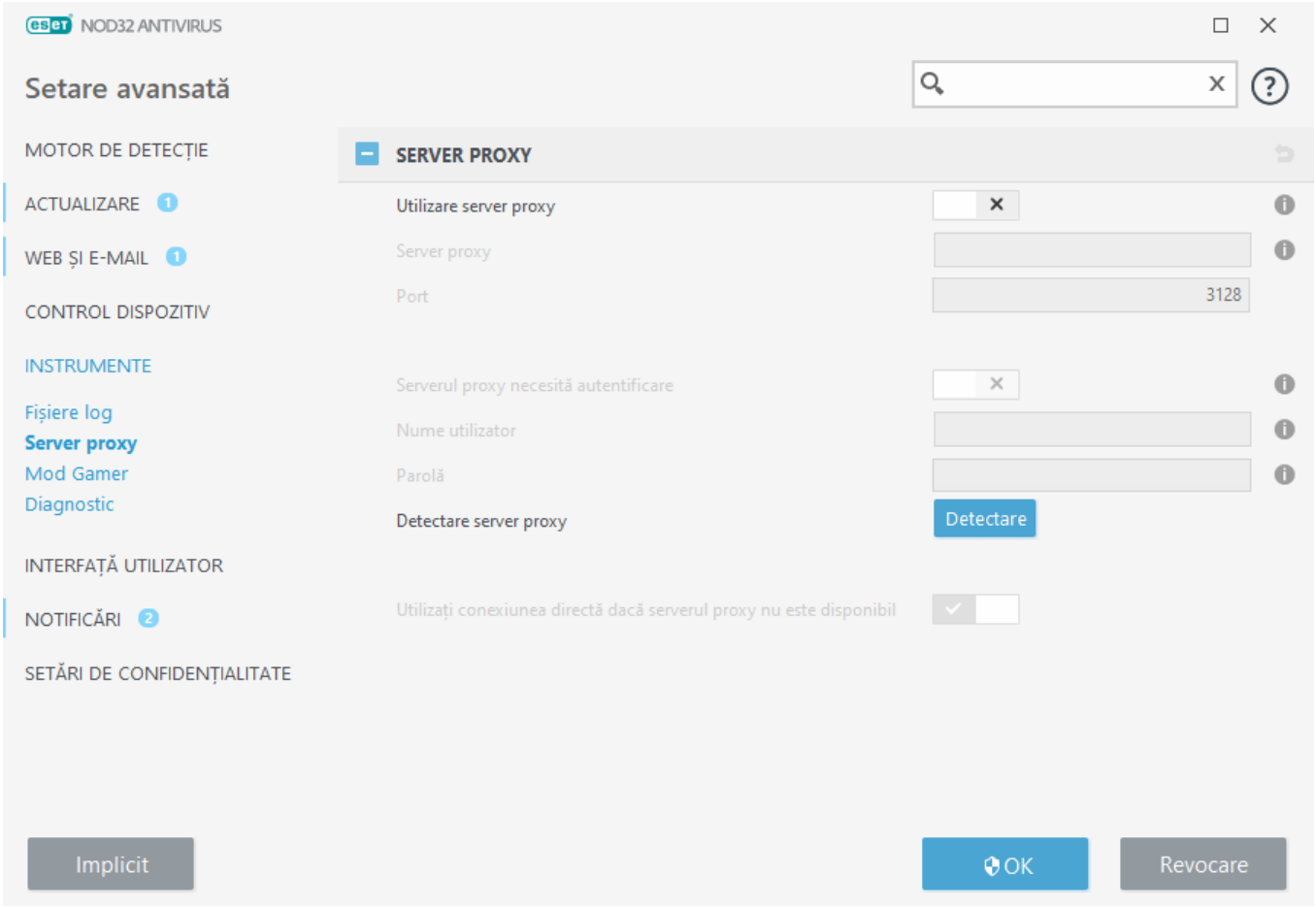
În cazul în care comunicația cu serverul proxy necesită autentificare, selectați **Serverul proxy necesită autentificare** și introduceți un **nume de utilizator** și o **parolă** valide în câmpurile respective. Faceți clic pe

Detectare server proxy pentru a detecta și a popula automat setările de server proxy. Se vor copia parametrii specificați în opțiunile internet pentru Internet Explorer sau Google Chrome.

Trebuie să introduceți manual numele de utilizator și parola în setările de **server proxy**.

Utilizați conexiunea directă dacă serverul proxy nu este disponibil – dacă ESET NOD32 Antivirus este configurat să utilizeze conexiunea proxy și nu se poate conecta la proxy, ESET NOD32 Antivirus va ocoli serverul proxy-ul și va comunica direct cu serverele ESET.

Setările de server proxy pot fi stabilite și în Setare actualizare avansată (**Setări avansate**> **Actualizare** > **Profiluri** > **Actualizări** > **Opțiuni de conectare** selectând **Conectare printr-un server proxy** din meniul vertical **Mod proxy**). Această setare se aplică pentru profilul de actualizare dat și este recomandată pentru laptopuri care primesc frecvent actualizări ale bazei de semnături virale din locații la distanță. Pentru mai multe informații despre această setare, consultați secțiunea Setare actualizare avansată.



Selectare mostră pentru analiză

Dacă găsiți un fișier suspect pe computer sau un site suspect pe internet, îl puteți trimite spre analiză către laboratorul de cercetare de la ESET (această opțiune poate fi indisponibilă, în funcție de configurarea ESET LiveGrid®).

Înainte de a trimite mostre către ESET

Nu trimiteți o mostră decât dacă îndeplinește cel puțin unul dintre criteriile următoare:

- Mostra nu este detectată de produsul dvs. ESET deloc
- Mostra este detectată în mod incorect ca fiind o amenințare
- Nu acceptăm ca mostre fișiere personale, care doriți să fie scanate pentru malware de către ESET. Laboratorul de cercetare ESET nu efectuează scanări la cerere pentru utilizatori
- Folosiți un subiect descriptiv și includeți cât mai multe informații posibil despre fișier (de exemplu, o captură de ecran sau site-ul web de unde l-ați descărcat)

Puteți să trimiteți o mostră (un fișier sau un site web) către ESET pentru analiză folosind una dintre următoarele metode:

1. Folosiți formularul pentru trimiterea probelor din produs. Îl găsiți în **Instrumente** > **Trimitere mostră pentru analiză**. Dimensiunea maximă a unei mostre trimise este de 256 MB.

2. Alternativ, puteți trimite fișierul prin e-mail. Dacă preferați această opțiune, arhivați fișierele folosind WinRAR/WinZIP, protejați arhiva cu parola „infectat” și trimiteți-o la samples@eset.com.

3. Pentru a raporta spam sau mesaje spam fals pozitive, consultați articolul din Baza de cunoștințe ESET.

În formularul **Selectare mostră pentru analiză**, selectați în meniul vertical **Motiv pentru trimiterea mostrei** descrierea care se potrivește cel mai bine scopului mesajului dvs.:

- fișier suspect,
- Site suspect (un site Web infectat de orice malware)
- site fals pozitiv,
- Fișier fals pozitiv (fișierul este detectat ca fiind infectat, dar nu este infectat)
- altele.

Fișier/Site – calea spre fișierul sau site-ul Web pe care doriți să-l trimiteți.

E-mail de contact – Acest e-mail de contact este trimis împreună cu fișierele suspecte la ESET și poate fi folosit pentru a vă contacta în cazul în care sunt necesare pentru analiză informații suplimentare. Introducerea e-mailului de contact este opțională. Selectați **Remitere în mod anonim** pentru a nu completa acest câmp.

Este posibil să nu primiți un răspuns de la ESET

Veți primi un răspuns de la ESET numai dacă mai sunt necesare informații suplimentare. Serverele noastre primesc zilnic zeci de mii de fișiere, așadar este imposibil să răspundem la toate trimiterile.
Dacă mostra se dovedește o aplicație dăunătoare sau un site web dăunător, detectarea sa va fi adăugată la una dintre actualizările ESET ulterioare.

Selectare mostră pentru analiză - Fișier suspect

Semne și simptome ale infectării cu malware observate – Introduceți o descriere a comportamentului fișierului suspect observat pe computer.

Originea fișierului (adresa URL sau vânzătorul) – Introduceți originea fișierului (sursa) și modul în care ați întâlnit

acest fișier.

Note și informații suplimentare – Aici puteți introduce informații suplimentare sau o descriere care va ajuta la identificarea fișierului suspect.

> Primul parametru – **Semne și simptome ale infectării cu malware observate** – este obligatoriu, dar furnizarea informațiilor suplimentare va ajuta semnificativ laboratoarele noastre în procesul de identificare și de procesarea a mostrelor.

Selectare mostră pentru analiză - Site suspect

Selectați una dintre următoarele opțiuni din meniul vertical **Ce probleme prezintă acest site**:

- **Infectat** – un site Web care conține viruși sau malware de alt tip distribuit prin diverse metode.
- **Phishing** – utilizat adesea pentru a obține acces la date sensibile, cum ar fi numere de cont bancar, coduri PIN etc. Citiți detalii despre acest tip de atac în glosar.
- **Înșelătorie** – un site Web fraudulos, destinat în special obținerii de profit rapid.
- Selectați **Altele**, dacă opțiunile menționate anterior nu reprezintă site-ul pe care intenționați să-l trimiteți.

Note și informații suplimentare – aici puteți introduce informații suplimentare sau o descriere care va ajuta la analizarea site-ului Web suspect.

Selectare mostră pentru analiză - Fișier fals pozitiv

Vă rugăm să trimiteți fișierele detectate ca infectate, chiar dacă acestea nu sunt infectate, pentru a ne ajuta să ne îmbunătățim motorul antivirus și antispyware și pentru a contribui la protejarea celorlalți utilizatori. Fals pozitivele (FP) pot apărea atunci când un model al unui fișier se potrivește cu un model inclus într-un motor de detecție.

Numele și versiunea aplicației – Titlul programului și versiunea acestuia (de exemplu, numărul, numele alternativ sau numele codului).

Originea fișierului (adresa URL sau vânzătorul) – Introduceți originea fișierului (sursa) și notați modul în care ați întâlnit acest fișier.

Scopul aplicației – Descrierea generală a aplicației, tipul aplicației (de ex., browser, media player...) și funcționalitatea aplicației.

Note și informații suplimentare – aici puteți introduce informații suplimentare sau descrieri care vor ajuta la procesarea fișierului suspect.

> Primii trei parametri sunt obligatorii pentru identificarea aplicațiilor legitime și pentru a le deosebi de codul dăunător. Furnizând informații suplimentare veți ajuta semnificativ laboratoarele noastre în procesul de identificare și de procesare a mostrelor.

Selectare mostră pentru analiză - Site fals pozitiv

Vă rugăm să trimiteți site-urile care sunt detectate ca infectate, înșelătoare sau de phishing, dar, de fapt, nu sunt astfel de site-uri. Fals pozitivele (FP) pot apărea atunci când un model al unui fișier se potrivește cu un model inclus într-un motor de detecție. Vă rugăm să trimiteți astfel de site-uri Web pentru a ne ajuta să ne îmbunătățim motorul anti-phishing și pentru a contribui la protejarea celorlalți utilizatori.

Note și informații suplimentare – aici puteți introduce informații suplimentare sau descrieri care vor ajuta la procesarea site-ului web suspect.

Selectare mostră pentru analiză - Altele

Utilizați acest formular dacă fișierul nu poate fi catalogat ca **Fișier suspect** sau ca **Fals pozitiv**.

Motiv pentru trimiterea fișierului – introduceți o descriere detaliată și motivul pentru trimiterea fișierului.

Actualizare Microsoft Windows®

Caracteristica de actualizare Windows reprezintă o componentă importantă a protecției utilizatorilor împotriva software-ului dăunător. Din acest motiv, este vital să instalați actualizările Microsoft Windows imediat ce devin disponibile. ESET NOD32 Antivirus vă notifică despre lipsa actualizărilor în funcție de nivelul specificat de dvs. Sunt disponibile următoarele niveluri:

- **Fără actualizări** – nu vor fi oferite pentru descărcare actualizări de sistem.
- **Actualizări opționale** – vor fi oferite pentru descărcare actualizările marcate cu prioritate redusă sau mai ridicată.
- **Actualizări recomandate** – vor fi oferite pentru descărcare actualizările marcate ca obișnuite sau cu prioritate mai ridicată.
- **Actualizări importante** – vor fi oferite pentru descărcare actualizările marcate ca importante sau cu prioritate mai ridicată.
- **Actualizări critice** – vor fi oferite pentru descărcare numai actualizările critice.

Faceți clic pe **OK** pentru a salva modificările. După verificarea stării cu serverul de actualizare se va afișa fereastra Actualizări de sistem. Prin urmare, este posibil ca informațiile despre actualizarea sistemului să nu fie disponibile imediat după salvarea modificărilor.

Fereastră de dialog – Actualizări de sistem

Dacă există actualizări disponibile pentru sistemul dumneavoastră de operare, notificarea se va afișa în fereastra ESET NOD32 Antivirus Home. Faceți clic pe **Informații suplimentare** pentru a deschide fereastra Actualizări de sistem.

Fereastra Actualizări de sistem afișează lista de actualizări disponibile gata pentru a fi descărcate și instalate. Tipul actualizării este afișat lângă numele actualizării.

Faceți clic pe orice rând de actualizare pentru a afișa fereastra Informații actualizare, care conține detalii suplimentare.

Faceți clic pe **Execută actualizarea de sistem** pentru a începe descărcarea și instalarea actualizărilor pentru sistemul de operare.

Informații actualizare

Informații despre actualizările Windows. Numele și numărul actualizării sunt afișate în partea de sus a ferestrei urmate de prioritate și de o descriere a problemei rezolvate de actualizare.

Interfață utilizator

Pentru a configura comportamentul interfeței grafice cu utilizatorul (GUI) a programului, în fereastra principală a programului, faceți clic pe **Setare** > **Setare avansată** (F5) > **Interfață utilizator**.

Puteți ajusta aspectul și efectele vizuale ale programului în ecranul Setare avansată din Elemente interfață utilizator.

Pentru a asigura securitatea maximă a software-ului de securitate, puteți preveni modificările neautorizate prin protejarea setărilor prin parolă utilizând instrumentul Setare acces.

> Pentru a configura comportamentul pentru notificări de sistem, alerte de detectare și stări aplicație, consultați secțiunea Notificări.

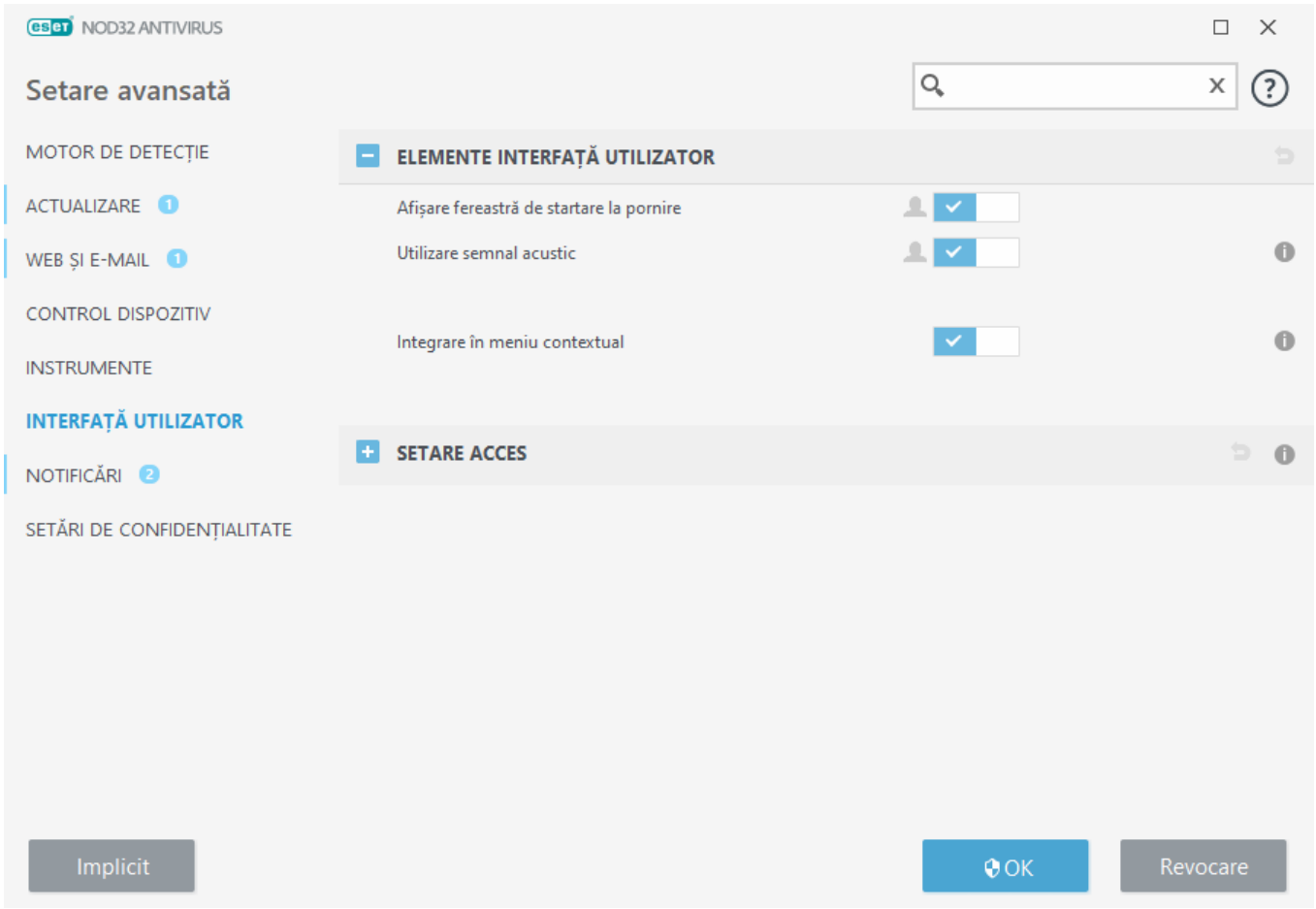
Elemente interfață utilizator

Opțiunile de configurare a interfeței de utilizator din ESET NOD32 Antivirus vă permit să ajustați mediul de lucru pentru a se adecva cerințelor dvs. Aceste opțiuni de configurare sunt disponibile accesând **Setări avansate** (F5) > **Interfață utilizator** > **Elemente interfață utilizator**.

Dacă doriți să dezactivați fereastra de întâmpinare ESET NOD32 Antivirus, deselectați **Afișare fereastră de întâmpinare la pornire**.

Utilizare semnal acustic – ESET NOD32 Antivirus redă un sunet atunci când apar evenimente importante în timpul unei scanări, de exemplu, la detectarea unei amenințări sau la terminarea unei scanări.

Integrare în meniu contextual – integrați elementele de control ale ESET NOD32 Antivirus în meniul contextual.



Setare acces

Setările pentru ESET NOD32 Antivirus reprezintă o parte esențială a politicii de securitate. Modificările neautorizate pot pune în pericol stabilitatea și protecția sistemului. Pentru a evita modificările neautorizate, parametrii de setare ai ESET NOD32 Antivirus și dezinstalarea sa pot fi protejați prin parolă.

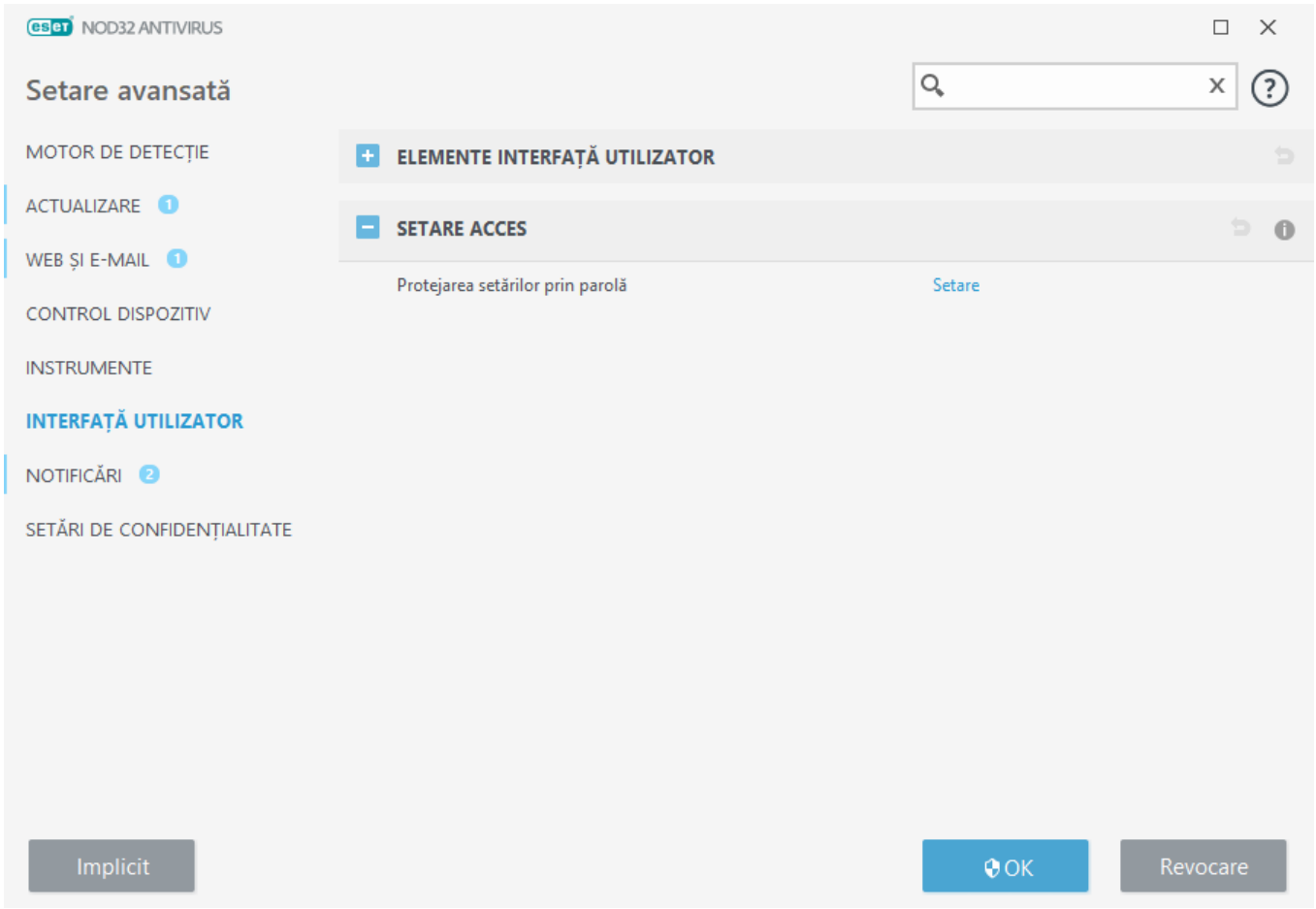
Pentru a seta o parolă pentru protejarea parametrilor de setare și împotriva dezinstalării ESET NOD32 Antivirus, faceți clic pe **Setare** lângă **Protejarea setărilor prin parolă**.

Când doriți să accesați secțiunea Setări avansate protejată prin parolă, se afișează fereastra pentru introducerea parolei. Dacă uitați sau pierdeți parola, faceți clic pe opțiunea **Reinițializare parolă** de mai jos și introduceți adresa de email pe care ați folosit-o pentru înregistrarea licenței. ESET vă va trimite un e-mail cu codul de verificare și cu instrucțiuni pentru resetarea parolei.

- Cum deblocați secțiunea Setări avansate

Pentru a schimba parola, faceți clic pe **Schimbare parolă** lângă **Protejarea setărilor prin parolă**.

Pentru a elimina parola, faceți clic pe **Eliminare** lângă **Protejarea setărilor prin parolă**.



Parolă pentru Setare avansată

Pentru a proteja setarea avansată pentru ESET NOD32 Antivirus în vederea prevenirii modificării neautorizate, trebuie setată o parolă nouă.

Atunci când doriți să schimbați o parolă existentă:

1. Tastați parola veche în câmpul **Parolă veche**.
2. Introduceți parola nouă în câmpurile **Parolă nouă** și **Confirmare parolă nouă**.
3. Faceți clic pe **OK**.

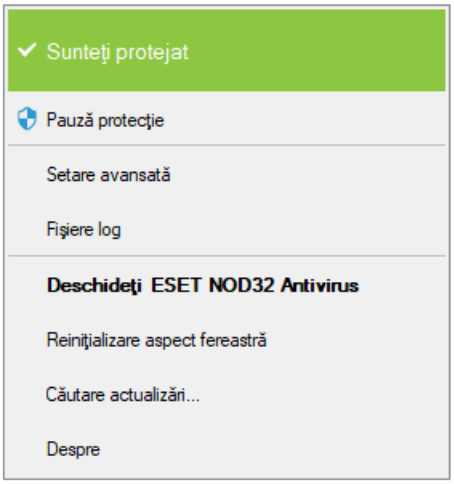
Această parolă va fi necesară pentru orice modificări aduse produsului ESET NOD32 Antivirus.

Dacă vă uitați parola, accesul la setările avansate poate fi restaurat folosind metoda „Reinițializare parolă”.

Pentru a recupera cheia de licență ESET pierdută, data expirării licenței sau alte informații despre licență pentru ESET NOD32 Antivirus, consultați articolul nostru din baza de cunoștințe.

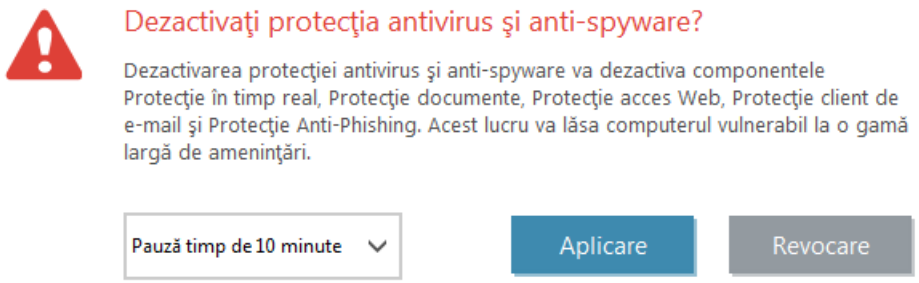
Pictograma barei de sistem

Unele dintre cele mai importante opțiuni de setare și caracteristici sunt disponibile făcând clic dreapta pe pictograma barei de sistem .



Pauză protecție – afișează caseta de dialog de confirmare care dezactivează Motorul de detecție, care protejează împotriva atacurilor provenite de la sisteme rău intenționate, controlând fișierele, site-urile web și comunicarea prin e-mail.

Meniul vertical **Interval de timp** reprezintă perioada de timp pentru care se va dezactiva protecția.



Setări avansate – select această opțiune pentru a accesa structura **Setări avansate**. Mai există și alte modalități de a deschide structura Setări avansate, cum ar fi apăsarea pe tasta F5 sau navigarea la **Setare** > **Setări avansate**.

Fișiere log – Fișierele log conțin informații despre evenimentele de program importante care au avut loc și oferă o prezentare generală a detectărilor.

Deschidere ESET NOD32 Antivirus – Deschide fereastra principală a programului ESET NOD32 Antivirus din pictograma bară.

Resetare aspect fereastră – resetează fereastra produsului ESET NOD32 Antivirus la dimensiunea și poziția implicite pe ecran.

Căutare actualizări – pornește actualizarea motorului de detecție (cunoscut anterior sub denumirea de „bază de semnături virale”) pentru a vă asigura nivelul de protecție împotriva codurilor dăunător.

Despre – furnizează informații despre sistem, detalii despre versiunea produsului ESET NOD32 Antivirus instalată și despre modulele de program instalate. Aici mai puteți găsi data de expirare a licenței și informații despre sistemul de operare și despre resursele de sistem.

Asistență pentru cititorul de ecran

ESET NOD32 Antivirus poate fi utilizat împreună cu cititoarele de ecran pentru a permite utilizatorilor ESET cu deficiențe de vedere să navigheze în produs sau să configureze setările. Următoarele cititoare de ecran sunt acceptate (JAWS, NVDA, Narrator).

Pentru a vă asigura că software-ul cititorului de ecran poate accesa interfața GUI a ESET NOD32 Antivirus în mod corect, urmați instrucțiunile din articolul din Baza de cunoștințe.

Ajutor și asistență

ESET NOD32 Antivirus conține instrumente de depanare și informații de asistență care vă vor ajuta la rezolvarea problemelor pe care le puteți întâlni.

Licență

- **Depanarea licențelor** - Faceți clic pe această legătură pentru a găsi soluții pentru probleme legate de activarea sau modificarea licenței.

- **Schimbare licență** – faceți clic pe această opțiune pentru a lansa fereastra de activare și a vă activa produsul. Dacă dispozitivul este conectat la ESET HOME, alegeți o licență din contul dvs. ESET HOME sau adăugați una nouă.

Produs instalat

- **Ce este nou**– Faceți clic pentru a deschide fereastra de informații despre funcții noi și îmbunătățite.

- **Despre ESET NOD32 Antivirus** – afișează informații despre copia produsului ESET NOD32 Antivirus.

- **Depanarea produselor** – Faceți clic pe această legătură pentru a găsi soluții la cele mai frecvente probleme întâlnite.

- **Schimbați produsul** – faceți clic pentru a vedea dacă ESET NOD32 Antivirus poate fi schimbat cu altă linie de produse cu licența curentă.

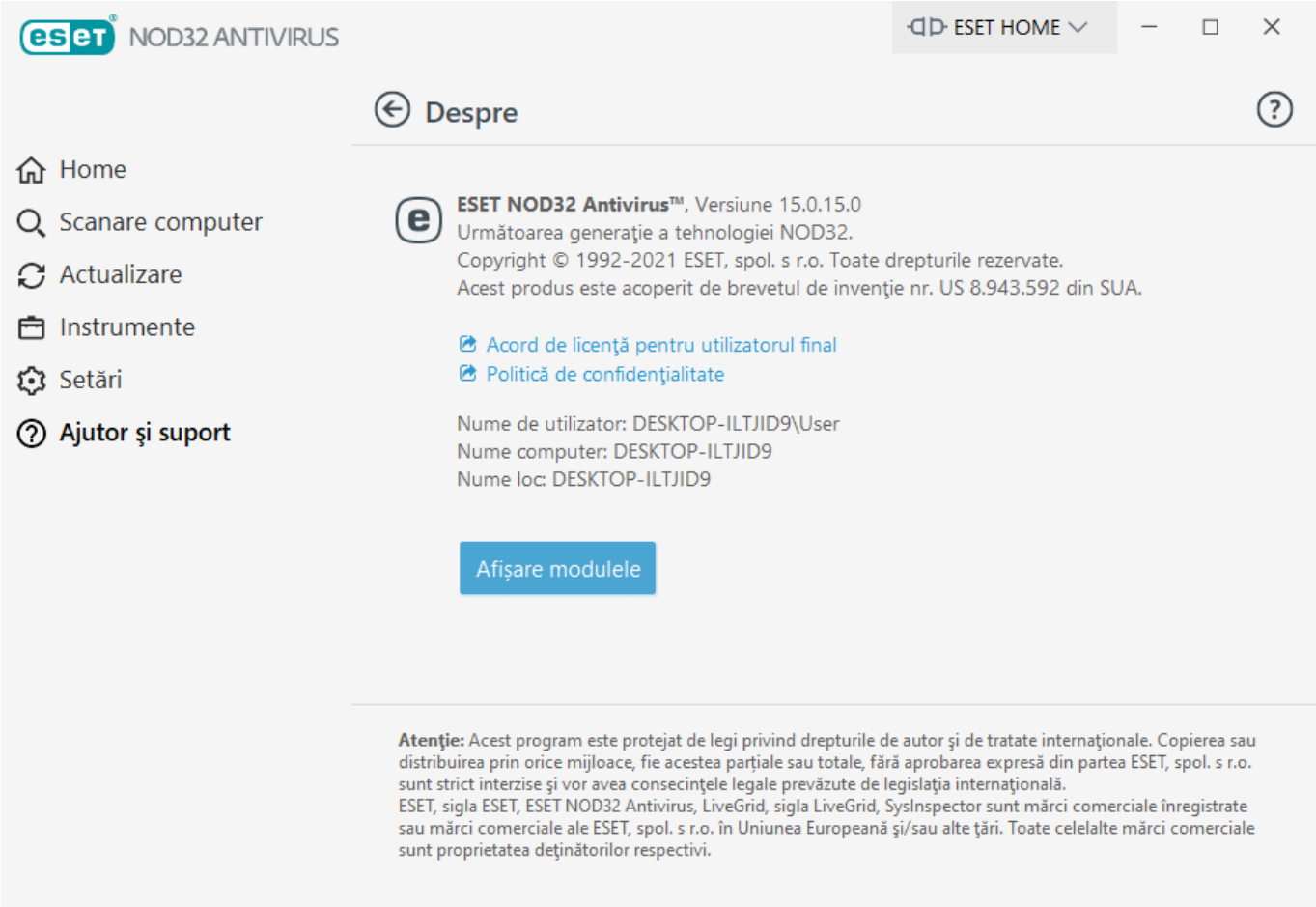
Pagina de ajutor – Faceți clic pe această legătură pentru a lansa paginile de ajutor ale produsului ESET NOD32 Antivirus.

Asistență tehnică

Baza de cunoștințe – Baza de cunoștințe ESET conține răspunsuri la cele mai frecvente întrebări și soluții recomandate pentru diverse probleme. Actualizată regulat de specialiștii tehnici ai ESET, baza de cunoștințe este instrumentul cel mai puternic pentru rezolvarea diferitelor probleme.

Despre ESET NOD32 Antivirus

Această fereastră furnizează detalii despre versiunea de ESET NOD32 Antivirus instalată și despre computerul dvs.



Faceți clic pe **Afișare modulele** pentru a vedea informații despre lista modulelor de program încărcate.

- Puteți copia informații despre module în clipboard făcând clic pe **Copiere**. Aceste informații pot fi utile pentru depanare sau atunci când contactați serviciul nostru de Asistență tehnică.

- Faceți clic pe **Motor de detecție** în fereastra Module pentru a deschide radarul ESET Virus, care conține informații despre fiecare versiune a motorului de detecție ESET.

Știri ESET

În această fereastră, ESET NOD32 Antivirus vă informează regulat despre știrile ESET.

Trimiterea de mesaje în cadrul produsului are scopul de a furniza utilizatorilor ESET știri și alte comunicări. Pentru transmiterea mesajelor de marketing este nevoie de acordul utilizatorului. Prin urmare, mesajele de marketing nu sunt transmise în mod implicit utilizatorilor (marcate cu semnul întrebării). Dacă activați această opțiune, vă exprimați acordul pentru a primi mesaje de marketing ESET. Dacă nu doriți să primiți materiale de marketing ESET, dezactivați opțiunea **Afișare mesaje de marketing**.

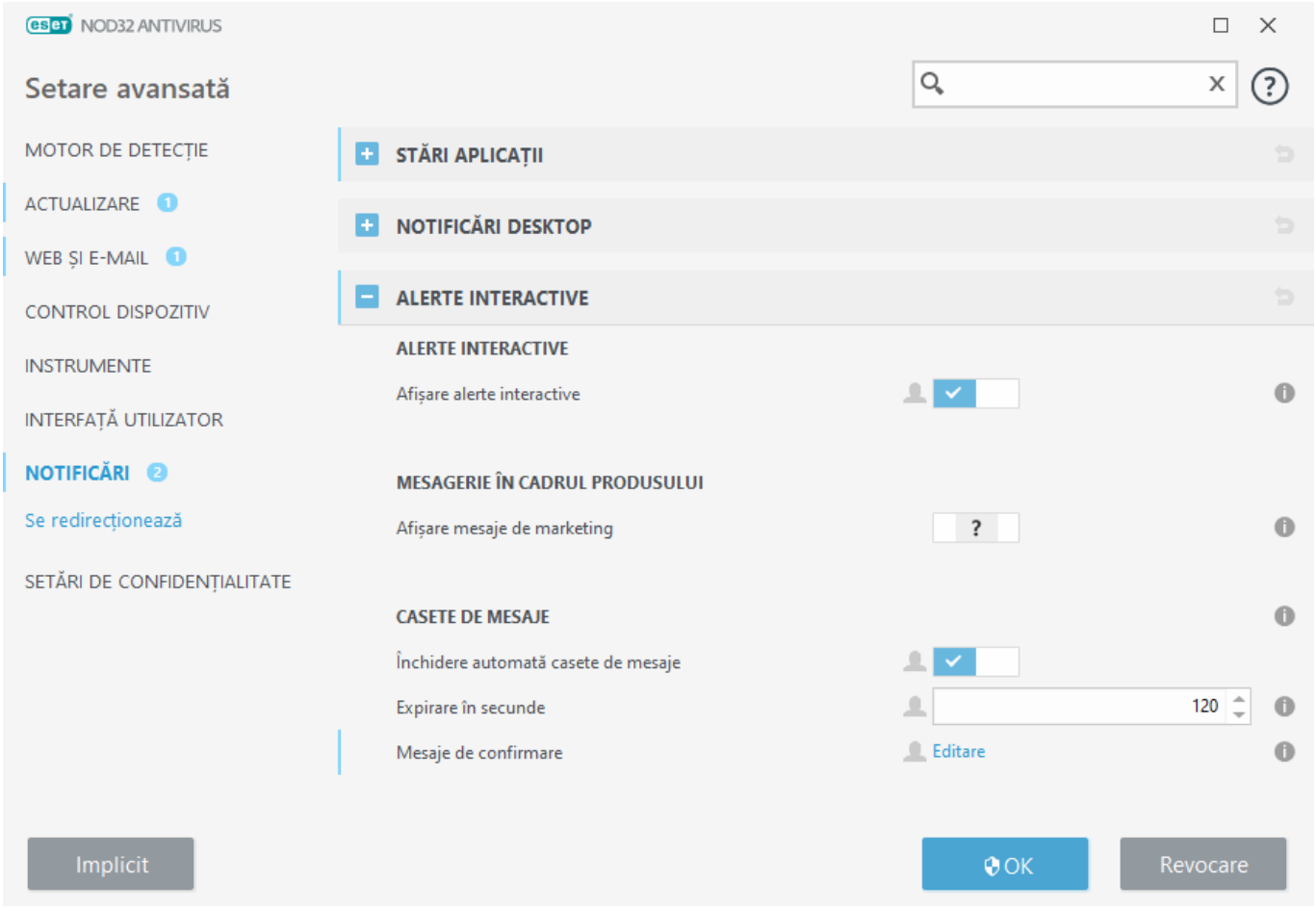
Pentru a activa sau a dezactiva primirea mesajelor de marketing printr-o fereastră pop-up, urmați instrucțiunile de mai jos.

1. Deschideți fereastra principală a produsului dvs. ESET.

2. Apăsați pe tasta **F5** pentru a accesa **Setare avansată**.

3. Apăsați pe **Notificări** > **Alerte interactive**.

4. Modificați opțiunea **Afișare mesaje de marketing**.



Trimiterea datelor de configurare a sistemului

Pentru a asigura asistență cât mai rapid și mai precis posibil, ESET are nevoie de informații despre configurația ESET NOD32 Antivirus, informații detaliate despre sistem, informații despre procesele care se execută (fișierul log ESET SysInspector) și date de registry. ESET va utiliza aceste date numai pentru furnizarea de asistență tehnică clientului.

Când trimiteți formularul web, datele de configurare a sistemului vor fi trimise la ESET. Selectați **Se trimit întotdeauna aceste informații** dacă doriți memorarea acestei acțiuni pentru acest proces. Pentru a remite formularul fără trimiterea niciunei date, faceți clic pe **Nu se trimit date** și puteți contacta Asistența tehnică ESET utilizând formularul de asistență online.

De asemenea, această setare poate fi configurată în **Setări avansate** > **Instrumente** > **Diagnostice** > Asistență tehnică.

> Dacă ați decis să trimiteți date despre sistem, trebuie să completați formularul Web, altfel biletul dvs. nu va fi creat și datele despre sistemul dvs. se vor pierde.

Asistență tehnică

În fereastra principală a programului, faceți clic pe **Ajutor și suport** > **Asistență tehnică**.

Contactați Asistența tehnică

Solicitați asistență – Dacă nu puteți găsi răspuns la problema dvs., folosiți acest formular de pe site-ul web ESET pentru a contacta rapid departamentul de asistență tehnică ESET. În funcție de setările dvs., fereastra de trimitere a datelor de configurare a sistemului este afișată înainte de a completa formularul web.

Obțineți informații pentru asistență tehnică

Detalii pentru Asistență tehnică – Când vi se solicită, puteți copia și trimite informații la Asistența tehnică ESET (cum ar fi detalii despre licență, numele produsului, versiunea produsului, sistemul de operare și informații despre computer).

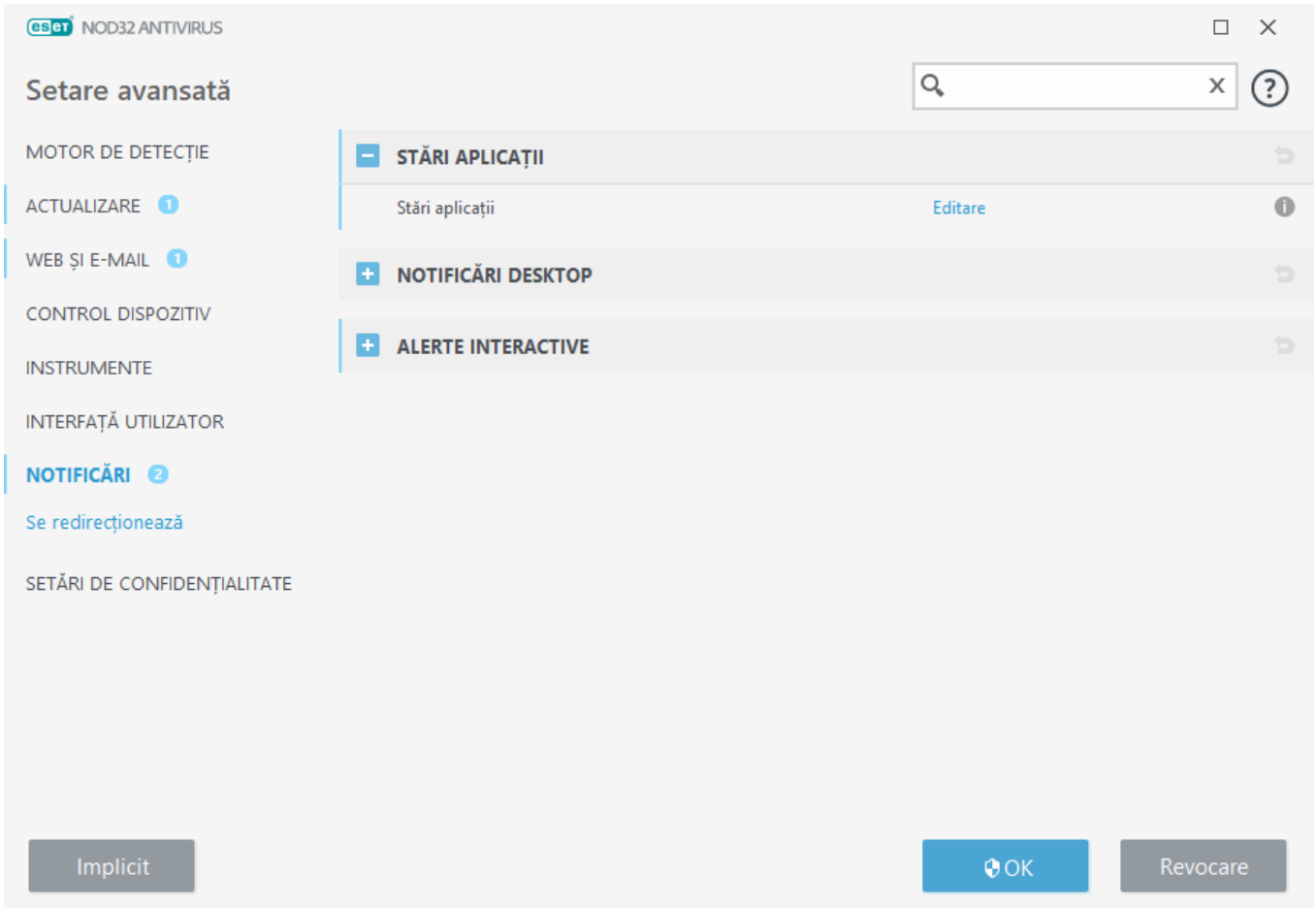
ESET Log Collector – Legături către articolul din Baza de cunoștințe ESET, de unde puteți descărca ESET Log Collector, o aplicație care colectează automat informații și loguri de pe un computer pentru a ajuta la rezolvarea mai rapidă a problemelor. Pentru mai multe informații, consultați ghidul de utilizare online pentru ESET Log Collector.

Activați opțiunea **Înregistrare avansată în log** și veți crea loguri avansate pentru toate caracteristicile care pot fi vizualizate, ajutând dezvoltatorii să diagnosticheze și să soluționeze problemele. Jurnalul de **Diagnostic** este setat pe nivelul minim de detalii. Scrierea avansată în log va fi dezactivată automat după două ore, cu excepția cazului în care o opriți mai devreme făcând clic pe **Oprire înregistrare avansată în log**. După ce au fost create toate logurile, se afișează fereastra de notificare din care puteți accesa direct folderul de Diagnostic cu logurile create.

Notificări

Pentru a gestiona notificările ESET NOD32 Antivirus, deschideți **Setare avansată** (F5) > **Notificări**. Puteți configura următoarele tipuri de notificări:

- Stări aplicație – Notificări afișate în secțiunea de pornire a ferestrei principale a programului.
- Notificări desktop – Ferestre pop-up mici de lângă bara de activități a sistemului.
- Alerte interactive – Ferestre de alertă și casete de mesaje care necesită o acțiune a utilizatorului.
- Se redirecționează (Notificări prin email) – Notificările prin e-mail sunt trimise la adresa de e-mail specificată.



Stări aplicații

Stări aplicație – Faceți clic pe **Editare** pentru a selecta stările aplicației care vor fi afișate în secțiunea de pornire a ferestrei principale a programului.

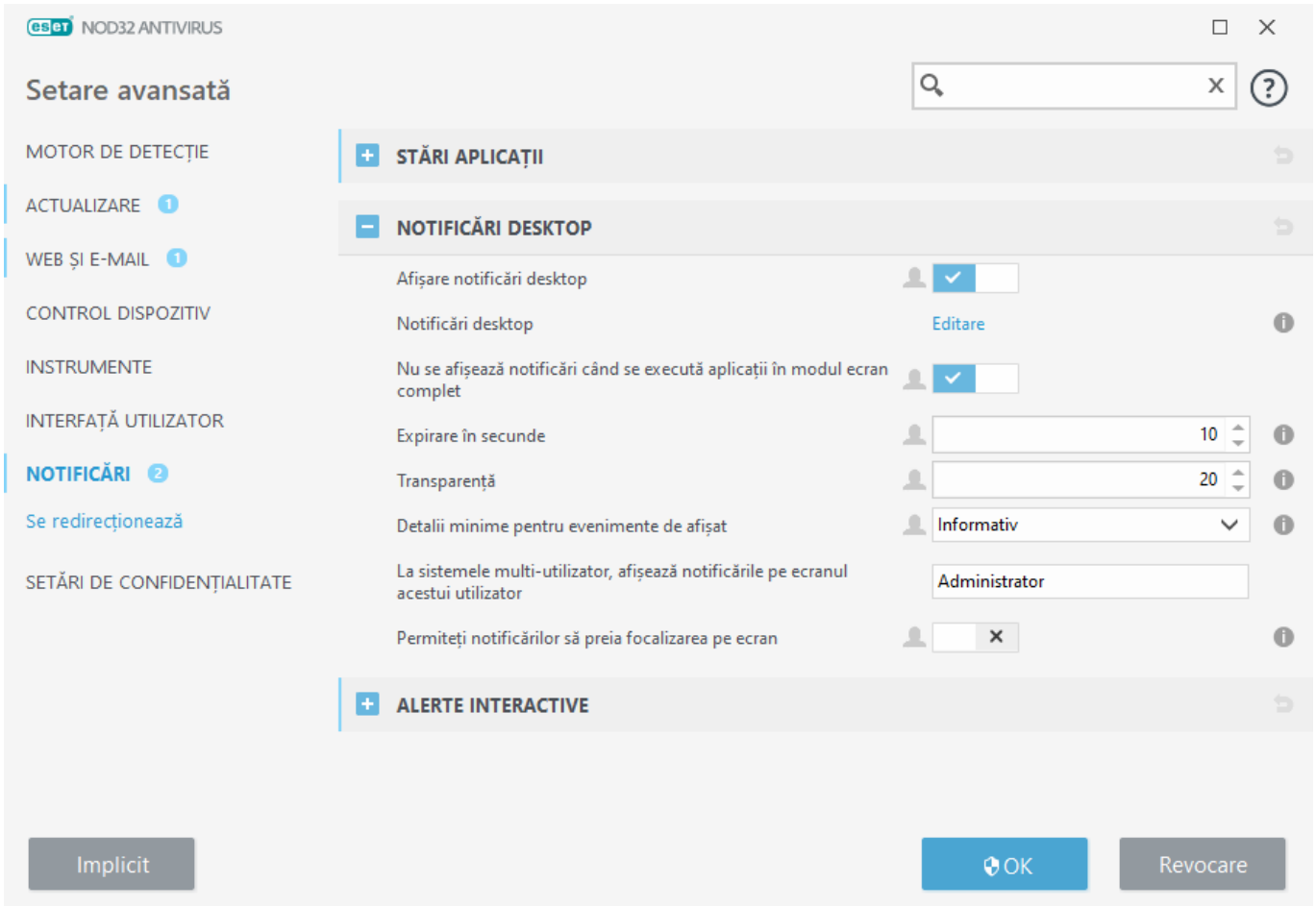
Fereastră de dialog - Stări aplicație

În această fereastră de dialog, puteți selecta ce stări de aplicație vor fi afișate. De exemplu, atunci când puneți în pauză protecția antivirus și anti-spyware sau activați modul gamer.

Starea aplicației va fi afișată și dacă produsul nu este activat sau licența a expirat.

Notificări desktop

Notificările desktop sunt reprezentate printr-o mică fereastră pop-up lângă bara de activități a sistemului. În mod implicit, sunt setate să se afișeze pentru 10 secunde, apoi dispar încet. Notificările includ: actualizări cu succes ale produsului, dispozitive noi conectate, finalizarea activităților de scanare de viruși sau amenințări noi găsite.



Afișare notificări pe desktop – Vă recomandăm să păstrați această opțiune activată, astfel încât produsul să vă poată informa atunci când are loc un eveniment nou.

Notificări desktop – Faceți clic pe **Editare** pentru a activa sau a dezactiva Notificări desktop specifice.

Nu se afișează notificări când se execută aplicații în modul ecran complet – Eliminați toate notificările neinteractive atunci când rulați aplicații în modul ecran complet.

Expirare în secunde – Setați durata vizibilității notificării. Valoarea trebuie să fie între 3-30 secunde.

Transparență – Setați procentul de transparență a notificării. Intervalul acceptat este de la 0 (fără transparență) la 80 (transparență foarte mare).

Detalii minime pentru evenimente de afișat – Setați nivelul de severitate al notificării de pornire afișat. Din meniul derulant, selectați una dintre următoarele opțiuni:

- **Diagnostic** – afișează informațiile necesare pentru reglajul fin al programului și toate înregistrările de mai sus.
- **Informativ** – afișează mesajele informative, cum ar fi evenimentele nestandard de rețea, inclusiv mesajele privind actualizarea cu succes plus toate înregistrările de mai sus.
- **Avertismente** - Afișează mesaje de avertizare, erori și erori critice (de exemplu, tehnologia Antistealth nu se execută corect sau actualizarea nu a reușit).
- **Erori** – Afișează erori (de exemplu, componenta Protecție documente nu a fost pornită) și erori critice.

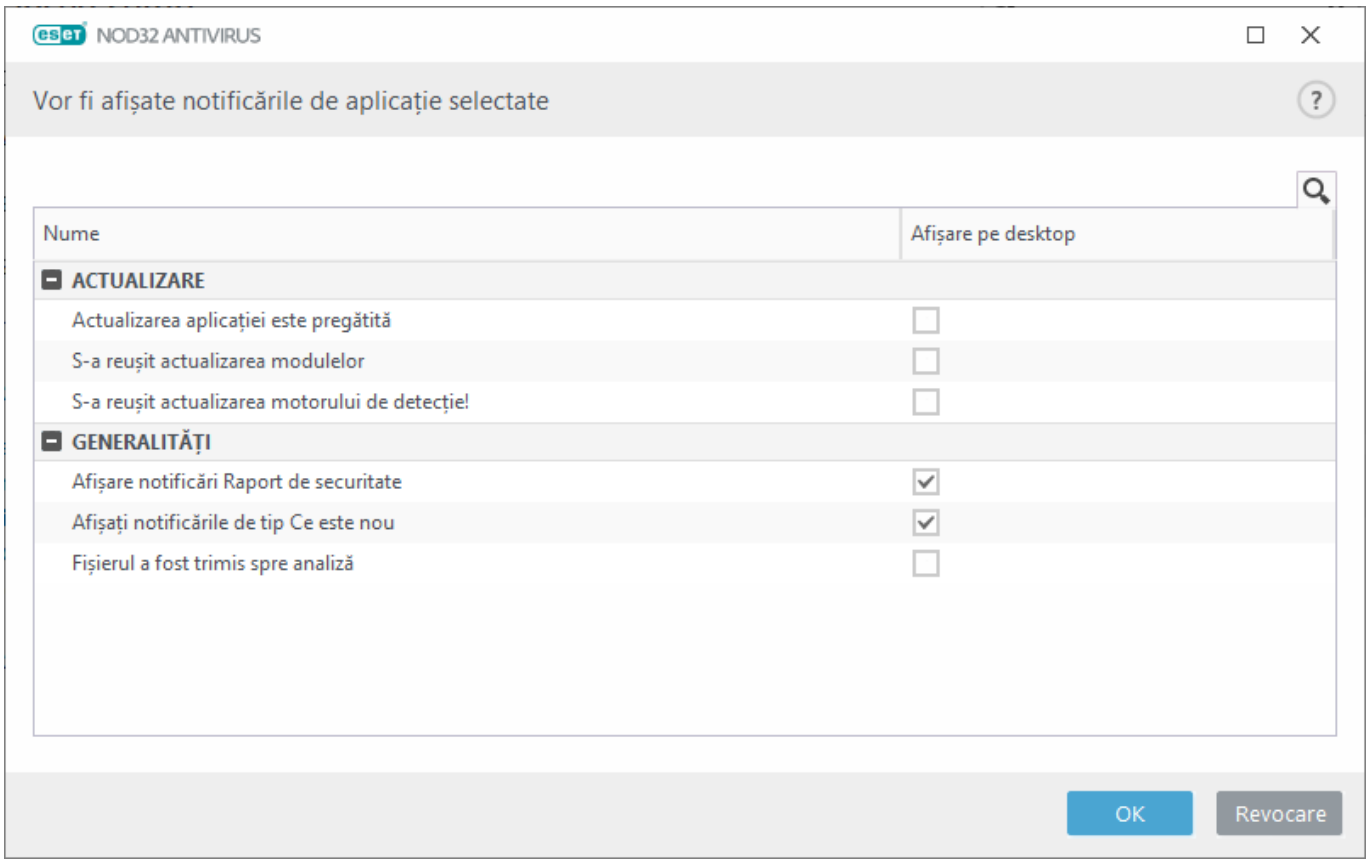
- **Critice** – Afișează numai erorile critice (erori la pornirea protecției antivirus sau sistem infectat etc.).

La sistemele multi-utilizator, afișează notificările pe ecranul acestui utilizator – Permite contului selectat să primească notificări desktop. De exemplu, dacă nu folosiți contul Administrator, tastați numele complet al contului și notificările desktop vor fi afișate pentru contul specificat. Un singur cont de utilizator poate primi notificări desktop.

Permiteți notificărilor să preia focalizarea pe ecran – Permite notificărilor să preia focalizarea pe ecran; acestea sunt accesibile în meniul **ALT + Tab**.

Lista Notificări desktop

Pentru a ajusta vizibilitatea notificărilor desktop (afișate în partea din dreapta jos a ecranului), deschideți **Setare avansată** > **Notificări** > **Notificări desktop**. Faceți clic pe **Editare** lângă **Notificări desktop** și bifați caseta de selectare **Afișare** corespunzătoare.



Generalități

Afișare notificări Raport de securitate – Primiți o notificare atunci când se generează un nou raport de securitate.

Afișați notificările de tip Ce este nou – Notificările despre toate funcțiile noi și îmbunătățite din cea mai recentă versiune de produs.

Fișierul a fost trimis spre analiză – Primiți o notificare de fiecare dată când ESET NOD32 Antivirus trimite un fișier spre analiză.

Actualizare

Actualizarea aplicației este pregătită – Primiți o notificare atunci când este pregătită o actualizare la o nouă versiune de ESET NOD32 Antivirus.

S-a reușit actualizarea motorului de detecție! – Primiți o notificare atunci când produsul actualizează modulele motorului de detecție.

S-a reușit actualizarea modulelor – Primiți o notificare atunci când produsul actualizează componentele programului.

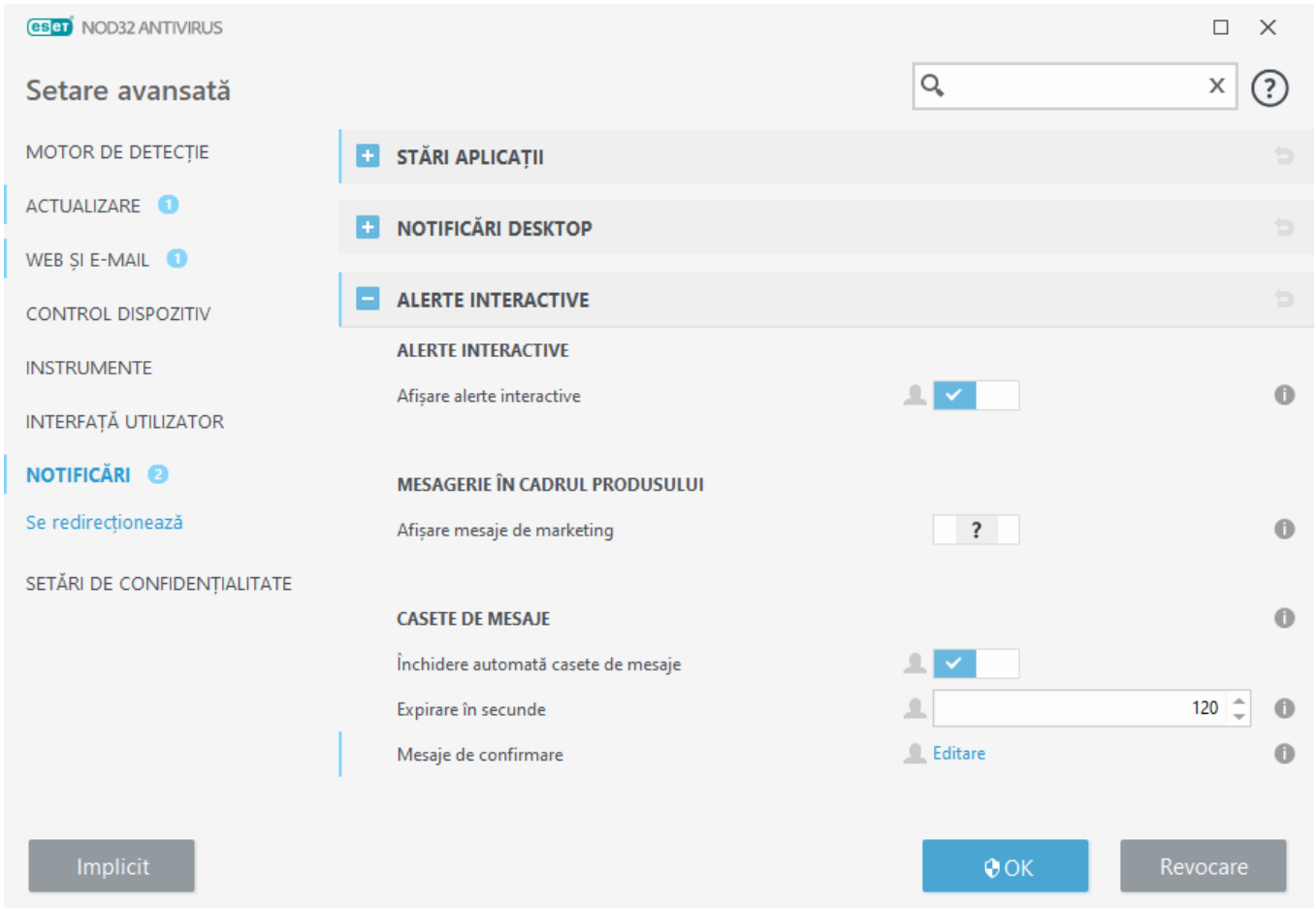
Pentru a configura setările generale pentru notificările Desktop, de exemplu, cât timp va fi afișat un mesaj sau detaliile minime pentru evenimente de afișat, consultați Notificări desktop în **Setare avansată** (F5) > **Notificări**.

Alerte interactive

Căutați informații despre alerte și notificări uzuale?

- Amenințare găsită
- Adresa a fost blocată
- Produsul nu a fost activat
- Treceți la un produs cu mai multe caracteristici
- Treceți la un produs cu mai puține caracteristici
- Este disponibilă o actualizare
- Informațiile de actualizare sunt inconsistente
- Depanarea mesajului „Nu s-a reușit actualizarea modulelor”
- Rezolvarea erorilor de actualizare a modulelor
- Certificat site Web revocat

Secțiunea **Alerte interactive** din **Setare avansată** (F5) > **Notificări** vă permite să configurați modul în care ESET NOD32 Antivirus gestionează casetele de mesaje și alertele interactive pentru detectări, în cazul în care este necesară o decizie a utilizatorului (de exemplu, un site web potențial de phishing).



Alerte interactive

Dezactivarea opțiunii **Afișare alerte interactive** va ascunde toate ferestrele de alertă și casetele de dialog din browser și este adecvată numai pentru un număr limitat de situații specifice. ESET vă recomandă să păstrați activată această opțiune.

Mesagerie în cadrul produsului

Trimiterea de mesaje în cadrul produsului are scopul de a furniza utilizatorilor ESET știri și alte comunicări. Pentru transmiterea mesajelor de marketing este nevoie de acordul utilizatorului. Prin urmare, mesajele de marketing nu sunt transmise în mod implicit utilizatorilor (marcate cu semnul întrebării). Dacă activați această opțiune, vă exprimați acordul pentru a primi mesaje de marketing ESET. Dacă nu doriți să primiți materiale de marketing ESET, dezactivați opțiunea **Afișare mesaje de marketing**.

Casete de mesaje

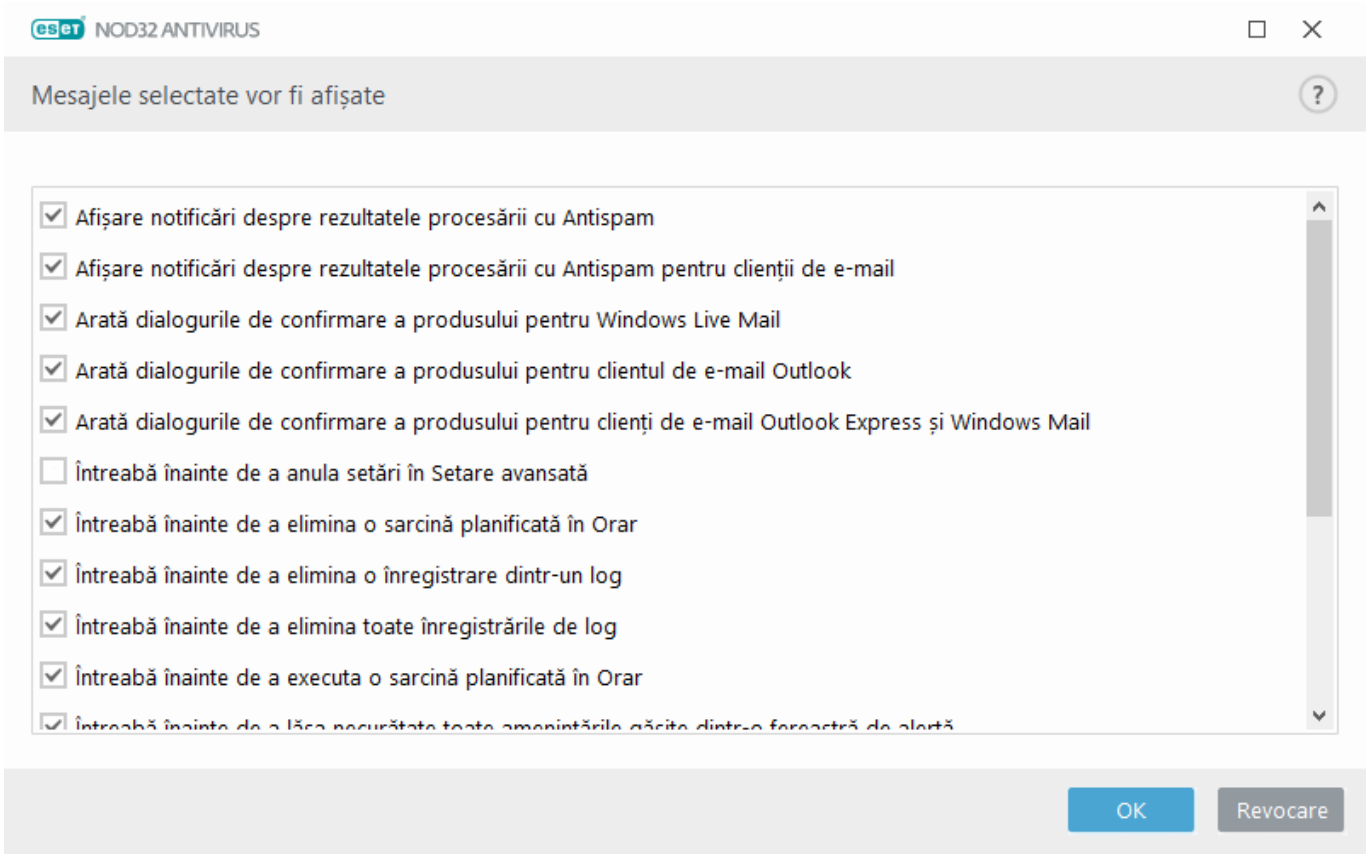
Pentru a închide după o perioadă casetele de mesaje, selectați **Închidere automată casete de mesaje**. Dacă nu sunt închise manual, ferestrele de alertă sunt închise automat după trecerea perioadei specificate.

Expirare în secunde – Setează durata vizibilității notificării. Valoarea trebuie să fie între 10–999 de secunde.

Mesaje de confirmare – Faceți clic pe **Editare** pentru a afișa o listă de mesaje de confirmare pe care le puteți selecta pentru afișare sau nu.

Mesaje de confirmare

Pentru a ajusta mesajele de confirmare, navigați la **Setare avansată** (F5) > **Notificări** > **Alerte interactive** și faceți clic pe **Editare** lângă **Mesaje de confirmare**.



Această fereastră de dialog afișează mesaje de confirmare care ESET NOD32 Antivirus vor fi afișate înainte de efectuarea oricărei acțiuni. Bifați sau debifați caseta de selectare de lângă fiecare mesaj de confirmare pentru a îl activa sau a îl dezactiva.

Aflați mai multe despre caracteristici specifice legate de mesajele de confirmare:

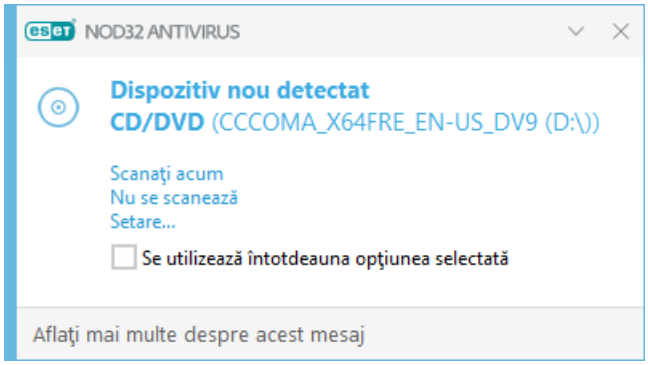
- Întreabă înainte de a șterge log-urile ESET SysInspector
- Întreabă înainte de a șterge toate logurile ESET SysInspector
- Întreabă înainte de a șterge obiecte din carantină
- Întreabă înainte de a anula setări în Setare avansată
- Întreabă înainte de a lăsa necurățate toate amenințările găsite dintr-o fereastră de alertă
- Întreabă înainte de a elimina o înregistrare dintr-un log
- Întreabă înainte de a elimina o sarcină planificată în Planificator
- Întreabă înainte de a elimina toate înregistrările de log
- Întreabă înainte de a reinițializa statistici

- Întreabă înainte de a restaura obiecte din carantină
- Întreabă înainte de a restaura obiecte din carantină și a le exclude de la scanare
- Întreabă înainte de a executa o sarcină planificată în Planificator
- Arată mesajele de dialog pentru confirmare produs pentru clienți de e-mail Outlook Express și Windows Mail
- Arată mesajele de dialog pentru confirmare produs pentru Windows Live Mail
- Arată mesajele de dialog pentru confirmare produs pentru clientul de e-mail Outlook

Unități media portabile

ESET NOD32 Antivirus asigură scanarea automată a unităților media portabile (CD/DVD/USB/...). Acest lucru poate fi util dacă administratorul computerului dorește să prevină folosirea de către utilizatori a unităților media portabile cu conținut nesolicitat.

Atunci când se introduce o unitate media portabilă, iar opțiunea **Afișare opțiuni de scanare** este configurată în ESET NOD32 Antivirus, se va afișa următorul dialog:



Opțiunile pentru acest dialog sunt:

- **Scanați acum** – se va declanșa scanarea unității media portabile.
- **Nu se scanează** – Unitățile media portabile nu vor fi scanate.
- **Setare** – Deschide secțiunea **Setare avansată**.
- **Se utilizează întotdeauna opțiunea selectată** – dacă această opțiune este selectată, se va efectua aceeași acțiune la următoarea introducere a unei unități media portabile.

În plus, ESET NOD32 Antivirus dispune de funcția de control a dispozitivului, care vă permite să definiți regulile de utilizare a dispozitivelor externe pe un anumit computer. Detalii suplimentare despre controlul dispozitivelor puteți găsi în secțiunea Control dispozitiv.

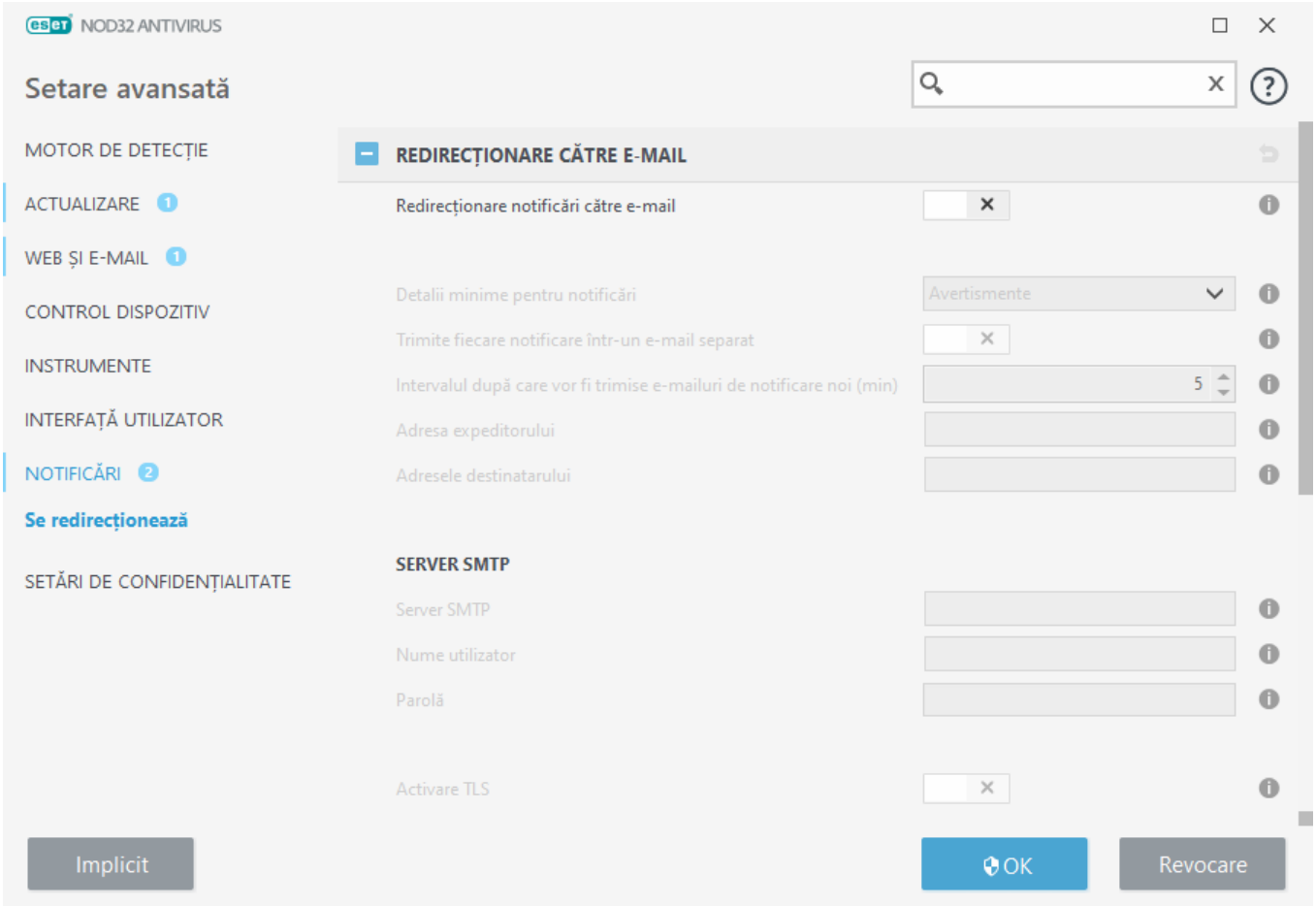
Pentru a accesa setările pentru scanarea unităților media portabile, deschideți Setare avansată (**F5**) > **Motor de detecție** > **Scanări malware** > **Unități media portabile**.

Acțiune de aplicat după inserarea unităților media portabile – Selectați acțiunea implicită care se va efectua la inserarea unui dispozitiv media portabil în computer (CD/DVD/USB). Alegeți acțiunea dorită care se va efectua la inserarea unei unități media portabile în computer:

- **Nu se scanează** – nu se va efectua nicio acțiune, iar fereastra **Dispozitiv nou detectat** nu se va deschide.
- **Scanare automată dispozitiv** – Se va efectua o scanare computer a dispozitivului media portabil introdus.
- **Afișare opțiuni de scanare** – Deschide secțiunea de setare **Unități media portabile**.

Se redirecționează

ESET NOD32 Antivirus poate trimite automat e-mailuri de notificare dacă are loc un eveniment cu nivelul de detalii selectat. Deschideți **Setare avansată** (F5) > **Notificări** > **Redirecționare** și activați **Redirecționare notificări către e-mail** pentru a activa notificările prin e-mail.



În meniul vertical **Detalii minime pentru notificări** puteți selecta nivelul de gravitate de pornire al notificărilor de trimis.

- **Diagnostic** – înregistrează informațiile necesare pentru reglajul fin al programului și toate înregistrările de mai sus.
- **Informativ** – înregistrează mesajele informative, cum ar fi evenimentele nestandard de rețea, inclusiv mesajele privind actualizarea cu succes plus toate înregistrările de mai sus.
- **Avertismente** – înregistrează erorile critice și mesajele de avertizare (tehnologia Antistealth nu se execută

corect sau actualizarea nu a reușit).

- **Erori** – înregistrează erorile (componenta Protecție documente nu este pornită) și erorile critice.

- **Critic** – înregistrează numai erorile critice (de exemplu, Eroare la pornirea protecției antivirus sau Amenințare găsită).

Trimite fiecare notificare într-un e-mail separat – atunci când această opțiune este activată, destinatarul va primi un e-mail nou pentru fiecare notificare individuală. Acest lucru poate cauza primirea unui număr mare de e-mailuri într-o perioadă scurtă de timp.

Intervalul după care vor fi trimise emailuri de notificare noi (min) – intervalul în minute după care notificările noi vor fi trimise prin email. Dacă setați această valoare la 0, notificările vor fi trimise imediat.

Adresa expeditorului – Specificați adresa expeditorului care va fi afișată în antetul mesajelor de email de notificare.

Adresele destinatarului – specificați adresele destinatarilor care vor fi afișate în antetul e-mailurilor de notificare. Se acceptă valori multiple. Utilizați punct și virgulă ca separator.

Serverul SMTP

Server **SMTP** – serverul SMTP utilizat pentru trimiterea notificărilor (de exemplu, smtp.provider.com:587, portul predefinit este 25).

Serverele SMTP cu criptare TLS sunt acceptate de ESET NOD32 Antivirus.

Nume utilizator și **Parolă** – Dacă serverul SMTP necesită autentificare, aceste câmpuri trebuie completate cu un nume de utilizator și o parolă valide pentru a se permite accesul la serverul SMTP.

Activare TLS – Secure Alert și notificări folosind criptarea TLS.

Testare conexiune SMTP – Se va trimite un mesaj e-mail de test către adresa de e-mail a destinatarului. Trebuie să completați valorile pentru Server SMTP, Nume utilizator, Parolă, Adresa expeditorului și Adresele destinatarilor.

Format mesaje

Comunicările între program și un utilizator la distanță sau un administrator de sistem se fac prin mesaje email sau LAN (utilizând serviciul de mesagerie Windows). **Formatul implicit al mesajelor** de alertă și notificărilor va fi optim în majoritatea cazurilor. În unele împrejurări, este posibil să trebuiască să modificați formatul mesajelor de evenimente.

Format pentru mesaje evenimente – Format al mesajelor despre evenimente care se afișează pe computerele la distanță.

Format pentru mesajele de avertizare amenințări – alertele și mesajele de notificare despre amenințări au un format implicit predefinit. Vă recomandăm să nu modificați acest format. Totuși, în unele situații (de exemplu, dacă aveți un sistem de procesare automată a mesajelor de email), este posibil să fiți nevoit să modificați formatul mesajului.

Set de caractere – convertește un mesaj de e-mail în codificarea caracterelor ANSI în funcție de setările regionale din Windows (de exemplu, windows-1250, Unicode (UTF-8), ACSII 7-bit sau japoneză (ISO-2022-JP)). Drept consecință, "á" se va schimba în "a", iar un simbol necunoscut se va schimba în "?".

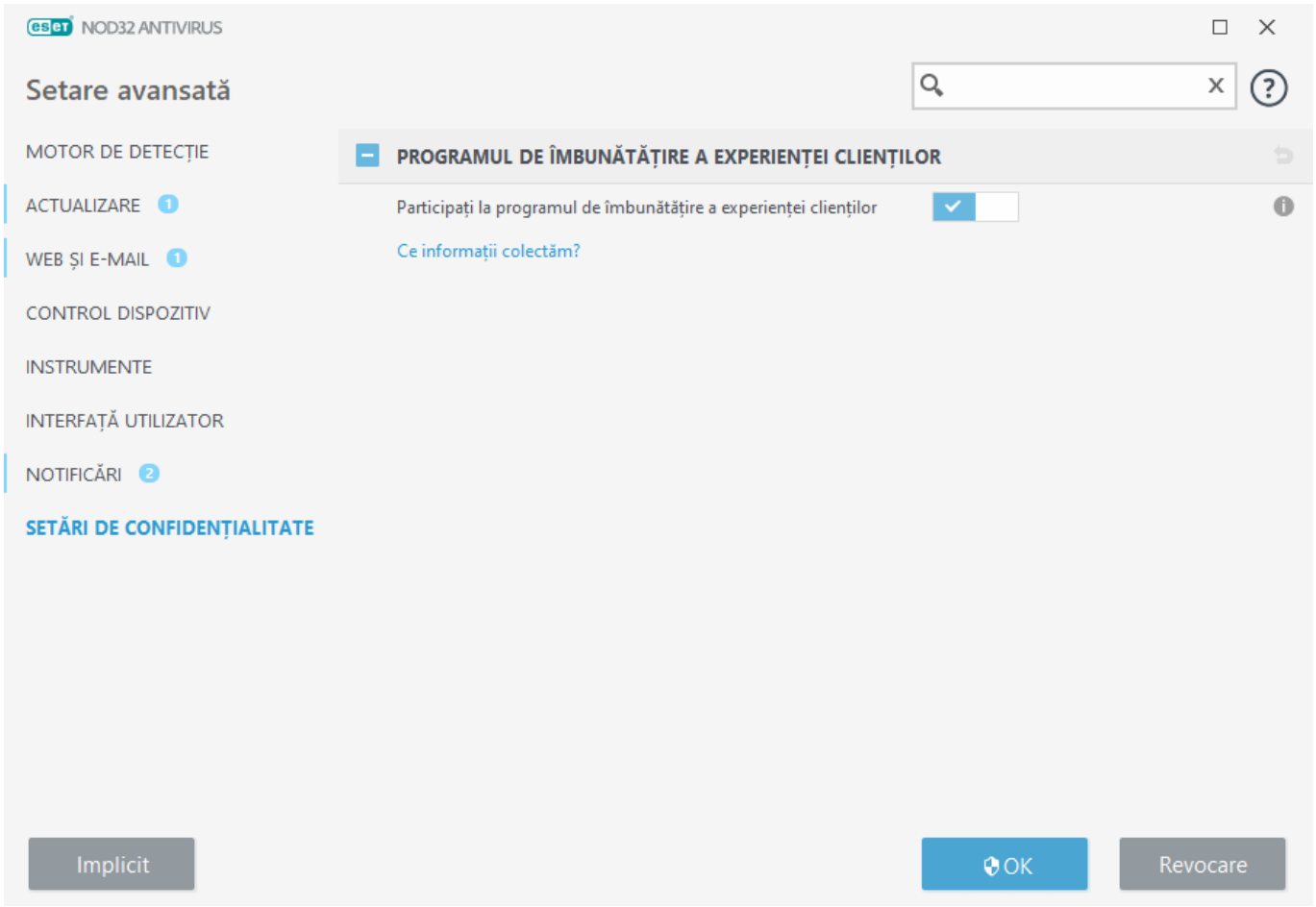
Utilizare codare cu caractere ASCII imprimabile – sursa mesajului de email va fi codată în formatul Quoted-printable (QP) care utilizează caractere ASCII și poate transmite corect caractere speciale ale alfabetului național prin email în formatul pe 8 biți (áéíóú).

- **%TimeStamp%** – data și ora evenimentului;
- **%Scanner%** – modulul în cauză;
- **%ComputerName%** – numele computerului unde a apărut alerta;
- **%ProgramName%** – programul care a generat alerta;
- **%InfectedObject%** – numele fișierului infectat, mesajului infectat etc.
- **%VirusName%** – identificarea infectării;
- **%Action%** – Acțiunea efectuată împotriva infiltrării
- **%ErrorDescription%** – descrierea unui eveniment care nu are legătură cu un virus.

Cuvintele cheie **%InfectedObject%** și **%VirusName%** se utilizează numai în mesajele de avertizare privind amenințările, iar **%ErrorDescription%** se utilizează numai în mesajele privind evenimentele.

Setări de confidențialitate

În fereastra principală a programului, faceți clic pe **Setare** > **Setare avansată** (F5) > **Setări de confidențialitate**.



Programul de îmbunătățire a experienței clienților

Activați bara glisorului de lângă **Participați la Programul de îmbunătățire a experienței clienților** pentru a vă alătura Programului de îmbunătățire a experienței clienților. Prin asociere, furnizați ESET informații anonime referitoare la utilizarea produselor ESET. Datele colectate ne vor ajuta să vă îmbunătățim experiența și nu vor fi niciodată partajate cu terțe părți. Ce informații colectăm?

Profiluri

Managerul de profil se utilizează în două locuri din ESET NOD32 Antivirus – în secțiunea **Scanare computer la cerere** și în secțiunea **Actualizare**.

Scanare computer

Există 4 profiluri de scanare predefinite în ESET NOD32 Antivirus:

- **Scanare inteligentă** – Acesta este profilul implicit de scanare avansată. Profilul Scanare inteligentă utilizează tehnologia Optimizare inteligentă, care exclude fișierele care s-au dovedit a fi curate într-o scanare anterioară și care nu au fost modificate de la acea scanare. Acest lucru permite reducerea timpilor de scanare, cu un impact minim asupra securității sistemului.

- **Scanare context menu** – Puteți începe o scanare la cerere a oricărui fișier din meniul contextual. Profilul Scanare context menu vă permite să definiți o configurație de scanare care va fi utilizată atunci când lansați scanarea în acest fel.

- **Scanare în profunzime** – Profilul Scanare în profunzime nu utilizează optimizarea inteligentă în mod implicit, astfel că niciun fișier nu este exclus de la scanare când se folosește acest profil.

- **Scanare computer** – Acesta este profilul implicit utilizat în scanarea standard a computerului.

Parametrii dvs. preferați de scanare pot fi salvați pentru scanări viitoare. Vă recomandăm să creați câte un profil diferit (cu diverse ținte de scanare, metode de scanare și alți parametri) pentru fiecare scanare utilizată în mod regulat.

Pentru a crea un profil nou, deschideți fereastra Setări avansate (F5) și faceți clic pe **Motor de detecție** > **Scanări malware** > **Scanare la cerere** > **Listă de profiluri**. Fereastra **Manager profil** include meniul vertical **Profil selectat** cu profilurile de scanare existente și opțiunea de a crea un profil de scanare nou. Pentru ajutor privind crearea unui profil de scanare adecvat cerințelor dvs., consultați secțiunea Setare parametri motor ThreatSense pentru o descriere a fiecărui parametru pentru configurarea scanării.

Să presupunem că doriți să creați propriul dvs. profil de scanare și configurația **Scanați computerul** este parțial adecvată, însă nu doriți să scanați pachete de rutină sau aplicații potențial periculoase și, de asemenea, doriți să aplicați **Remediați întotdeauna detectarea**. Introduceți numele profilului nou în fereastra **Manager profil** și faceți clic pe **Adăugare**. Selectați profilul nou din meniul vertical **Profil selectat**, modificați parametrii rămași astfel încât să îndeplinească cerințele dvs., apoi faceți clic pe **OK** pentru a salva profilul nou.

Actualizare

Editorul de profiluri din secțiune Setare actualizare permite utilizatorilor să creeze profiluri noi de actualizare. Creați-vă propriile profiluri personalizate (altele decât **Profilul meu** implicit) numai în cazul în care computerul folosește moduri multiple de conectare la serverele de actualizare.

De exemplu, un laptop care în mod normal se conectează la un server local (Oglindă) din rețeaua locală, dar care descarcă actualizările direct de pe serverele de actualizare ale ESET atunci când este deconectat de la rețeaua locală (călătorie de afaceri) ar putea utiliza două profiluri: primul pentru conectarea la serverul local; celălalt pentru conectarea la serverele ESET. După ce sunt configurate aceste profiluri, navigați la **Instrumente** > **Orar** și editați parametrii sarcinii de actualizare. Desemnați un profil ca fiind principal și pe celălalt ca secundar.

Profil de actualizare – Profilul de actualizare utilizat actualmente. Pentru modificarea acestuia, alegeți un profil din meniul vertical.

Listă de profiluri – creați profiluri de actualizare noi sau eliminați profiluri existente.

Scurtături tastatură

Pentru o navigare mai bună în ESET NOD32 Antivirus, puteți utiliza următoarele scurtături de la tastatură:

Scurtături tastatură	Acțiune
F1	deschide paginile de ajutor
F5	deschide Setare avansată
Săgeată sus/jos	navigarea în elementele de meniu vertical
TAB	trece la următorul element GUI într-o fereastră
Shift+TAB	trece la precedentul element GUI într-o fereastră

Scurtături tastatură	Acțiune
ESC	închide fereastra de dialog activă
Ctrl+U	afișează informații despre licența ESET și despre computer (Detalii pentru Asistență tehnică)
Ctrl+R	resetează fereastra produsului la dimensiunea și poziția implicite din ecran
ALT + Săgeată stânga	navigare înapoi
ALT + Săgeată dreapta	navigare înainte
ALT+Home	navigare acasă

De asemenea, puteți folosi pentru navigare butoanele înapoi sau înainte ale mouse-ului.

Diagnostic

Modulul Diagnostic furnizează imagini ale proceselor ESET (de exemplu, ekrn). Dacă o aplicație se oprește neașteptat, va fi generată o imagine. Aceasta îi poate ajuta pe dezvoltatori să depaneze și să remedieze diverse ESET NOD32 Antivirus probleme.

Faceți clic pe meniul vertical de lângă **Dump Memorie** și selectați una dintre cele trei opțiuni disponibile:

- Selectați **Dezactivare** pentru a dezactiva această caracteristică.
- **Mini** (implicit)– înregistrează setul cel mai restrâns de informații utile care pot ajuta la identificarea cauzei opririi neașteptate a aplicației. Acest tip de fișier cu imaginea memoriei poate fi util atunci când spațiul este limitat. Cu toate acestea, datorită informațiilor limitate incluse, este posibil ca erorile care nu au fost cauzate direct de firul de execuție activ la momentul apariției problemei să nu fie descoperite în urma analizării acestui fișier.
- **Complet** – înregistrează întregul conținut al memoriei sistemului la oprirea neașteptată a aplicației. O imagine completă a memoriei poate conține date din procesele care se executau la colectarea imaginii memoriei.

Director de destinație – director unde se va genera imaginea memoriei la oprirea neașteptată a aplicației.

Deschidere director diagnostic – faceți clic pe **Deschidere** pentru a deschide acest director într-o fereastră *Windows Explorer* nouă.

Creare imagine diagnosticare – faceți clic pe **Creare** pentru a crea fișiere imagine de diagnosticare în **Director de destinație**.

Înregistrare avansată în log

Activare înregistrare în log avansată în mesajele de marketing - Înregistrați toate evenimentele legate de mesajele de marketing din produs.

Activați înregistrarea în log avansată pentru scanare computer – înregistrați toate evenimentele care apar la scanarea fișierelor și folderelor de către componenta Scanare computer.

Activați înregistrarea avansată în log pentru Control dispozitiv – înregistrați toate evenimentele care se produc în componenta Control dispozitiv. Acest lucru poate ajuta dezvoltatorii să diagnosticheze și să remedieze

probleme legate de componenta Control dispozitiv.

Activare înregistrare în log avansată Direct Cloud – Înregistrați toate evenimentele care se produc în componenta ESET LiveGrid®. Acest lucru poate ajuta dezvoltatorii să diagnosticheze și să remedieze probleme legate de componenta ESET LiveGrid®.

Activare înregistrarea în log avansată pentru Protecție documente – Înregistrați toate evenimentele care apar în Protecție documente pentru a permite diagnosticarea și rezolvarea problemelor.

Activare înregistrare avansată în log pentru Protecție client e-mail – Înregistrați toate evenimentele care apar în Protecție client e-mail și în pluginul clientului de e-mail pentru a permite diagnosticarea și rezolvarea problemelor.

Activare înregistrare în log avansată kernel – Înregistrați toate evenimentele care apar în kernelul ESET (ekrn).

Activați înregistrarea avansată în log pentru Licențe – Înregistrați toate comunicările produsului cu serverele de activare ESET sau ESET License Manager.

Activare urmărire memorie – Înregistrați toate evenimentele care-i pot ajuta pe dezvoltatori să diagnosticheze pierderile de memorie.

Activați înregistrarea în log avansată pentru sistemul de operare – Se înregistrează informații suplimentare despre sistemul de operare, cum ar fi procesele care se execută, activitatea CPU și operațiunile discului. Acest lucru îi poate ajuta pe dezvoltatori să diagnosticheze și să remedieze problemele legate de produsul ESET care se execută pe sistemul dvs. de operare.

Activați înregistrarea avansată în log pentru Filtrare protocoale – înregistrați toate datele din rețea care trec prin motorul Filtrare protocoale în format PCAP pentru a ajuta dezvoltatorii să diagnosticheze și să remedieze probleme legate de filtrarea protocoalelor.

Activați înregistrarea în log avansată pentru mesajele push – Înregistrați toate evenimentele care apar în mesaje push.

Activați înregistrarea în log avansată pentru componenta Protecția în timp real pentru sistemul de fișiere – înregistrați toate evenimentele care apar la scanarea fișierelor și folderelor de către componenta Scanare computer sau Protecție în timp real pentru sistemul de fișiere.

Activați înregistrarea avansată în log pentru motorul de actualizare – înregistrați toate evenimentele care se produc în timpul procesului de actualizare. Această opțiune îi ajuta pe dezvoltatori să diagnosticheze și să remedieze probleme legate de motorul de actualizare.

Fișierele log se află în *C:\ProgramData\ESET\ESET Security\Diagnostics*.

Asistență tehnică

Când contactați Asistența tehnică ESET din ESET NOD32 Antivirus, puteți să trimiteți date de configurare a sistemului. Selectați **Trimitere întotdeauna** în meniul vertical **Trimitere date configurare sistem** pentru a trimite automat datele sau selectați **Întreabă înainte de trimitere** pentru a fi întrebat înainte de remiterea datelor.

Importarea și exportarea setărilor

Puteți importa sau exporta fișierul de configurare .xml particularizată pentru ESET NOD32 Antivirus din meniul **Setare**.

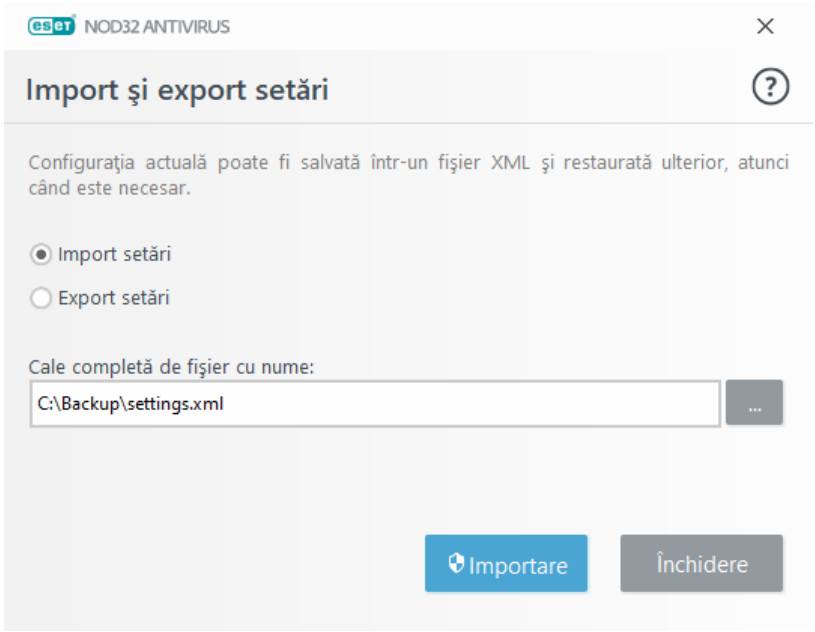
> **Instrucțiuni ilustrate**
> Consultați Importarea sau exportarea setărilor de configurare ESET utilizând un fișier .xml pentru a vedea instrucțiunile ilustrate disponibile în limba engleză și în alte câteva limbi.

Importarea și exportarea fișierelor de configurare este utilă dacă doriți să efectuați copia de rezervă a configurației curente a programului ESET NOD32 Antivirus, pentru a fi utilizată ulterior. Opțiunea setărilor de export este, de asemenea, utilă când doriți să folosiți configurația preferată pe mai multe sisteme. Puteți importa cu ușurință un fișier .xml pentru a transfera aceste setări.

Pentru a importa o configurație, în fereastra principală a meniului, faceți clic pe **Setare** > **Importare/exportare setări** și selectați **Importare setări**. Tastați numele fișierului de configurare sau faceți clic pe butonul **...** pentru a căuta fișierul de configurare pe care doriți să-l importați.

Pentru a exporta o configurație, în fereastra principală a programului, faceți clic pe **Setare** > **Importare/exportare setări**. Selectați **Exportare setări** și tastați numele complet al căii fișierului. Faceți clic pe **...** pentru a naviga către o locație pe computer pentru a salva fișierul de configurare.

> Este posibil să apară o eroare la exportarea setărilor dacă nu aveți drepturi suficiente pentru scrierea fișierului exportat în directorul specificat.



Restaurează toate setările în secțiunea curentă

Faceți clic pe săgeata curbă pentru a restaura toate setările din secțiunea curentă la setările implicite definite de ESET.

Rețineți că orice modificare efectuată se va pierde după ce faceți clic pe **Revenire la valoare implicită**.

Revenire pentru conținutul tabelelor – atunci când opțiunea este activată, regulile, sarcinile și profilurile adăugate manual sau automat se vor pierde.

Consultați și secțiunea Importarea și exportarea setărilor.

Revenire la setări implicite

Apăsați pe **Implicit** în **Setare avansată** (F5) pentru a restaura toate setările programului, pentru toate modulele. Acest lucru va reseta setările la starea pe care ar fi avut-o după o instalare nouă.

Consultați și secțiunea Importarea și exportarea setărilor.

Eroare la salvarea configurării

Acest mesaj de eroare indică faptul că setările nu s-au salvat corect din cauza unei erori.

Aceasta înseamnă de obicei că utilizatorul care a încercat să modifice parametrii programului:

- nu are suficiente drepturi de acces sau nu are privilegiile necesare în sistemul de operare pentru a modifica fișierele de configurare și registry-ul de sistem.
  > Pentru a efectua modificările dorite, administratorul de sistem trebuie să se conecteze.

- a activat recent modul de învățare în HIPS sau în Firewall și a încercat să efectueze modificări în Setare avansată.
  > Pentru a salva configurația și a evita un conflict de configurare, închideți Setare avansată fără să salvați și încercați să efectuați din nou modificările dorite.

A doua cea mai frecventă cauză este că programul nu mai funcționează corect, este deteriorat și prin urmare trebuie să fie reinstalat.

Scaner linie de comandă

Modulul Antivirus al ESET NOD32 Antivirus poate fi lansat prin intermediul liniei de comandă – manual (cu ajutorul comenzii „ecls”) sau cu ajutorul unui fișier de comenzi („bat”).

Utilizarea scanerului ESET în linie de comandă:

```
ecls [OPTIONS..] FILES..
```

Parametrii și butoanele următoare pot fi folosite la executarea scanerului la cerere din linia de comandă:

Opțiuni

/base-dir=DIRECTOR	încărcare module din DIRECTOR
/quar-dir=DIRECTOR	DIRECTOR carantină
/exclude=MASCĂ	exclude de la scanare fișiere care corespund cu MASCĂ

/subdir	scanează subdirectoare (implicit)
/no-subdir	nu scana subdirectoare
/max-subdir-level=NIVEL	nivel maxim de subdirectoare în directoarele de scanat
/symlink	urmează legături simbolice (implicit)
/no-symlink	ignoră legături simbolice
/ads	scanează ADS (implicit)
/no-ads	nu scana ADS
/log-file=FIȘIER	înregistrează ieșirile în FIȘIER
/log-rewrite	suprascrie fișier de ieșire (implicit – adăugare)
/log-console	înregistrează ieșiri în consolă (implicit)
/no-log-console	nu înregistra ieșiri în consolă
/log-all	înregistrează în log și fișierele curate
/no-log-all	nu înregistra în log fișierele curate (implicit)
/aind	afișează indicator de activitate
/auto	scanează și curăță automat toate discurile locale

Opțiuni scaner

/files	scanare fișiere (implicit)
/no-files	nu scana fișiere
/memory	scanare memorie
/boots	scanează sectoarele de boot
/no-boots	nu scana sectoarele de boot (implicit)
/arch	scanare arhive (implicit)
/no-arch	nu scana arhive
/max-obj-size=DIMENSIUNE	scanare numai fișiere mai mici de DIMENSIUNE megaocteți (implicit 0 = nelimitat)
/max-arch-level=NIVEL	nivel maxim de arhive în arhive (arhive imbricate) de scanat
/scan-timeout=LIMITĂ	scanare arhivă timp de maxim LIMITĂ secunde
/max-arch-size=DIMENSIUNE	scanează fișiere dintr-o arhivă numai dacă sunt mai mici de DIMENSIUNE (implicit 0 = nelimitat)
/max-sfx-size=DIMENSIUNE	scanează numai fișiere din arhivă SFX dacă sunt mai mici de DIMENSIUNE megaocteți (implicit 0 = nelimitat)
/mail	scanează fișiere email (implicit)
/no-mail	nu scana fișiere email
/mailbox	scanează cutii poștale (implicit)
/no-mailbox	nu scana cutii poștale
/sfx	scanează arhive SFX (implicit)
/no-sfx	nu scana arhive SFX
/rtp	scanează pachete de rutină (implicit)
/no-rtp	nu scana pachete de rutină
/unsafe	scanează după aplicații potențial periculoase

/no-unsafe	nu scana după aplicații potențial periculoase (implicit)
/unwanted	scanează după aplicații potențial nedorite
/no-unwanted	nu scana după aplicații potențial nedorite (implicit)
/suspicious	scanează aplicații suspecte (implicit)
/no-suspicious	nu scana aplicații suspecte
/pattern	folosește semnături (implicit)
/no-pattern	nu folosi semnături
/heur	activează euristica (implicit)
/no-heur	dezactivează euristica
/adv-heur	activează Euristica avansată (implicit)
/no-adv-heur	dezactivează Euristica avansată
/ext-exclude=EXTENSII	exclude de la scanare EXTENSII de fișiere delimitate prin două puncte
/clean-mode=MOD	utilizează MOD curățare pentru obiectele infectate Sunt disponibile următoarele opțiuni: • `none` (implicit) – nu se va efectua nicio curățare automată. • `standard` – ecls.exe va încerca să curețe sau să șteargă automat fișierele infectate. • `strict` – ecls.exe va încerca să curețe sau să șteargă automat fișierele infectate fără intervenția utilizatorului (nu vi se va solicita confirmarea înainte de ștergerea fișierelor). • `riguros` – ecls.exe va șterge fișierele fără a încerca să le curețe, indiferent de ce reprezintă fișierele. • `ștergere` – ecls.exe va șterge fișierele fără a încerca să le curețe, însă nu va șterge fișiere sensibile, cum ar fi fișierele de sistem Windows.
/quarantine	copiază fișiere infectate (dacă sunt curățate) în Carantină (suplimentează acțiunea efectuată în timpul curățării)
/no-quarantine	nu copia fișierele infectate în Carantină

Opțiuni generale

/help	afișare ajutor și ieșire
/version	afișare informații despre versiune și ieșire
/preserve-time	păstrare ultimul marcaj temporal

Coduri de ieșire

0	nu a fost găsită nicio amenințare
1	amenințări găsite și curățate
10	imposibil de scanat unele fișiere (pot fi amenințări)
50	amenințare găsită
100	eroare

Codurile de ieșire a căror valoare este mai mare decât 100 semnifică faptul că fișierul nu a fost scanat și, din acest motiv, este posibil să fie infectat.

ESET CMD

Aceasta este o caracteristică care activează comenzi ecmd avansate. Caracteristica vă permite să exportați și să importați setări utilizând linia de comandă (ecmd.exe). Până acum, setările puteau fi exportate doar prin intermediul GUI. ESET NOD32 Antivirus configurația poate fi exportată într-un fișier *.xml*.

Atunci când ați activat ESET CMD, sunt disponibile două metode de autorizare:

- **Niciuna** – nicio autorizare. Nu vă recomandăm această metodă deoarece permite importarea oricărei configurații nesemnate, fapt care constituie un potențial risc.

- **Parolă pentru setări avansate** – pentru importarea unei configurații dintr-un fișier .xml aveți nevoie de o parolă; fișierul trebuie să fie semnat, (consultați secțiunea Semnarea fișierelor de configurare .xml de mai jos). Înainte de a putea importa o configurație nouă va trebui să introduceți parola specificată în secțiunea Setare acces. Dacă nu aveți configurată setarea accesului, parola nu se potrivește sau fișierul de configurație .xml nu este semnat, configurația nu va fi importată.

După ce ați activat ESET CMD, puteți utiliza linia de comandă pentru a importa sau exporta configurații ESET NOD32 Antivirus. Puteți face acest lucru manual sau creând un script pentru automatizare.

Pentru a utiliza comenzi ecmd avansate, trebuie să le executați cu privilegii de administrator sau să deschideți linia de comandă Windows (cmd) utilizând **Run as administrator (Executare ca administrator)**. Altfel veți primi mesajul **Error executing command**. De asemenea, la exportarea unei configurații, trebuie să existe directorul de destinație. Comanda de exportare funcționează chiar dacă setările ESET CMD sunt dezactivate.

Comanda de exportare a setărilor:
`ecmd /getcfg c:\config\settings.xml`

Comanda de importare a setărilor:
`ecmd /setcfg c:\config\settings.xml`

Comenzile ecmd avansate pot fi executate doar local.

Semnarea unui fișier de configurație *.xml*:

1. Descărcați fișierul executabil XmlSignTool.

2. Deschideți linia de comandă Windows (cmd) utilizând **Run as administrator (Executare ca administrator)**.

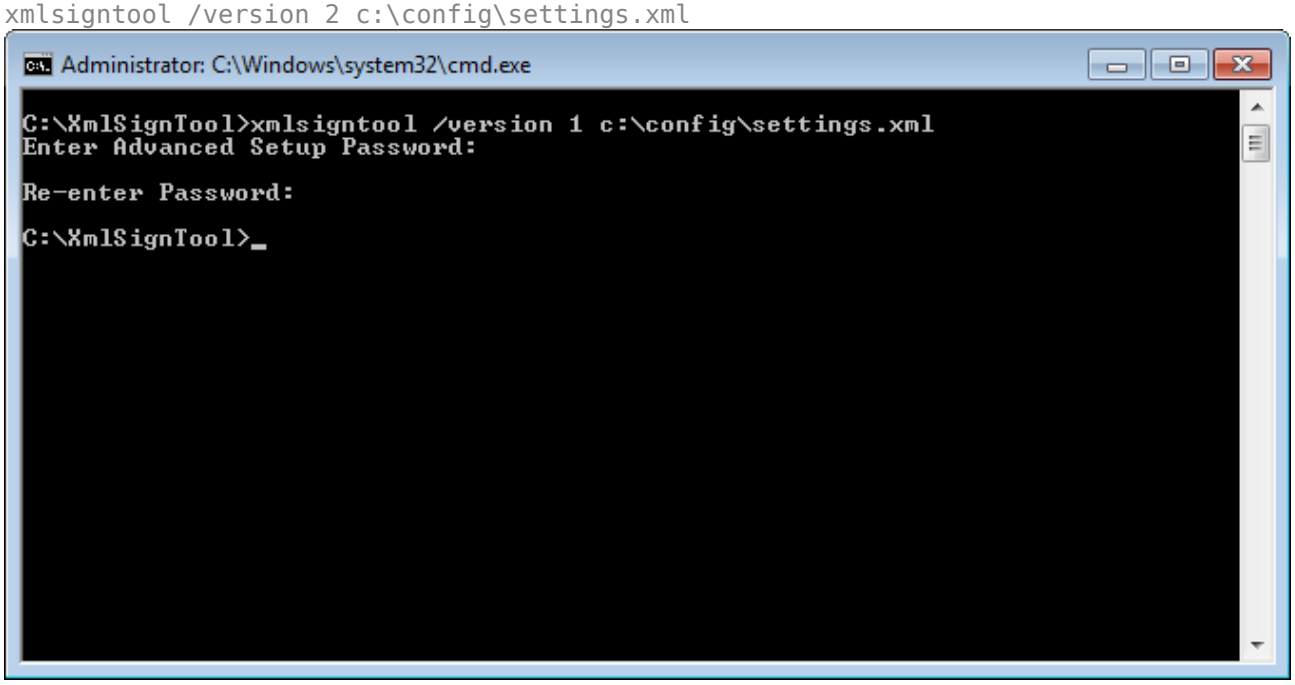
3. Navigați în locația de salvare `xmlsigntool.exe`

4. Executați o comandă de semnare a fișierului de configurație *.xml*, utilizare: `xmlsigntool /version 1|2 <xml_file_path>`

Valoarea parametrului `/version` depinde de versiunea ESET NOD32 Antivirus deținută de dvs. Utilizați `/version 1` pentru versiuni ale ESET NOD32 Antivirus anterioare 11.1. Utilizați `/version 2` pentru versiunea curentă a ESET NOD32 Antivirus.

5. Introduceți și reintroduceți parola pentru Setări avansate atunci când vă solicită XmlSignTool. Fișierul dvs. de configurație *.xml* este acum semnat și poate fi utilizat pentru importarea pe altă instanță a ESET NOD32 Antivirus cu ESET CMD folosind metoda de autorizare cu parolă.

Comanda de semnare a fișierului de configurație exportat:
`xmlsigntool /version 2 c:\config\settings.xml`



În cazul în care parola pentru Setare acces se modifică și doriți să importați configurația semnată anterior cu vechea parolă, va trebui să semnați din nou fișierul de configurație *.xml* cu parola curentă. Astfel, veți putea utiliza un fișier de configurație mai vechi, fără a-l exporta pe o altă mașină pe care rula ESET NOD32 Antivirus înainte de import.

Activarea ESET CMD fără o autorizare nu este recomandată deoarece astfel se va permite importarea oricărei configurații fără semnătură. Setați parola în **Setări avansate** > **Interfață utilizator** > **Setare acces** pentru a împiedica modificarea sa neautorizată de către utilizatori.

Detectare stare de inactivitate

Setările de detectare pentru starea de inactivitate pot fi configurate în **Setare avansată**, sub **Motor de detecție** > **Scanări malware** > **Scanare în stare de inactivitate** > **Detectare stare de inactivitate**. Aceste setări specifică un declanșator pentru Scanare în stare de inactivitate:

- **Ecran sau economizor de ecran dezactivat**
- **Blocare computer**
- **Deconectare utilizator**

Utilizați barele cu glisor corespunzătoare stărilor respective pentru a activa sau a dezactiva condițiile de declanșare a detectării stării de inactivitate.

Întrebări frecvente

Mai jos găsiți unele dintre întrebările frecvente și problemele întâmpinate. Faceți clic pe titlul subiectului pentru a afla cum să vă soluționați problema:

- Cum se actualizează ESET NOD32 Antivirus

- Cum se elimină un virus din PC
- Cum se creează o sarcină nouă în Orar
- Cum se planifică o sarcină de scanare (săptămânală)
- Cum deblocați secțiunea Setări avansate
- Cum se rezolvă dezactivarea produsului în ESET HOME

Dacă problema dvs. nu este inclusă în lista de mai sus, încercați să căutați în Ajutorul online al produsului ESET NOD32 Antivirus.

Dacă nu puteți găsi o soluție pentru problema/întrebare dvs. în Ajutorul online al produsului ESET NOD32 Antivirus, puteți vizita Baza de cunoştinţe ESET online, care este actualizată în mod regulat. Mai jos aveți la dispoziție legături către cele mai populare articole din Baza de cunoștințe:

- Cum îmi reînnoiesc licența?
- A apărut o eroare de activare la instalarea produsului meu ESET. Ce înseamnă acest lucru?
- Activarea produsului ESET Windows Home utilizând numele de utilizator, parola sau cheia de licență
- Dezinstalarea sau reinstalarea produsului ESET Home
- Am primit mesajul conform căruia instalarea ESET s-a încheiat prematur
- Ce trebuie să fac după ce reînnoiesc licența? (utilizatori domestici)
- Ce se întâmplă dacă îmi schimb adresa de email?
- Cum îmi transfer produsul ESET pe un computer sau pe un dispozitiv nou
- Cum pornesc Windows în modul de siguranță sau în modul de siguranță cu conectare la rețea
- Excluderea unui site web sigur, astfel încât acesta să nu fie blocat
- Se permite accesul software-ului cititoarelor de ecran la GUI-ul ESET

Dacă este cazul, puteți contacta Asistența tehnică pentru întrebări sau probleme.

Cum se actualizează ESET NOD32 Antivirus

Actualizarea ESET NOD32 Antivirus se poate efectua manual sau automat. Pentru a declanșa actualizarea, faceți clic pe **Actualizare** în fereastra principală a programului și apoi faceți clic pe **Căutare actualizări**.

Setările de instalare implicită creează o sarcină de actualizare automată care este efectuată în fiecare oră. Dacă doriți să modificați intervalul, navigați la **Instrumente** > **Orar**.

Cum se elimină un virus din PC

În cazul în care computerul prezintă simptome de infectare malware, de exemplu funcționează mai lent, deseori se blochează, vă recomandăm să efectuați următoarele:

1. În fereastra principală a programului, faceți clic pe **Scanare computer**.

2. Faceți clic pe **Scanați computerul** pentru a porni scanarea sistemului.

3. După finalizarea scanării, examinați logul care conține numărul de fișiere scanate, infectate și curățate.

4. Dacă doriți să scanați numai o anumită parte a discului dvs., faceți clic pe **Scanare personalizată** și selectați țintele ce urmează a fi scanate pentru detectarea virușilor.

Pentru informații suplimentare, consultați articolul din baza de cunoștințe ESET actualizat periodic.

Cum se creează o sarcină nouă în Orar

Pentru a crea o sarcină nouă în **Instrumente** > **Orar**, faceți clic pe **Adăugare** sau faceți clic dreapta și selectați **Adăugare** în meniul contextual. Sunt disponibile cinci tipuri de sarcini planificate:

- **Rulare aplicație externă** – Programează executarea unei aplicații externe.

- **Întreținere log** – fișierele log conțin și resturi din înregistrările șterse. Această sarcină optimizează regulat înregistrările din fișierele log pentru a funcționa mai eficient.

- **Verificare fișier la pornire sistem** – Verifică fișierele cărora li se permite executarea la pornirea sistemului sau la conectare.

- **Creați un instantaneu cu starea computerului** – Creează un instantaneu ESET SysInspector al computerului - adună informații detaliate despre componentele sistemului (de exemplu, drivere, aplicații) și evaluează nivelul de risc al fiecărei componente.

- **Scanare computer la cerere** – se efectuează o scanare a fișierelor și a directoarelor de pe calculator.

- **Actualizare** – planifică o sarcină Actualizare prin actualizarea modulelor.

Deoarece **Actualizare** este una dintre sarcinile planificate utilizată cel mai frecvent, vă vom explica mai jos modul de adăugare a unei sarcini de actualizare noi:

În meniul vertical **Sarcină programată**, selectați **Actualizare**. Introduceți numele sarcinii în câmpul **Nume sarcină** și faceți clic pe **Următorul**. Selectați frecvența de efectuare a sarcinii. Sunt disponibile următoarele opțiuni: **O dată**, **Repetat**, **Zilnic**, **Săptămânal** și **Declanșată de eveniment**. Selectați **Omitere sarcină când computerul funcționează pe baterie** pentru a minimiza utilizarea resurselor sistemului când un laptop funcționează alimentat de la baterie. Activitatea va fi executată la data și ora specificate în câmpurile **Executare sarcină**. În continuare, definiți acțiunea de efectuat în cazul în care sarcina nu poate fi efectuată sau finalizată la ora planificată. Sunt disponibile următoarele opțiuni:

- **La următoarea oră planificată**

- **Cât de curând posibil**

- **Imediat, dacă timpul scurs de la ultima executare depășește o valoare specificată** (intervalul poate fi definit utilizând caseta de desfășurare **Timp scurs de la ultima executare (ore)**).

În pasul următor se afișează o fereastră rezumativă cu informații despre sarcina planificată curentă. După ce terminați efectuarea modificărilor, faceți clic pe **Terminare**.

Se va afișa o fereastră de dialog care vă permite să alegeți profiluri de utilizat pentru sarcina planificată. Aici puteți seta profilul principal și profilul alternativ. Profilul alternativ se utilizează atunci când sarcina nu poate fi finalizată utilizându-se profilul principal. Confirmați făcând clic pe **Terminare** și sarcina planificată nouă va fi adăugată la lista de sarcini planificate curente.

Cum se programează o scanare săptămânală a computerului

Pentru a programa o sarcină regulată, deschideți fereastra principală a programului și faceți clic pe **Instrumente** > **Orar**. Mai jos găsiți un ghid succint pentru modul de programare a unei sarcini care va scana unitățile locale în fiecare săptămână. Consultați articolul din Baza de cunoștințe pentru instrucțiuni mai detaliate.

Pentru a planifica o sarcină de scanare:

1. Faceți clic pe **Adăugare** în ecranul principal al Orarului.

2. Introduceți un nume pentru activitate și selectați **Scanare computer la cerere** din meniul vertical **Tip de activitate.**

3. Selectați **Săptămânal** ca frecvență pentru activitate.

4. Setați data și ora la care se va executa sarcina.

5. Selectați **Execută sarcina cât de curând posibil** pentru a efectua sarcina ulterior, dacă sarcina planificată nu se execută dintr-un anumit motiv (de exemplu, computerul era oprit).

6. Examinați rezumatul sarcinii planificate și faceți clic pe **Finalizare**.

7. În meniul vertical **Ținte**, selectați **Unități locale**.

8. Faceți clic pe **Terminare** pentru a aplica sarcina.

Cum deblocați secțiunea Setări avansate protejată prin parolă

Când doriți să accesați secțiunea Setări avansate protejată prin parolă, se afișează fereastra pentru introducerea parolei. Dacă uitați sau pierdeți parola, faceți clic pe **Reinițializare parolă** și tastați adresa de email pe care ați folosit-o pentru înregistrarea licenței. ESET vă va trimite un e-mail cu codul de verificare. Tastați codul de verificare, apoi scrieți și confirmați noua parolă. Codul de verificare este valabil timp de șapte zile.

Restaurați parola prin intermediul contului ESET HOME – Folosiți această opțiune dacă licența utilizată pentru activare este asociată cu contul dvs. ESET HOME. Tastați adresa de e-mail pe care o folosiți pentru a vă conecta la contul dvs. ESET HOME.

Dacă ați uitat adresa de e-mail sau dacă întâmpinați dificultăți legate de restaurarea parolei, faceți clic pe **Contactați Asistența tehnică**. Veți fi redirecționat către site-ul web ESET, unde puteți contacta rapid departamentul de asistență tehnică.

Generare cod pentru Asistență tehnică – Această opțiune generează un cod pentru Asistența tehnică. Copiați codul furnizat de Asistența tehnică și faceți clic pe **Am un cod de verificare**. Tastați codul de verificare, apoi introduceți și confirmați noua parolă. Codul de verificare este valabil timp de șapte zile.

Pentru mai multe informații, consultați secțiunea Deblocarea parolei pentru setări în produsele ESET Windows destinate persoanelor fizice.

Cum se rezolvă dezactivarea produsului în ESET HOME

Produsul nu a fost activat

Acest mesaj de eroare apare atunci când proprietarul licenței dezactivează produsul dvs. ESET NOD32 Antivirus din portalul ESET HOME sau licența partajată cu contul dvs. ESET HOME nu mai este partajată. Pentru a rezolva această problemă:

- Faceți clic pe **Activare** și utilizați una dintre metodele de activare pentru a activa ESET NOD32 Antivirus.
- Contactați pe proprietarul licenței și informați-l că produsul dvs. ESET NOD32 Antivirus a fost dezactivat de proprietarul licenței sau licența nu mai este partajată cu dvs. Proprietarul poate rezolva problema în ESET HOME.

Produs dezactivat, dispozitiv deconectat

Acest mesaj de eroare apare după eliminarea unui dispozitiv din contul ESET HOME. Pentru a rezolva această problemă:

- Faceți clic pe **Activare** și utilizați una dintre metodele de activare pentru a activa ESET NOD32 Antivirus.
- Contactați pe proprietarul licenței și informați-l că ESET NOD32 Antivirus a fost dezactivat și dispozitivul a fost deconectat de la ESET HOME.
- Dacă sunteți proprietarul licenței și nu sunteți la curent cu aceste modificări, examinați Jurnalul de activități din ESET HOME. Dacă observați vreo activitate suspectă, schimbați-vă parola contului ESET HOME și contactați Asistența tehnică ESET.

Produs dezactivat, dispozitiv deconectat

Acest mesaj de eroare apare după eliminarea unui dispozitiv din contul ESET HOME. Pentru a rezolva această problemă:

- Faceți clic pe **Activare** și utilizați una dintre metodele de activare pentru a activa ESET NOD32 Antivirus.

• Contactați pe proprietarul licenței și informați-l că ESET NOD32 Antivirus a fost dezactivat și dispozitivul a fost deconectat de la ESET HOME.

• Dacă sunteți proprietarul licenței și nu sunteți la curent cu aceste modificări, examinați Jurnalul de activități din ESET HOME. Dacă observați vreo activitate suspectă, schimbați-vă parola contului ESET HOME și contactați Asistența tehnică ESET.

Produsul nu a fost activat

Acest mesaj de eroare apare atunci când proprietarul licenței dezactivează produsul dvs. ESET NOD32 Antivirus din portalul ESET HOME sau licența partajată cu contul dvs. ESET HOME nu mai este partajată. Pentru a rezolva această problemă:

• Faceți clic pe **Activare** și utilizați una dintre metodele de activare pentru a activa ESET NOD32 Antivirus.

• Contactați pe proprietarul licenței și informați-l că produsul dvs. ESET NOD32 Antivirus a fost dezactivat de proprietarul licenței sau licența nu mai este partajată cu dvs. Proprietarul poate rezolva problema în ESET HOME.

Programul de îmbunătățire a experienței clienților

Asociindu-vă la Programul de îmbunătățire a experienței clienților veți furniza ESET informații anonime privind utilizarea produselor noastre. Găsiți mai multe informații despre procesarea datelor în politica noastră de confidențialitate.

Consimţământul dvs.

Participarea la acest Program este voluntară și pentru ea este nevoie de consimțământul dvs. După ce vă asociați la acest program, participarea va avea un caracter pasiv, adică nu mai este nevoie de nicio altă acțiune din partea dvs. Vă puteți revoca oricând consimțământul modificând setările pentru produs. Dacă procedați astfel, nu vom mai procesa datele dvs. anonime.

Vă puteți revoca consimțământul oricând modificând setările pentru produs:

- Schimbarea setărilor Programului de îmbunătățire a experienței clienților în produsele ESET Windows Home

Ce tipuri de informaţii colectăm?

Date despre interacțiunile cu produsul

Aceste informații ne spun mai multe despre modul în care sunt folosite produsele noastre. Astfel putem afla, de exemplu, ce funcții sunt utilizate mai des, ce setări sunt modificate de utilizatori sau cât timp petrec folosind produsul.

Date despre dispozitive

Colectăm aceste informații pentru a înțelege unde și pe ce dispozitive sunt folosite produsele noastre. Exemple tipice includ modelul dispozitivului, țara, versiunea și numele sistemului de operare.

Date pentru diagnosticarea erorilor

Sunt colectate și informații despre erori și blocări. De exemplu, ce eroare s-a petrecut și ce acțiuni au condus la ea.

De ce colectăm aceste informații?

Aceste informații anonime ne ajută să ne îmbunătățim produsele, beneficiarul final fiind dvs., utilizatorul nostru. Aceste informații ne ajută să facem produse mai relevante, mai ușor de folosit și cu mai puține erori.

Cine controlează aceste informații?

ESET, spol. s r.o. este singura organizație care controlează datele colectate în cadrul acestui Program. Aceste informații nu sunt partajate cu terți.

Acord de licență pentru utilizatorul final

Data intrării în vigoare: 19 octombrie 2021.

IMPORTANT: Citiți cu atenție termenii și condițiile produsului stabilite mai jos înainte de descărcare, instalare, copiere sau utilizare. **PRIN DESCĂRCAREA, INSTALAREA, COPIEREA SAU UTILIZAREA SOFTWARE-ULUI VĂ EXPRIMAȚI ACORDUL PRIVIND TERMENII ȘI CONDIȚIILE ȘI CONFIRMAȚI POLITICA DE CONFIDENȚIALITATE.**

Acord de licență pentru utilizatorul final

Conform clauzelor acestui Acord de licență pentru utilizatorul final („Acord”) încheiat de și între ESET, spol. s r. o., societate cu sediul social în Einsteinova 24, 85101 Bratislava, Slovak Republic, înregistrată în Registrul Comerțului administrat de Judecătoria districtului Bratislava I, secția Sro, cu nr. de înregistrare 3586/B, cod fiscal 31333532 („ESET” sau „Furnizor”) și dvs., o persoană fizică sau o entitate legală („Dvs.” sau „Utilizatorul final”), aveți dreptul de a utiliza Software-ul definit la articolul 1 din acest Acord. Software-ul definit la articolul 1 din acest Acord poate fi stocat pe un suport de date, trimis prin poștă electronică, descărcat de pe internet, descărcat de pe serverele Furnizorului sau obținut din alte surse, sub rezerva respectării clauzelor și a condițiilor menționate mai jos.

ACESTA ESTE UN ACORD PRIVIND DREPTURILE UTILIZATORULUI FINAL, NU ESTE UN ACORD DE VÂNZARE. Furnizorul deține în continuare copia Software-ului și suportul fizic inclus în pachetul de vânzare și orice altă copie pe care Utilizatorul final are dreptul să o facă în conformitate cu acest Acord.

Făcând clic pe opțiunea „Accept” sau „Accept...” la instalarea, descărcarea, copierea sau utilizarea Software-ului, sunteți de acord cu clauzele și condițiile acestui Acord și luați la cunoștință dispozițiile din Politica de confidențialitate. Dacă nu sunteți de acord cu toate clauzele și condițiile din Acord și/sau cu Politica de confidențialitate, faceți clic imediat pe opțiunea de revocare, revocați instalarea sau descărcarea ori distrugeți sau returnați Software-ul, suportul de instalare, documentația însoțitoare și bonul de vânzare către Furnizor sau către magazinul de la care ați achiziționat Software-ul.

SUNTEȚI DE ACORD CĂ UTILIZAREA SOFTWARE-ULUI INDICĂ FAPTUL CĂ AȚI CITIT ACEST ACORD, L-AȚI ÎNȚELES ȘI SUNTEȚI DE ACORD SĂ RESPECTAȚI TERMENII ȘI CONDIȚIILE ACESTUIA.

1. **Software-ul.** Conform utilizării în prezentul Acord, termenul „Software” înseamnă: (i) programul informatic care însoțește prezentul Acord și toate componentele acestuia; (ii) întregul conținut al discurilor, CD-ROM-urilor, DVD-urilor, mesajelor de e-mail și atașărilor sau alt suport cu care este prevăzut acest Acord, inclusiv forma codului obiect al Software-ului furnizat pe un suport de date, prin poștă electronică sau descărcat de pe Internet;

(iii) orice material explicativ scris asociat și orice altă eventuală documentație asociată Software-ului, mai ales orice descriere a Software-ului, specificațiile acestuia, orice descriere a proprietăților și funcționării Software-ului, orice descriere a mediului de funcționare în care se utilizează Software-ul, instrucțiunile de utilizare sau instalare a Software-ului sau orice descriere a modului de utilizare a Software-ului („Documentație"); (iv) copiile Software-ului, corecțiile eventualelor erori ale Software-ului, adăugirile aduse Software-ului, extensiile Software-ului, versiunile modificate ale Software-ului și actualizările componentelor Software-ului, dacă există, care vă sunt acordate prin licență de către Furnizor în conformitate cu articolul 3 din acest Acord. Software-ul se va furniza exclusiv sub formă de cod de obiect executabil.

2. **Instalarea, computerul și cheie de licență**. Software-ul furnizat pe un suport de date, trimis prin poștă electronică, descărcat de pe internet, descărcat de pe serverele Furnizorului sau obținut din alte surse necesită instalare. Trebuie să instalați Software-ul pe un Computer configurat corect, care respectă cel puțin cerințele prevăzute în Documentație. Metodologia de instalare este descrisă în Documentație. Pe Computerul pe care instalați Software-ul nu trebuie instalate programe de computer sau hardware care pot avea un efect advers asupra Software-ului. Computer înseamnă hardware, inclusiv, dar fără a se limita la computere personale, laptopuri, stații de lucru, computere palmtop, telefoane inteligente, dispozitive electronice portabile sau alte dispozitive electronice pentru care este conceput Software-ul, pe care acesta va fi instalat și/sau utilizat. Cheie de licență înseamnă o secvență unică de simboluri, de litere, de cifre sau de semne speciale furnizate Utilizatorului final pentru a permite utilizarea legală a Software-ului, versiunea sa specifică sau o prelungire a perioadei Licenței în conformitate cu acest Acord.

3. **Licență**. În condițiile în care ați fost de acord cu termenii acestui Acord și respectați toți termenii și toate condițiile stipulate aici, Furnizorul vă va acorda următoarele drepturi („Licența"):

a) **Instalare și utilizare.** Aveți dreptul neexclusiv și netransferabil de instalare a Software-ului pe hard diskul calculatorului sau pe alt suport permanent de stocare a datelor, de instalare și stocare a Software-ului în memoria unui sistem de calculator și de implementare, stocare și afișare a Software-ului.

b) **Stipularea numărului de licențe.** Dreptul de utilizare a Software-ului depinde de numărul de Utilizatori finali. Un Utilizator final înseamnă următoarele: (i) instalarea Software-ului pe un singur sistem de computer sau, (ii) dacă întinderea licenței este limitată de numărul de căsuțe poștale, atunci un Utilizator final înseamnă un utilizator de calculator care acceptă poștă electronică prin Mail User Agent („MUA"). Dacă MUA acceptă poștă electronică și o distribuie ulterior automat către mai mulți utilizatori, atunci numărul de Utilizatori finali se va stabili în funcție de numărul efectiv de utilizatori pentru care se distribuie poșta electronică. Dacă un server de mail funcționează ca poartă poștală, numărul de Utilizatori finali va fi egal cu numărul utilizatorilor de servere de mail pentru care o astfel de poartă oferă servicii. Dacă un număr nespecificat de adrese de poștă electronică sunt direcționate către și acceptate de un utilizator (de ex., prin denumiri alternative) și mesajele nu sunt distribuite automat de client către un număr mai mare de utilizatori, se va solicita o Licență pentru un calculator. Nu se va utiliza simultan aceeași Licență pe mai multe calculatoare. Utilizatorul final are dreptul de a introduce cheia de Licență în Software doar în măsura în care Utilizatorul final are dreptul de a utiliza Software-ul în conformitate cu limitările care decurg din numărul de Licențe acordate de Furnizor. Cheia de Licență este considerată a fi confidențială, iar Dvs. nu trebuie să partajați Licența cu terții sau să permiteți terților să utilizeze cheia de Licență decât dacă acest Acord sau Furnizorul permite acest lucru. În cazul în care este compromisă cheia de Licență, notificați imediat Furnizorul.

c) **Home/Business Edition.** O versiune Home Edition a Software-ului va fi utilizată exclusiv în medii private și/sau necomerciale, doar pentru uz rezidențial și în cadrul familiei. Pentru a utiliza Software-ul pe servere de poștă electronică, servere de transmitere a poștei electronice, gateway-uri de corespondență sau de Internet trebuie să obțineți versiunea Business Edition a Software-ului destinată utilizării într-un mediu comercial.

d) **Termenul Licenței.** Dreptul Dvs. de a utiliza Software-ul va fi pe durată limitată.

e) **Software OEM.** Software-ul clasificat drept „OEM” va fi limitat la Computerul pe care l-ați obținut. Nu se poate transfera pe un alt calculator.

f) **NFR, Software de ÎNCERCARE.** Software-ul clasificat ca „Nu este destinat revânzării”, NFR sau ÎNCERCARE nu poate fi supus plății și se poate utiliza numai în scop demonstrativ sau pentru testarea caracteristicilor Software-ului.

g) **Încetarea Licenței.** Licența va înceta automat la sfârșitul perioadei pentru care a fost acordată. Dacă nu respectați prevederile Acordului, Furnizorul va avea dreptul de a se retrage din Acord, fără a prejudicia drepturile sau daunele legale ce pot fi pretinse Furnizorului într-o astfel de eventualitate. În cazul anulării Licenței, trebuie să ștergeți, distrugeți sau returnați imediat Software-ul și toate copiile de rezervă, suportând costurile, către ESET sau către partenerul de la care ați obținut Software-ul. La încetarea Licenței, Furnizorul va mai avea dreptul să anuleze dreptul Utilizatorului final de a folosi funcțiile Software-ului, ceea ce necesită conectarea la serverele Furnizorului sau la serverele terțe.

4. **Cerințe privind funcțiile care necesită colectarea datelor și conexiunea la internet.** Pentru a funcționa corect, Software-ul necesită conectare la internet și trebuie să se conecteze la intervale regulate la serverele Furnizorului sau la servere terțe și la opțiuni aplicabile de colectare a datelor în conformitate cu Politica de confidențialitate. Conexiunea la internet și opțiunile aplicabile de colectare a datelor sunt necesare pentru următoarele funcții ale Software-ului:

a) **Actualizări de Software.** Furnizorul va avea dreptul să publice din timp actualizări sau upgrade-uri ale Software-ului („Actualizări”), dar nu este obligat să furnizeze Actualizări. Această funcție se activează în setările standard ale Software-ului, iar Actualizările se instalează automat dacă Utilizatorul final nu a dezactivat instalarea automată a Actualizărilor. Pentru furnizarea de Actualizări este necesară verificarea autenticității Licenței, inclusiv informații despre Computer și/sau platforma pe care este instalat Software-ul în conformitate cu Politica de confidențialitate.

Furnizarea oricăror actualizări poate face obiectul Politicii privind sfârșitul ciclului de viață („Politica EOL”), care este disponibilă la adresa https://go.eset.com/eol_home. Nu se va mai furniza nicio Actualizare după ce Software-ul sau oricare dintre funcțiile sale ajunge la sfârșitul ciclului de viață definit în Politica EOL.

b) **Redirecționarea infiltrărilor și informațiilor către Furnizor.** Software-ul conține funcții care colectează mostre ale virușilor de computer și ale altor programe de computer rău intenționate și ale obiectelor suspecte, problematice, potențial nedorite sau potențial nesigure, cum ar fi fișiere, adrese URL, pachete IP și cadre ethernet („Infiltrări”) și pe care le trimite apoi Furnizorului, inclusiv, dar fără a se limita la informații despre procesul de instalare, despre Computerul și/ori platforma pe care este instalat Software-ul, informații despre operațiunile și funcționalitatea Software-ului („Informații”). Informațiile și Infiltrările pot conține date (inclusiv date cu caracter personal obținute aleatoriu sau întâmplător) despre Utilizatorul final ori despre alți utilizatori ai computerului pe care este instalat Software-ul și despre fișierele afectate de Infiltrări cu metadatele asociate.

Informațiile și Infiltrările pot fi colectate cu următoarele funcții ale Software-ului:

i. Funcția sistemului de reputație LiveGrid include colectarea și trimiterea codurilor hash într-o singură direcție legate de Infiltrări către Furnizor. Această funcție este activată în setările standard ale Software-ului.

ii. Funcția Sistem de feedback LiveGrid include colectarea și transmiterea de Infiltrări cu metadate asociate și de Informații către Furnizor. Această funcție poate fi activată de Utilizatorul final în timpul procesului de instalare a Software-ului.

Furnizorul va utiliza Informațiile și Infiltrările primite doar în scop de analiză și cercetare a Infiltrărilor, de îmbunătățire a Software-ului și de verificare a autenticității Licenței și va lua măsurile corespunzătoare pentru a se asigura că Infiltrările și Informațiile primite rămân securizate. Prin activarea acestei funcții a Software-ului,

Infiltrările și Informațiile pot fi colectate și procesate de către Furnizor conform celor specificate în Politica de confidențialitate și în conformitate cu reglementările legale relevante. Puteți dezactiva aceste funcții în orice moment.

În sensul acestui Acord, este necesar să se colecteze, să se proceseze și să se stocheze date care permit Furnizorului să vă identifice în conformitate cu Politica de confidențialitate. Prin prezenta, sunteți de acord ca Furnizorul să efectueze verificări prin propriile mijloace cu privire la utilizarea de către Dvs. a Software-ului în conformitate cu prevederile acestui Acord. Prin prezenta, sunteți de acord că, în sensul acestui Acord, este necesar ca datele dvs. să fie transferate, în timpul comunicării dintre Software și sistemele informatice ale Furnizorului sau cele ale partenerilor săi de afaceri ca parte a rețelei de asistență și de distribuție a Furnizorului, pentru a asigura funcționalitatea Software-ului și autorizația de utilizare a Software-ului și pentru protecția drepturilor Furnizorului.

În urma încheierii acestui Acord, Furnizorul sau oricare dintre partenerii săi de afaceri ca parte a rețelei de asistență și de distribuție a Furnizorului va avea dreptul de a transfera, a procesa și a stoca date esențiale care vă identifică în scopul facturării, al executării obligațiilor din Acord și al transmiterii notificărilor pe Computerul dvs.

Detalii privind confidențialitatea, protecția datelor cu caracter personal și drepturile dvs. ca persoană vizată se găsesc în Politica de confidențialitate, care este disponibilă pe site-ul web al furnizorului, precum și direct din procesul de instalare. De asemenea, o puteți accesa prin secțiunea de ajutor a software-ului.

5. **Exercitarea drepturilor Utilizatorului final**. Trebuie să vă exercitați drepturile de Utilizator final personal sau prin intermediul angajaților dvs. Aveți dreptul de a utiliza Software-ul numai pentru a proteja operațiunile și Computerele sau sistemele de computer pentru care ați obținut Licență.

6. **Restricționarea drepturilor.** Nu puteți copia, distribui, extrage componente sau efectua lucrări derivate din Software. Când utilizați Software-ul, aveți obligația de a respecta următoarele restricții:

a) Efectuați o singură copie a Software-ului pe un suport de stocare permanent sub formă de copie de rezervă arhivată, cu condiția ca respectiva copie de rezervă arhivată să nu fie instalată sau utilizată pe un calculator. Orice altă copie de Software efectuată se va considera o încălcare a acestui Acord.

b) Nu puteți utiliza, modifica, traduce, reproduce sau transfera drepturile de utilizare a Software-ului sau a copiilor Software-ului sub nicio altă formă decât cea stabilită în mod expres în acest Acord.

c) Nu puteți vinde, sublicenția, închiria sau împrumuta Software-ul sau utiliza Software-ul în scopuri comerciale.

d) Nu puteți reface programul sursă, decompila sau dezasambla Software-ul şi nu puteți încerca să descoperiți codul sursă al Software-ului, cu excepția cazului în care această restricție este interzisă prin lege.

e) Sunteți de acord să utilizați Software-ul numai respectând toate legile în vigoare din jurisdicția în care utilizați Software-ul, inclusiv, dar fără a se limita la acestea, restricțiile în vigoare privind drepturile de autor şi alte drepturi de proprietate intelectuală.

f) Sunteți de acord să utilizați Software-ul şi funcțiile sale astfel încât să nu limitați capacitatea altor Utilizatori finali de a accesa aceste servicii. Furnizorul își rezervă dreptul de a limita domeniul serviciilor oferite fiecărui Utilizator final în parte pentru a permite utilizarea serviciilor de către un număr maxim de Utilizatori finali. Limitarea domeniului serviciilor va mai însemna terminarea definitivă a posibilității de utilizare a funcțiilor Software-ului și ștergerea Datelor și informațiilor de pe serverele Furnizorului sau de pe serverele părților terțe legate de o anumită funcția a Software-ului.

g) Sunteți de acord să nu desfășurați niciun fel de activități care implică utilizarea cheii de Licență și care sunt contrare clauzelor acestui Acord sau care conduc la furnizarea cheii de Licență către o persoană care nu are

dreptul de a utiliza Software-ul, cum ar fi transferul sub orice formă al unei chei de Licență utilizate sau neutilizate, precum și reproducerea sau distribuirea neautorizată a unor chei de Licență generate sau duplicat ori utilizarea Software-ului ca rezultat al utilizării unei chei de Licență obținute din alte surse decât de la Furnizor.

7. **Drept de autor**. Software-ul și toate drepturile, fără limitare și incluzând drepturile de deținere și drepturile de proprietate intelectuală sunt deținute de ESET și/sau licențiatorii săi. Acestea sunt protejate prin prevederile tratatelor internaționale și prin toate celelalte legi naționale în vigoare în țara în care este utilizat Software-ul. Structura, organizarea și codul Software-ului se constituie în secrete de firmă și informații confidențiale ale ESET și/sau ale licențiatorilor săi. Nu puteți copia Software-ul, cu excepția specificată în articolul 6 (a). Orice copie pe care aveți dreptul să o efectuați conform acestui Acord trebuie să conțină aceleași drepturi de autor și alte notificări privind proprietatea conținute în Software. Dacă refaceți programul sursă, îl decompilați sau îl dezasamblați sau încercați să descoperiți codul sursă al Software-ului, încălcând prevederile acestui Acord, sunteți de acord prin prezentul Acord că orice informație astfel obținută va fi transferată în întregime Furnizorului şi va fi considerată automat şi irevocabil deținută de Furnizor, din momentul obținerii informației respective; aceasta nu va afecta drepturile Furnizorului referitoare la încălcarea Acordului.

8. **Rezervarea drepturilor**. Prin acest Acord, Furnizorul își rezervă toate drepturile asupra Software-ului, cu excepția drepturilor acordate Dvs. în mod expres prin termenii acestui Acord, în calitate de Utilizator final al Software-ului.

9. **Mai multe versiuni lingvistice, software pe suport dual, mai multe copii**. În cazul în care Software-ul acceptă mai multe limbi sau platforme sau dacă primiți mai multe copii ale Software-ului, puteți utiliza Software-ul numai pentru numărul de sisteme de calculatoare și pentru versiunile pentru care ați obținut Licența. Nu puteți vinde, închiria, sublicența, împrumuta sau transfera versiuni sau copii ale Software-ului pe care nu le utilizați.

10. **Intrarea în vigoare şi încetarea Acordului.** Acest Acord intră în vigoare de la data la care Dvs. sunteți de acord cu termenii Acordului. Puteți înceta oricând acest Acord prin dezinstalarea, distrugerea sau returnarea permanentă, suportând costurile, a Software-ului, a tuturor copiilor de rezervă și a tuturor materialelor asociate furnizate de Furnizor sau de partenerii săi de afaceri. Dreptul dvs. de a utiliza Software-ul și oricare dintre funcțiile sale pot fi supuse Politicii EOL. După ce Software-ul sau oricare dintre funcțiile sale ajunge la sfârșitul ciclului de viață definit în Politica EOL, dreptul dvs. de a utiliza Software-ul va înceta. Indiferent de modul de încetare a acestui Acord, prevederile articolelor 7, 8, 11, 13, 19 și 21 se vor aplica în continuare pentru o perioadă nelimitată.

11. **DECLARAȚIILE UTILIZATORULUI FINAL**. ÎN CALITATE DE UTILIZATOR FINAL, AȚI LUAT LA CUNȘTINȚĂ CĂ SOFTWARE-UL SE FURNIZEAZĂ „CA ATARE”, FĂRĂ NICIUN FEL DE GARANȚIE, EXPRESĂ SAU IMPLICITĂ, ÎN LIMITELE PERMISE DE LEGISLAȚIA ÎN VIGOARE. FURNIZORUL, LICENȚIATORII SĂI, PARTENERII SAU DEȚINĂTORII DREPTURILOR DE AUTOR NU POT ACORDA REPREZENTARE SAU GARANȚII, EXPRESE SAU IMPLICITE, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA ACESTEA, GARANȚIILE DE COMERCIALIZARE SAU DE ADECVARE LA UN ANUMIT SCOP ȘI NU POT GARANTA CĂ SOFTWARE-UL NU VA ÎNCĂLCA BREVETE, DREPTURI DE AUTOR, MĂRCI COMERCIALE SAU ALTE DREPTURI ALE UNOR TERȚI. NU EXISTĂ NICIO GARANȚIE DIN PARTEA FURNIZORULUI SAU A ALTEI PĂRȚI CĂ FUNCȚIILE CONȚINUTE ÎN SOFTWARE VOR SATISFACE CERINȚELE DVS. SAU CĂ FUNCȚIONAREA SOFTWARE-ULUI VA FI NEÎNTRERUPTĂ SAU LIPSITĂ DE ERORI. VĂ ASUMAȚI ÎNTREAGA RESPONSABILITATE ȘI RISCURILE PENTRU ALEGEREA SOFTWARE-ULUI CU SCOPUL DE A OBȚINE REZULTATELE SCONTATE ȘI PENTRU INSTALAREA, UTILIZAREA ȘI REZULTATELE OBȚINUTE DE PE URMA ACESTUIA.

12. **Lipsa altor obligații**. Acest Acord nu creează alte obligații din partea Furnizorului și a licențiatorilor săi în afara celor specificate aici.

13. **LIMITAREA RĂSPUNDERII**. ÎN LIMITA MAXIMĂ PERMISĂ PRIN LEGILE ÎN VIGOARE FURNIZORUL, ANGAJAȚII SAU LICENȚIATORII SĂI NU VOR FI CONSIDERAȚI ÎN NICIUN CAZ RĂSPUNZĂTORI PENTRU NICIUN FEL DE PIERDERE DE PROFIT, BENEFICII, VÂNZĂRI, PIERDERI DE DATE, COSTURI PENTRU A PROCURA PIESE DE SCHIMB SAU SERVICII, DAUNE ADUSE PROPRIETĂȚII, DAUNE PERSONALE, RĂNIRI, ÎNTRERUPEREA ACTIVITĂȚII, PIERDEREA DE

INFORMAȚII DE AFACERI SAU PENTRU ORICE DAUNĂ SPECIALĂ, DIRECTĂ, INDIRECTĂ, ACCIDENTALĂ, ECONOMICĂ, ASIGURATĂ, PENALĂ, SPECIALĂ SAU ULTERIOARĂ CAUZATĂ PRIN ORICE MIJLOACE, INDIFERENT DACĂ A REZULTAT DINTR-UN CONTRACT, DIN PROASTĂ ADMINISTRARE VOITĂ, DIN NEGLIJENȚĂ SAU DIN ALTĂ FAPTĂ CE ATRAGE DUPĂ SINE ASUMAREA RESPONSABILITĂȚII, APĂRUTĂ DATORITĂ INSTALĂRII, UTILIZĂRII SAU IMPOSIBILITĂȚII DE A UTILIZA SOFTWARE-UL, CHIAR ȘI ÎN CAZUL ÎN CARE FURNIZORUL SAU LICENȚIATORII SĂI AU FOST NOTIFICAȚI DESPRE POSIBILITATEA UNEI ASTFEL DE DAUNE. DEOARECE UNELE ȚĂRI ȘI JURISDICȚII NU PERMIT EXCLUDEREA RĂSPUNDERII, DAR POT PERMITE LIMITAREA RĂSPUNDERII, ÎN ASTFEL DE CAZURI RĂSPUNDEREA FURNIZORULUI, A ANGAJAȚILOR, A LICENȚIATORILOR SAU A PARTENERILOR SĂI SE VA LIMITA LA SUMA PLĂTITĂ DE DVS. PENTRU LICENȚĂ.

14. Nimic din acest Acord nu va prejudicia drepturile statutare ale părților în calitate de consumator dacă intră în conflict cu cele prevăzute.

15. **Asistența tehnică**. ESET sau părțile terțe împuternicite de ESET vor asigura asistența tehnică conform propriilor decizii, fără garanții sau declarații. Nu se va mai furniza asistență tehnică după ce Software-ul sau oricare dintre funcțiile sale ajunge la sfârșitul ciclului de viață definit în Politica EOL. Utilizatorul final i se solicită să efectueze copia de rezervă a tuturor datelor existente, a software-ului și a componentelor programului înainte de asigurarea asistenței tehnice. ESET și/sau părțile terțe împuternicite de ESET nu pot accepta răspunderea pentru pierderea datelor, proprietății, software-ului sau hardware-ului sau pierderea profitului din cauza asigurării asistenței tehnice. ESET și/sau părțile terțe împuternicite de ESET își rezervă dreptul de a decide dacă rezolvarea problemei depășește domeniul asistenței tehnice. ESET își rezervă dreptul de a refuza, suspenda sau înceta asigurarea asistenței tehnice conform propriilor decizii. Este posibil să fie necesare informațiile Licenței, Informații și alte date în conformitate cu Politica de confidențialitate, în scopul furnizării serviciilor de asistență tehnică.

16. **Transferarea Licenței**. Software-ul se poate transfera de pe un calculator pe altul dacă nu contravine termenilor Acordului. Dacă nu contravine termenilor Acordului, Utilizatorul final va avea numai dreptul de a transfera permanent Licența și toate drepturile care decurg din acest Acord altui Utilizator final cu aprobarea Furnizorului, respectând condiția ca (i) Utilizatorul final inițial să nu rețină nicio copie a Software-ului; (ii) transferarea drepturilor trebuie să fie directă, adică de la Utilizatorul final inițial la Utilizatorul final nou; (iii) Utilizatorul final nou trebuie să preia toate drepturile și obligațiile deținute de Utilizatorul final inițial conform termenilor acestui Acord; (iv) Utilizatorul final inițial trebuie să furnizeze Utilizatorului final nou documentația care-i permite verificarea autenticității Software-ului, conform specificațiilor de la articolul 17.

17. **Verificarea autenticității Software-ului.** Utilizatorul final poate demonstra dreptul de a utiliza Software-ul printr-una dintre următoarele modalități: (i) printr-un certificat de licență emis de Furnizor sau de un terț numit de Furnizor; (ii) printr-un acord de licență scris, dacă s-a încheiat un astfel de acord; (iii) prin trimiterea unui mesaj de e-mail către Furnizor conținând detaliile licenței (numele de utilizator și parola). Este posibil să fie necesare informațiile Licenței și datele de identificare a Utilizatorului final în conformitate cu Politica de confidențialitate, în scopul verificării autenticității Software-ului.

18. **Licențierea pentru autorități publice și guvernul S.U.A**. Software-ul se va furniza autorităților publice, inclusiv guvernului S.U.A., drepturile de licență și restricțiile descrise în acest Acord.

19. **Conformarea pentru controalele comerciale**.

a) Nu veți exporta, re-exporta, transfera sau face într-un alt mod disponibil, în mod direct sau indirect, Software-ul către nicio persoană și nu îl veți utiliza și nu veți fi implicat în nicio acțiune care ar putea avea drept rezultat încălcarea de către ESET sau de către companiile din holding, filialele și filialele companiilor din holding, precum și de către entitățile controlate de către companiile din holding („Afiliați”) a legislației referitoare la controalele comerciale sau expunerea la eventuale consecințe negative ale acestei legislații, care include

i. toate legile care controlează, restricționează sau impun cerințe de licențiere pentru exportul, re-exportul sau transferul bunurilor, software-ului, tehnologiei sau serviciilor, emise sau adoptate de orice guvern, stat sau

autoritate de reglementare din Statele Unite ale Americii, Singapore, Marea Britanie, Uniunea Europeană sau oricare dintre Statele Membre ale acesteia sau orice altă țară în care trebuie îndeplinite obligații în baza Acordului sau în care ESET sau oricare dintre Afiliații săi este înregistrată sau își desfășoară activitatea și

ii. orice sancțiune, restricție, embargo, interdicție de import sau de export, interdicție privind transferul de fonduri sau de active sau de prestare a serviciilor sau orice altă măsură echivalentă de natură economică, financiară, comercială sau de altă natură, emisă sau adoptată de orice guvern, stat sau autoritate de reglementare din Statele Unite ale Americii, Singapore, Marea Britanie, Uniunea Europeană sau oricare dintre Statele Membre ale acesteia sau orice altă țară în care trebuie îndeplinite obligații în baza Acordului sau în care ESET sau oricare dintre Afiliații săi este înregistrată sau își desfășoară activitatea.

(actele juridice menționate la punctele i și ii de mai sus poartă în mod colectiv denumirea de „Legi privind controlul comercial").

b) ESET are dreptul de a-și suspenda obligațiile sau de a încheia acești Termeni cu efect imediat în cazul în care:

i. ESET determină faptul că, în opinia sa rezonabilă, Utilizatorul a încălcat sau probabil va încălca Articolul 19 a) din Acord; sau

ii. Utilizatorul final și/sau Software-ul devine subiect al Legilor privind controalele comerciale și, ca urmare, ESET determină faptul că, în opinia sa rezonabilă, continuarea îndeplinirii obligațiilor din baza Acordului ar avea drept rezultat ca ESET sau Afiliații săi să se găsească în postura de a încălca sau de a fi supuși unor consecințe negative ale Legilor privind controalele comerciale.

c) Nicio prevedere din acest Acord nu are scopul și nu trebuie să fie interpretată sau argumentată precum că ar induce sau ar necesita ca o altă parte să acționeze sau să nu acționeze (sau să fie de acord să acționeze sau să nu acționeze) într-o manieră care să nu fie de acord, să fie penalizată sau interzisă de către Legile privind controalele comerciale aplicabile.

20. **Înștiințări**. Toate înștiințările și retururile de Software și Documentație trebuie trimise către: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, fără a aduce atingere dreptului ESET de a vă comunica orice modificare a prezentului Acord, a Politicilor de confidențialitate, a Politicii EOL și a Documentației în conformitate cu art. 22 al Acordului. ESET poate să vă trimită e-mailuri, notificări în aplicație prin intermediul Software-ului sau să posteze comunicările pe site-ul nostru web. Sunteți de acord să primiți comunicări legale de la ESET în format electronic, inclusiv comunicări privind modificarea Condițiilor, a Condițiilor speciale sau a Politicilor de confidențialitate, orice propunere/acceptare contractuală sau invitații în acest sens, notificări sau alte comunicări legale. O astfel de comunicare electronică va fi considerată ca fiind primită în scris, cu excepția cazului în care o altă formă de comunicare este cerută în mod explicit în legislația aplicabilă.

21. **Legislația în vigoare**. Prezentul Acord este reglementat și interpretat în conformitate cu legile din Republica Slovacă. Prin prezenta, Utilizatorul final și Furnizorul sunt de acord că principiile conflictuale ale legislației și cele ale Convenției Națiunilor Unite privind Contractele Internaționale pentru Comercializarea Bunurilor nu se aplică. Sunteți de acord, în mod expres, că orice conflict sau reclamație care decurge din acest Acord privitoare la Furnizor sau orice conflict sau reclamație legată de utilizarea Software-ului va fi rezolvată de Judecătoria 1 din Bratislava și vă exprimați, în mod expres, acordul pentru exercitarea jurisdicției judecătoriei respective.

22. **Prevederi generale**. Dacă o prevedere din acest Acord nu este valabilă sau nu se poate aplica, acesta nu va afecta valabilitatea altor prevederi din Acord, care va rămâne valabil și în vigoare conform condițiilor stipulate aici. Acest Acord a fost executat în limba engleză. În cazul în care o traducere a Acordului este elaborată pentru comoditatea utilizatorului sau pentru orice alt scop sau în cazul unor diferențe între versiunile în limbi diferite ale acestui Acord, versiunea în limba engleza va prevala.

ESET își rezervă dreptul de a aduce modificări Software-ului, precum și de a revizui condițiile prezentului acord,

anexele sale, Politica de confidențialitate, Politica EOL și documentația sau orice parte a acestora, în orice moment, prin actualizarea documentului relevant (i) pentru a reflecta modificările aduse Software-ului sau modului în care ESET își desfășoară activitatea, (ii) din motive legale, de reglementare sau de securitate sau (iii) pentru a preveni abuzul sau conținutul inadecvat. Veți fi înștiințat asupra oricărei modificări ale Acordului prin e-mail, notificare în aplicație sau alte mijloace electronice. Dacă nu sunteți de acord cu modificările propuse ale Acordului, îl puteți rezilia în conformitate cu art. 10 în termen de 30 de zile de la primirea unei notificări privind modificarea. Cu excepția cazului în care reziliați acordul în acest termen, modificările propuse vor fi considerate acceptate și vor deveni executorii în relația cu dvs. începând cu data la care ați primit notificarea privind modificarea.

Acesta este Acordul în întregime încheiat între Furnizor și Dvs. cu privire la Software și înlocuiește orice reprezentare, discuție, întreprindere, comunicare sau anunț anterior cu privire la Software.

ANEXĂ LA ACORD

Evaluarea securității dispozitivelor conectate la rețea. Dispoziții suplimentare se aplică în cazul evaluării securității dispozitivelor conectate la rețea, după cum urmează:

Software-ul include o funcție pentru verificarea securității rețelei locale a Utilizatorului final și a securității dispozitivelor din rețeaua locală, funcție pentru care este nevoie de numele rețelei locale și de informații despre dispozitivele din rețeaua locală, cum ar fi prezență, tip, nume, adresă IP și adresă MAC a dispozitivului în rețeaua locală, împreună cu informațiile despre licență. Informațiile includ tipul de securitate wireless și tipul de criptare wireless pentru dispozitivele ruter. Această funcție poate oferi și informații despre disponibilitatea unei soluții software de securitate pentru securizarea dispozitivelor din rețea.

Protecția împotriva utilizării necorespunzătoare a datelor. Dispoziții suplimentare se aplică în cazul protecției împotriva utilizării necorespunzătoare a datelor, după cum urmează:

Software-ul conține o funcție care previne pierderea sau utilizarea necorespunzătoare a datelor critice în legătură directă cu furtul unui Computer. Această funcție este dezactivată în setările implicite ale Software-ului. Contul ESET HOME trebuie creat pentru a fi activat, iar prin acesta funcția activează colectarea datelor în cazul furtului computerului. Dacă alegeți să activați această funcție a Software-ului, datele despre Computerul furat vor fi colectate și trimise Furnizorului, iar acestea pot include date despre localizarea rețelei Computerului, date despre conținutul afișat pe ecranul Computerului, date despre configurația Computerului și/sau date înregistrate de o cameră conectată la Computer (denumite în continuare „Date”). Utilizatorul final va avea dreptul de a utiliza Datele obținute de această funcție și furnizate prin Contul ESET HOME exclusiv pentru a remedia o situație adversă cauzată de furtul Computerului. Exclusiv în acest scop, Furnizorul procesează Datele conform celor specificate în Politica de confidențialitate și în conformitate cu reglementările legale relevante. Furnizorul va permite Utilizatorului final să acceseze Datele pentru perioada necesară atingerii scopului pentru care au fost obținute datele, care nu va depăși perioada de păstrare specificată în Politica de confidențialitate. Protecția împotriva utilizării necorespunzătoare a datelor va fi utilizată exclusiv pentru Computerele și conturile la care Utilizatorul final are acces legitim. Orice utilizare ilegală va fi raportată autorităților competente. Furnizorul va respecta legislația relevantă și va ajuta autoritățile de aplicare a legii în cazul utilizării necorespunzătoare. Sunteți de acord și recunoașteți că Dvs. sunteți responsabil pentru păstrarea în siguranță a parolei pentru accesarea Contului ESET HOME și sunteți de acord că nu veți divulga parola niciunui terț. Utilizatorul final este responsabil pentru orice activitate care utilizează funcția Protecție împotriva utilizării necorespunzătoare a datelor și Contul ESET HOME, în mod autorizat sau nu. În cazul în care Contul ESET HOME este compromis, notificați imediat Furnizorul. Utilizarea funcției Protecție împotriva utilizării necorespunzătoare a datelor este aplicabilă exclusiv Utilizatorilor finali ai produselor ESET Internet Security și ESET Smart Security Premium.

ESET Secure Data. Dispoziții suplimentare se aplică în cazul ESET Secure Data, după cum urmează:

1. Definiții. În aceste dispoziții suplimentare la ESET Secure Data, următorii termeni au semnificațiile atribuite mai

jos:

a) „Informații” orice informații sau date criptate ori decriptate cu ajutorul software-ului;

b) „Produse” software-ul ESET Secure Data și documentația aferentă;

c) „ESET Secure Data„ programul/programele software utilizat(e) pentru criptarea și decriptarea datelor electronice;

Toate referirile la forma de plural vor include forma de singular și toate referirile la genul masculin vor include genurile feminin și neutru și invers. Termenii fără definiție specifică vor fi utilizați în conformitate cu definițiile stipulate în Acord.

2. Declarație suplimentară a Utilizatorului final. Recunoașteți și acceptați următoarele:

a) Dvs. vă revine responsabilitatea de a proteja, a păstra și a face o copie de rezervă pentru Informații;

b) Dvs. trebuie să faceți o copie de rezervă completă pentru toate informațiile și datele (inclusiv, dar fără a se limita la orice informații și date esențiale) de pe computer înainte de instalarea software-ului ESET Secure Data;

c) Dvs. trebuie să păstrați în siguranță o înregistrare a oricăror parole sau a altor informații utilizate pentru configurarea și utilizarea programului ESET Secure Data; de asemenea, trebuie să faceți copii de rezervă pe suporturi de stocare separate pentru toate cheile de criptare, codurile de licență, fișierele cheie și alte date generate;

d) Dvs. sunteți responsabil pentru utilizarea Produselor. Furnizorul nu va fi răspunzător pentru niciun fel de pierderi, de pretenții sau de daune suferite drept consecință a unei criptări ori decriptări neautorizate sau eronate a Informațiilor ori a datelor, indiferent de modul și de locul în care sunt stocate Informațiile sau datele respective;

e) deși Furnizorul a luat toate măsurile rezonabile pentru a asigura integritatea și securitatea software-ului ESET Secure Data, Produsele (sau oricare dintre acestea) nu trebuie utilizate în niciun domeniu care depinde de un nivel de securitate cu protecție în caz de nereușită ori care este potențial periculos, inclusiv, dar fără a se limita la instalații nucleare, navigație aeriană, sisteme de comunicații sau de control, sisteme de armament și de apărare, precum și sisteme de menținere ori de monitorizare a funcțiilor vitale;

f) Utilizatorului final îi revine responsabilitatea de a se asigura că nivelul de securitate și de criptare oferit de produse este adecvat cerințelor Dvs.;

g) Dvs. sunteți responsabil pentru utilizarea Produselor (sau a oricăruia dintre acestea), inclusiv, dar fără a se limita la asigurarea faptului că o astfel de utilizare respectă toate legile și reglementările aplicabile ale Republicii Slovace ori ale oricărei alte țări, regiuni sau stat în care sunt utilizate Produsele. Trebuie să vă asigurați că, înaintea oricărei utilizări a Produselor, v-ați asigurat că acestea nu contravin niciunui embargou guvernamental (în Republica Slovacă sau oriunde altundeva);

h) ESET Secure Data poate contacta periodic serverele Furnizorului pentru a căuta informații privind licența, corecții disponibile, pachete service pack și alte actualizări care pot să îmbunătățească, să întrețină, să modifice sau să optimizeze funcționarea programului ESET Secure Data și poate trimite informații generale de sistem legate de funcționarea acestuia în conformitate cu Politica de confidențialitate.

i) Furnizorul nu va fi responsabil pentru niciun fel de pierderi, de daune, de cheltuieli sau de pretenții care decurg din pierderea, furtul, utilizarea necorespunzătoare, deteriorarea ori distrugerea parolelor, a informațiilor de configurare, a cheilor de criptare, a codurilor de activare a licenței și a altor date generate sau stocate în timpul utilizării software-ului.

Dispozițiile suplimentare pentru ESET Secure Data vor fi aplicabile exclusiv utilizatorilor finali ai produsului ESET Smart Security Premium.

Password Manager Software-ul. Dispoziții suplimentare se aplică în cazul software-ului Password Manager, după cum urmează:

1. Declarație suplimentară a Utilizatorului final. Recunoașteți și acceptați următoarele:

a) utilizați Software-ul Password Manager pentru a opera niciun fel de aplicații esențiale pentru activitate în cazul în care există riscuri la adresa bunurilor materiale sau a vieții umane. Înțelegeți că Software-ul Password Manager nu este proiectat în astfel de scopuri și că defectarea acestuia în astfel de cazuri poate duce la deces, la vătămări corporale sau la pagube materiale și de mediu grave, pentru care Furnizorul nu este responsabil.

SOFTWARE-UL PASSWORD MANAGER NU ESTE PROIECTAT, DESTINAT SAU LICENȚIAT PENTRU UTILIZARE ÎN MEDII PERICULOASE CARE NECESITĂ SISTEME DE CONTROL CU PROTECȚIE ÎN CAZ DE NEREUȘITĂ, INCLUSIV, DAR FĂRĂ A SE LIMITA LA PROIECTAREA, CONSTRUCȚIA, ÎNTREȚINEREA ORI OPERAREA INSTALAȚIILOR NUCLEARE, A SISTEMELOR DE COMUNICAȚII SAU DE NAVIGAȚIE AERIANĂ, A SISTEMELOR DE CONTROL AL TRAFICULUI AERIAN ȘI A SISTEMELOR DE ARMAMENT ORI DE MENȚINERE A FUNCȚIILOR VITALE. FURNIZORUL EXCLUDE ÎN MOD SPECIFIC ORICE GARANȚII EXPLICITE SAU IMPLICITE DE ADECVARE PENTRU ASTFEL DE SCOPURI.

b) utilizați Software-ul Password Manager într-un mod care încalcă acest acord sau legile Republicii Slovace ori cele din jurisdicția dvs. În mod specific, nu aveți dreptul să utilizați Software-ul Password Manager pentru a desfășura sau a promova activități ilegale, inclusiv încărcarea de date cu conținut dăunător sau cu conținut care poate fi utilizat pentru activități ilegale sau care încalcă în orice mod legea sau drepturile terților (inclusiv drepturile de proprietate intelectuală), inclusiv, dar fără a se limita la încercările de a obține acces la conturi în Spațiul de stocare (în sensul acestor dispoziții suplimentare pentru software-ul Password Manager, „Spațiul de stocare” se referă la spațiul de stocare a datelor gestionat de Furnizor sau de un terț, altul decât Furnizorul și utilizatorul, în scopul activării sincronizării și al copierii de rezervă a datelor utilizatorului) sau la orice conturi și date ale altor utilizatori ai Software-ului Password Manager sau ai Spațiului de stocare. Dacă încălcați oricare dintre aceste prevederi, Furnizorul are dreptul de a rezilia imediat acest acord și de a vă transfera costurile măsurilor necesare de reparație, precum și de a lua orice măsuri necesare pentru a vă împiedica să mai utilizați Software-ul Password Manager fără posibilitatea rambursării.

2. LIMITAREA RĂSPUNDERII. SOFTWARE-UL PASSWORD MANAGER ESTE FURNIZAT „CA ATARE”. NU SE ACORDĂ NICIUN FEL DE GARANȚIE EXPLICITĂ SAU IMPLICITĂ. UTILIZAȚI SOFTWARE-UL PE PROPRIUL DVS. RISC. PRODUCĂTORUL NU ESTE RĂSPUNZĂTOR PENTRU PIERDEREA DATELOR, PENTRU DAUNE, PENTRU LIMITAREA DISPONIBILITĂȚII SERVICIULUI, INCLUSIV ORICE DATE TRIMISE DE SOFTWARE-UL PASSWORD MANAGER CĂTRE SPAȚIUL EXTERN DE STOCARE ÎN SCOPUL SINCRONIZĂRII ȘI AL COPIERII DE REZERVĂ A DATELOR. CRIPTAREA DATELOR CU AJUTORUL SOFTWARE-ULUI PASSWORD MANAGER NU IMPLICĂ NICIO RĂSPUNDERE A FURNIZORULUI ÎN CEEA CE PRIVEȘTE SECURITATEA DATELOR RESPECTIVE. SUNTEȚI DE ACORD ÎN MOD EXPLICIT CĂ DATELE OBȚINUTE, UTILIZATE, CRIPTATE, STOCATE, SINCRONIZATE SAU TRIMISE CU AJUTORUL SOFTWARE-ULUI PASSWORD MANAGER POT FI STOCATE ȘI PE SERVERE TERȚE (SE APLICĂ DOAR UTILIZĂRII SOFTWARE-ULUI PASSWORD MANAGER ÎN CAZUL ÎN CARE SUNT ACTIVATE SERVICIILE DE SINCRONIZARE ȘI DE COPIERE DE REZERVĂ). DACĂ FURNIZORUL, LA DISCREȚIA SA EXCLUSIVĂ, ALEGE SĂ UTILIZEZE UN ASTFEL DE SPAȚIU DE STOCARE, SITE WEB, PORTAL WEB, SERVER SAU SERVICIU TERȚ, FURNIZORUL NU ESTE RĂSPUNZĂTOR PENTRU CALITATEA, SECURITATEA ORI DISPONIBILITATEA UNUI ASTFEL DE SERVICIU TERȚ ȘI NU ESTE RĂSPUNZĂTOR ÎN NICIUN CAZ ÎN FAȚA DVS. PENTRU NICIUN FEL DE ÎNCĂLCARE A OBLIGAȚIILOR CONTRACTUALE SAU LEGALE DIN PARTEA TERȚULUI ȘI NICI PENTRU DAUNE, PIERDEREA PROFITURILOR, DAUNE PECUNIARE ORI NEPECUNIARE SAU PENTRU NICIUN ALT FEL DE PIERDERI ÎN TIMPUL UTILIZĂRII ACESTUI SOFTWARE. FURNIZORUL NU ESTE RĂSPUNZĂTOR PENTRU CONȚINUTUL DATELOR OBȚINUTE, UTILIZATE, CRIPTATE, STOCATE, SINCRONIZATE SAU TRIMISE CU AJUTORUL SOFTWARE-ULUI PASSWORD MANAGER ORI AFLATE ÎN SPAȚIUL DE STOCARE. RECUNOAȘTEȚI FAPTUL CĂ FURNIZORUL NU ARE ACCES LA CONȚINUTUL DATELOR STOCATE ȘI NU ARE POSIBILITATEA DE A LE MONITORIZA SAU DE A ELIMINA CONȚINUTUL DĂUNĂTOR.

Furnizorul deține toate drepturile asupra îmbunătățirilor, a upgrade-urilor și a remedierilor legate de Software-ul Password MANAGER („Îmbunătățiri”), chiar și în cazul în care orice astfel de îmbunătățiri au fost create pe baza feedbackului, a ideilor sau a sugestiilor remise de către dvs. în orice formă. Nu aveți dreptul la niciun fel de compensații, inclusiv orice tip de redevențe legate de astfel de Îmbunătățiri.

LICENȚIATORII ȘI ENTITĂȚILE FURNIZOARE NU VOR FI RĂSPUNZĂTOARE ÎN FAȚA DVS. PENTRU NICIUN FEL DE PRETENȚII ȘI DE OBLIGAȚII CARE DECURG SAU SUNT LEGATE ÎN ORICE MOD DE UTILIZAREA SOFTWARE-ULUI PASSWORD MANAGER DE CĂTRE DVS. ORI DE CĂTRE TERȚI, DE UTILIZAREA SAU DE LIPSA UTILIZĂRII UNEI FIRME DE INTERMEDIERE ORI DISTRIBUITOR SAU DE VÂNZAREA ORI DE ACHIZIȚIA ORICĂRUI SERVICIU DE SECURITATE, INDIFERENT DACĂ ACESTE PRETENȚII ȘI OBLIGAȚII SE ÎNTEMEIAZĂ PE O TEORIE JURIDICĂ SAU DE DREPT NATURAL.

LICENȚIATORII ȘI ENTITĂȚILE FURNIZOARE NU VOR FI RĂSPUNZĂTOARE ÎN FAȚA DVS. PENTRU NICIUN FEL DE DAUNE DIRECTE, SPECIALE, ACCESORII, INDIRECTE SAU CONEXE CARE DECURG ORI SUNT LEGATE DE ORICE SOFTWARE TERȚ, DE ORICE DATE ACCESATE PRIN SOFTWARE-UL PASSWORD MANAGER, DE UTILIZAREA DE CĂTRE DVS. SAU DE IMPOSIBILITATEA UTILIZĂRII ORI A ACCESĂRII SOFTWARE-ULUI PASSWORD MANAGER SAU DE ORICE DATE FURNIZATE PRIN SOFTWARE-UL PASSWORD MANAGER, INDIFERENT DACĂ ACESTE PRETENȚII DE DAUNE SUNT RIDICATE ÎN TEMEIUL UNEI TEORII JURIDICE ORI AL DREPTULUI NATURAL. DAUNELE EXCLUSE PRIN PREZENTA CLAUZĂ INCLUD, FĂRĂ A SE LIMITA LA DAUNELE PENTRU PIERDEREA PROFITURILOR, PENTRU VĂTĂMĂRI CORPORALE SAU DAUNE MATERIALE, PENTRU ÎNTRERUPEREA ACTIVITĂȚII, PENTRU PIERDEREA INFORMAȚIILOR CU CARACTER PERSONAL ORI PROFESIONAL. ANUMITE JURISDICȚII NU PERMIT LIMITAREA DAUNELOR ACCESORII SAU CONEXE, ASTFEL CĂ ESTE POSIBIL CA ACEASTĂ RESTRICȚIE SĂ NU VI SE APLICE. ÎN ASTFEL DE CAZURI, ÎNTINDEREA RĂSPUNDERII FURNIZORULUI VA FI LIMITA MINIMĂ PERMISĂ ÎN TEMEIUL LEGII APLICABILE.

ESTE POSIBIL CA INFORMAȚIILE FURNIZATE PRIN SOFTWARE-UL PASSWORD MANAGER, INCLUSIV COTAȚIILE ACȚIUNILOR, ANALIZE, INFORMAȚII DE PIAȚĂ, ȘTIRI ȘI DATE FINANCIARE, SĂ FIE ÎNTÂRZIATE, INEXACTE ORI SĂ CONȚINĂ ERORI SAU OMISIUNI, IAR LICENȚIATORII ȘI ENTITĂȚILE FURNIZOARE NU VOR AVEA NICIO RĂSPUNDERE ÎN LEGĂTURĂ CU ACESTEA. ESTE POSIBIL CA FURNIZORUL SĂ MODIFICE ORI SĂ ÎNTRERUPĂ ORICE ASPECT SAU CARACTERISTICĂ A SOFTWARE-ULUI PASSWORD MANAGER ORI UTILIZAREA TUTUROR SAU A UNOR CARACTERISTICI ORI TEHNOLOGII DIN SOFTWARE-UL PASSWORD MANAGER ÎN ORICE MOMENT, FĂRĂ A VĂ TRANSMITE O NOTIFICARE PREALABILĂ.

DACĂ PREVEDERILE DIN PREZENTUL ARTICOL SUNT NULE, INDIFERENT DE MOTIV SAU FURNIZORUL ESTE CONSIDERAT RĂSPUNZĂTOR PENTRU PIERDERI, DAUNE ETC. ÎN TEMEIUL LEGILOR APLICABILE, PĂRȚILE CONVIN CA RĂSPUNDEREA FURNIZORULUI ÎN FAȚA DVS. SĂ FIE LIMITATĂ LA VALOAREA TOTALĂ A TAXELOR DE LICENȚĂ PLĂTITE DE CĂTRE DVS.

SUNTEȚI DE ACORD SĂ DESPĂGUBIȚI, SĂ APĂRAȚI ȘI SĂ SCUTIȚI DE RESPONSABILITATE FURNIZORUL ȘI ANGAJAȚII SĂI, FILIALELE, SOCIETĂȚILE AFILIATE, SOCIETĂȚILE CARE ȘI-AU SCHIMBAT MARCA ȘI ALȚI PARTENERI FAȚĂ DE ȘI ÎMPOTRIVA ORICĂROR TERȚI (INCLUSIV DEȚINĂTORII DISPOZITIVULUI SAU PĂRȚILE ALE CĂROR DREPTURI AU FOST AFECTATE DE DATELE UTILIZATE ÎN SOFTWARE-UL PASSWORD MANAGER ORI ÎN SPAȚIUL DE STOCARE) PENTRU PRETENȚII, OBLIGAȚII, DAUNE, PIERDERI, COSTURI, CHELTUIELI, ONORARII PE CARE ESTE POSIBIL CA ACESTE PĂRȚI SĂ LE SUPORTE DREPT REZULTAT AL UTILIZĂRII DE CĂTRE DVS. A SOFTWARE-ULUI PASSWORD MANAGER.

3. Datele din Software-ul Password Manager. Cu excepția unei opțiuni contrare și explicite din partea dvs., toate datele pe care le introduceți și care sunt salvate într-o bază de date a Software-ului Password Manager sunt stocate în format criptat pe computerul dvs. sau pe un alt dispozitiv de stocare pe care l-ați definit. Înțelegeți că, în cazul ștergerii sau al deteriorării unei baze de date a Software-ului Password Manager ori a altor fișiere, toate datele cuprinse în acestea vor fi pierdute definitiv și înțelegeți și acceptați riscul unei astfel de pierderi. Faptul că datele dvs. cu caracter personal sunt stocate în format criptat pe computer nu înseamnă că informațiile nu pot fi furate sau utilizate în mod necorespunzător de către o persoană care descoperă parola principală ori care obține

acces la dispozitivul de activare definit de client pentru deschiderea bazei de date. Sunteți responsabil pentru păstrarea securității tuturor metodelor de acces.

4. Transmiterea datelor cu caracter personal către furnizor sau către spațiul de stocare. Dacă selectați astfel și exclusiv în scopul asigurării sincronizării și a copierii de rezervă în timp util a datelor, Software-ul Password Manager transmite datele cu caracter personal din baza de date a Software-ului Password Manager, respectiv parolele, informațiile de conectare, Conturile și Identitățile, prin Internet către Spațiul de stocare. Datele sunt transmise exclusiv în format criptat. Este posibil ca utilizarea Software-ului Password Manager pentru completarea formularelor online cu parole, informații de conectare sau alte date să necesite transmiterea informațiilor prin Internet către site-ul Web identificat de dvs. Această transmisie de date nu este inițiată de Software-ul Password Manager și, prin urmare, Furnizorul nu poate fi considerat responsabil pentru securitatea unor astfel de interacțiuni cu orice site Web susținut de diverși furnizori. Orice tranzacții prin Internet, indiferent dacă au sau nu legătură cu Software-ul Password Manager, se realizează la discreția dvs. exclusivă și pe propriul dvs. risc, iar dvs. vă asumați întreaga răspundere pentru orice daune produse sistemului dvs. informatic ori pentru pierderea de date care rezultă din descărcarea și/sau utilizarea unui astfel de material ori de serviciu. Pentru a reduce la minimum riscul de pierdere a datelor valoroase, Furnizorul recomandă clienților să efectueze periodic copii de rezervă pentru baza de date și pentru alte fișiere sensibile pe unități externe. Furnizorul nu vă poate oferi niciun fel de asistență la recuperarea datelor pierdute sau deteriorate. Dacă Furnizorul oferă servicii de copiere de rezervă pentru fișierele din baza de date a utilizatorului în cazul deteriorării sau al ștergerii fișierelor de pe PC-urile utilizatorilor, astfel de servicii de copiere de rezervă nu beneficiază de garanție și nu implică niciun fel de răspundere a Furnizorului în fața dvs.

Prin utilizarea Software-ului Password Manager, sunteți de acord că este posibil ca software-ul să contacteze periodic serverele Furnizorului pentru a căuta informații privind licența, corecții disponibile, pachete service pack și alte actualizări care pot să îmbunătățească, să întrețină, să modifice sau să optimizeze funcționarea Software-ului Password Manager. Este posibil ca software-ul să trimită informații generale de sistem legate de funcționarea Software-ului Password Manager.

5. Informații și instrucțiuni privind dezinstalarea. Orice informații pe care doriți să le păstrați din baza de date trebuie exportate înaintea dezinstalării Software-ului Password Manager.

Dispozițiile suplimentare pentru software-ul Password Manager vor fi aplicabile exclusiv utilizatorilor finali ai produsului ESET Smart Security Premium.

ESET LiveGuard. Dispoziții suplimentare se aplică în cazul ESET LiveGuard, după cum urmează:

Software-ul conține o funcție de analiză suplimentară a fișierelor trimise de către utilizatorul final. Furnizorul va utiliza fișierele transmise de către utilizatorul final și rezultatele analizei numai în conformitate cu Politica de confidențialitate și cu reglementările legale relevante.

Dispozițiile suplimentare pentru ESET LiveGuard vor fi aplicabile exclusiv utilizatorilor finali ai produsului ESET Smart Security Premium.

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

Politica de confidenţialitate

Protecția datelor cu caracter personal are o importanță deosebită pentru ESET, spol. s r. o., cu sediul social pe Einsteinova 24, 851 01 Bratislava, Slovak Republic, înregistrată în Registrul comerțului administrat de Tribunalul Districtual Bratislava I, secțiunea Sro, cu nr. de înregistrare 3586/B și cu codul unic de înregistrare 31333532 în calitate de Operator de date („ESET“ sau „Noi“). Dorim să respectăm cerința de transparență, așa cum este standardizată din punct de vedere juridic în temeiul Regulamentului general al UE privind protecția datelor

(„GDPR“). Pentru a realiza acest obiectiv, publicăm această Politică de confidențialitate cu unicul scop de informare a clientului („Utilizator final” sau „Dvs.”) în calitate de persoană vizată despre subiectele următoare privind protecția datelor cu caracter personal:

- temeiul juridic al prelucrării datelor cu caracter personal,
- partajarea datelor și confidențialitatea acestora,
- securitatea datelor,
- drepturile dvs. în calitate de persoană vizată,
- prelucrarea datelor dvs. cu caracter personal.
- Informații de contact.

Temeiul juridic al prelucrării datelor cu caracter personal

Utilizăm doar câteva temeiuri juridice în ceea ce privește prelucrarea datelor, conform cadrului legislativ aplicabil aferent protejării datelor cu caracter personal. Prelucrarea datelor cu caracter personal de către ESET este necesară în principal pentru îndeplinirea clauzelor din Acord de licență pentru utilizatorul final („EULA“) [articolul 6, alineatul (1), litera (b) din GDPR], care se aplică pentru furnizarea de produse sau servicii ESET, cu excepția cazului în care se prevede altfel în mod explicit, de exemplu:

- Temeiul juridic reprezentat de interesul legitim [articolul 6, alineatul (1), litera (b) din GDPR], care ne permite să prelucrăm date privind modul în care clienții noștri utilizează Serviciile noastre și satisfacția acestora, pentru a oferi utilizatorilor noștri cea mai bună protecție, asistență și experiență pe care le putem oferi. Chiar și marketingul este recunoscut de către legislația aplicabilă drept interes legitim, prin urmare ne bazăm de obicei pe acest temei pentru comunicările noastre de marketing cu clienții noștri.

- Consimțământul [articolul 6, alineatul (1), litera (b) din GDPR], pe care vi-l putem solicita în situații specifice în care considerăm că acest temei juridic este cel mai potrivit sau dacă este impus de lege.

- Conformitatea cu obligațiile legale [articolul 6, alineatul (1), litera (b) din GDPR], de exemplu, stipularea cerințelor pentru comunicarea electronică și păstrarea documentelor pentru facturare și chitanțe.

Partajarea datelor și confidențialitatea acestora

Nu partajăm datele dumneavoastră niciunui terț. Cu toate acestea, ESET este o companie care funcționează la nivel global prin companii afiliate sau prin parteneri, care fac parte din rețeaua noastră de vânzări, servicii și asistență. Informațiile despre licențe, facturare și asistență tehnică prelucrate de ESET pot fi transferate către și de la afiliați sau parteneri pentru a îndeplini clauzele din Acordul de licență pentru utilizatorul final, cum ar fi asigurarea de servicii sau de asistență.

ESET preferă să-și prelucreze datele în Uniunea Europeană (UE). Cu toate acestea, în funcție de locația dumneavoastră (utilizarea produselor și/sau a serviciilor noastre în afara UE) și/sau de serviciul pe care îl alegeți, poate fi necesar să vă transferați datele într-o țară din afara UE. De exemplu, utilizăm servicii terțe legate de cloud computing. În aceste cazuri, selectăm cu atenție furnizorii de servicii și asigurăm un nivel adecvat de protecție a datelor prin măsuri contractuale, precum și tehnice și organizatorice. De regulă, suntem de acord cu clauzele contractuale standard ale UE și, dacă este necesar, cu reglementări contractuale suplimentare.

Pentru unele țări din afara UE, cum ar fi Regatul Unit și Elveția, UE a stabilit deja un nivel comparabil de protecție

a datelor. Datorită nivelului comparabil de protecție a datelor, transferul de date către aceste țări nu necesită nicio autorizație sau acord special.

Securitatea datelor

ESET implementează măsuri tehnice și organizaționale adecvate pentru a asigura un nivel de securitate conform riscurilor potențiale. Facem tot posibilul ca să asigurăm permanent confidențialitatea, integritatea, disponibilitatea și continuitatea serviciilor și sistemelor de prelucrare. Cu toate acestea, în cazul unei încălcări a datelor care are ca rezultat un risc pentru drepturile și libertățile dvs., suntem pregătiți să anunțăm autoritatea de supraveghere relevantă, precum și utilizatorii finali afectați în calitate de persoane vizate.

Drepturile subiectului datelor

Drepturile fiecărui Utilizator final contează și dorim să vă informăm că toți Utilizatorii finali (din orice țară din UE sau din afara UE) au următoarele drepturi garantate la ESET. Pentru a vă exercita drepturile de persoană vizată, ne puteți contacta prin intermediul formularului de asistență sau prin e-mail la dpo@eset.sk. În scopul identificării, vă solicităm următoarele informații: Numele, adresa de e-mail și, dacă este disponibilă, cheia de licență sau numărul clientului și afilierea companiei. Abțineți-vă să ne trimiteți orice alte date cu caracter personal, cum ar fi data nașterii. Dorim să subliniem faptul că, pentru a putea procesa solicitarea dvs., precum și în scop de identificare, vom prelucra datele dvs. cu caracter personal.

Dreptul de a retrage consimțământul. Dreptul de a retrage consimțământul se aplică în cazul prelucrării numai pe baza consimțământului. Dacă vă prelucrăm datele cu caracter personal pe baza consimțământului, aveți dreptul de a retrage consimțământul în orice moment, fără a oferi motive. Retragerea consimțământului este valabilă numai pentru viitor și nu afectează legalitatea datelor prelucrate înainte de retragere.

Dreptul la opoziție. Dreptul la opoziție față de prelucrare se aplică în cazul prelucrării pe baza interesului legitim al ESET sau al unui terț. Dacă prelucrăm datele dvs. cu caracter personal pentru a proteja un interes legitim, dvs., în calitate de persoana vizată, aveți dreptul de a vă opune interesului legitim numit de noi și prelucrării datelor dvs. cu caracter personal în orice moment. Opoziția dvs. este valabilă numai pentru viitor și nu afectează legalitatea datelor prelucrate înainte de opoziție. În cazul în care prelucrăm datele dvs. cu caracter personal în scopuri de marketing direct, nu este necesar să vă justificați opoziția. Acest lucru se aplică, de asemenea, profilării, în măsura în care aceasta este legată de un astfel de marketing direct. În toate celelalte cazuri, vă rugăm să ne informați pe scurt cu privire la reclamațiile dvs. cu privire la interesul legitim al ESET de a prelucra datele dvs. cu caracter personal.

Rețineți că, în unele cazuri, în ciuda retragerii consimțământului, avem dreptul să prelucrăm în continuare datele dvs. cu caracter personal pe baza unui alt temei juridic, de exemplu, pentru executarea unui contract.

Dreptul de acces. În calitate de persoana vizată, aveți dreptul de a obține gratuit informații despre datele dvs. stocate de ESET în orice moment.

Dreptul la rectificare. Dacă prelucrăm din greșeală date cu caracter personal incorecte despre dvs., aveți dreptul de a corecta acest lucru.

Dreptul la ștergere și dreptul la restricționarea prelucrării. În calitate de persoana vizată, aveți dreptul de a solicita ștergerea sau restricționarea prelucrării datelor dvs. cu caracter personal. Dacă prelucrăm datele dvs. cu caracter personal, de exemplu, cu consimțământul dvs., le retrageți și nu există niciun alt temei juridic, de exemplu, un contract, vi le ștergem imediat. Datele dvs. cu caracter personal vor fi, de asemenea, șterse de îndată ce nu mai sunt necesare pentru scopurile declarate pentru acestea la sfârșitul perioadei de păstrare.

Dacă utilizăm datele dvs. cu caracter personal exclusiv în scopul marketingului direct și v-ați revocat

consimțământul sau v-ați opus interesului legitim subiacent al ESET, vom restricționa prelucrarea acestor date în măsura în care includem datele dvs. de contact în lista noastră neagră internă pentru a evita contactarea nesolicitată. În caz contrar, datele dvs. cu caracter personal vor fi șterse.

Rețineți că este posibil să ni se solicite să stocăm datele dvs. până la expirarea obligațiilor de păstrare și a perioadelor emise de legiuitor sau de autoritățile de supraveghere. Obligațiile și perioadele de păstrare pot rezulta, de asemenea, din legislația slovacă. Ulterior, datele corespunzătoare vor fi șterse în mod obișnuit.

Dreptul la portabilitatea datelor. Suntem bucuroși să vă oferim, în calitate de persoana vizată, datele cu caracter personal prelucrate de ESET în format xls.

Dreptul de a depune o plângere. În calitate de persoana vizată, aveți dreptul de a depune o plângere la o autoritate de supraveghere în orice moment. ESET se supune reglementărilor legislației slovace și Noi ne obligăm să respectăm legislația privind protecția datelor impusă de Uniunea Europeană. Autoritatea relevantă de supraveghere în domeniul datelor este Oficiul pentru Protecția Datelor cu Caracter Personal al Republicii Slovace, cu sediul la Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Prelucrarea datelor dvs. cu caracter personal

Serviciile furnizate de ESET și implementate în produsul nostru sunt furnizate conform termenilor EULA, dar unele pot necesita o atenție specială. Dorim să vă furnizăm mai multe detalii despre culegerea datelor în legătură cu asigurarea serviciilor noastre. Oferim servicii diverse, care sunt descrise în Acordul de licență pentru utilizatorul final și în documentație. Pentru ca toate acestea să funcționeze, trebuie să culegem informațiile următoare:

Datele privind licențierea și facturarea. Numele, adresa de e-mail, cheia de licență și (dacă este cazul) adresa, afilierea companiei și datele privind plata sunt colectate și prelucrate de ESET pentru a facilita activarea licenței, livrarea cheii de licență, mementouri privind expirarea, solicitări de asistență, verificarea autenticității licenței, furnizarea serviciului nostru și alte notificări, inclusiv mesaje de marketing, în conformitate cu legislația în vigoare sau cu consimțământul dvs. ESET este obligată prin lege să păstreze informațiile de facturare pentru o perioadă de 10 ani, însă informațiile de licențiere vor fi anonimizate în termen de cel mult 12 luni de la expirarea licenței.

Actualizarea și alte statistici. Printre informațiile procesate se numără informații referitoare la procesul de instalare și computerul dvs., inclusiv platforma pe care este instalat produsul nostru, precum și informații despre operațiunile și funcționalitatea produselor noastre, cum ar fi sistemul de operare, informații despre hardware, ID-urile de instalare, ID-urile de licență, adresa IP și adresa MAC; setările de configurare a produsului sunt prelucrate în scopul furnizării de servicii de actualizare și upgrade și în cel al întreținerii, securității și îmbunătățirii infrastructurii noastre de backend.

Aceste informații sunt păstrate separat de informațiile de identificare necesare în scopul acordării de licențe și de facturare, deoarece nu necesită identificarea Utilizatorului final. Perioada de păstrare este de până la 4 ani.

Sistemul bazat pe reputație ESET LiveGrid®. Codurile hash unirecționale legate de infiltrare sunt procesate în scopul Sistemului bazat pe reputație ESET LiveGrid®, care îmbunătățește eficiența soluțiilor noastre anti-malware prin compararea fișierelor scanate cu o bază de date cu elemente de pe lista albă și lista neagră din cloud. Utilizatorul final nu este identificat în timpul acestui proces.

Sistemul de feedbackESET LiveGrid®. Mostre și metadate suspecte de oriunde ca parte a sistemului de feedback ESET LiveGrid®, care îi permite companiei ESET să reacționeze imediat la nevoile utilizatorilor finali și îi permite să reacționeze la cele mai recente amenințări furnizate. Depindem de Dvs. ca să ne trimiteți

- Infiltrări, cum ar fi eventualele mostre de viruși și alte programe rău intenționate; obiecte potențial nesigure, nedorite sau problematice, cum ar fișiere executabile și mesaje de e-mail raportate de Dvs. ca fiind spam sau

semnalate de produsul nostru;

- Informații despre utilizarea internetului, cum ar fi adrese IP și informații geografice, pachete IP, URL-uri și cadre ethernet;

- Fișiere dump pentru cădere și informațiile conținute.

Nu dorim să culegem datele dvs. în afara acestui scop dar, uneori, acest lucru este imposibil de evitat. Datele culese accidental pot fi incluse în programul malware în sine (culese fără cunoștința sau aprobarea dvs.) sau ca parte a numelor de fișiere sau a adreselor URL și fără intenția noastră ca acestea să facă parte din sistemele noastre sau să fie procesate în scopul declarat în această Politică de confidențialitate.

Toate informațiile obținute și procesate prin intermediul Sistemului de feedback ESET LiveGrid® sunt menite să fie utilizate fără identificarea Utilizatorului final.

Evaluarea securității dispozitivelor conectate la rețea. Pentru a furniza funcția de evaluare a securității, procesăm numele rețelei locale și informații despre dispozitivele din rețeaua locală, cum ar fi prezența, tipul, numele, adresa IP și adresa MAC a dispozitivului în rețeaua dvs. locală în legătură cu informațiile despre licență. Informațiile includ tipul de securitate wireless și tipul de criptare wireless pentru dispozitivele ruter. Informațiile de licență care identifică Utilizatorul final vor fi anonimizate în termen de cel mult 12 luni de la expirarea licenței.

Asistența tehnică. Informațiile de contact și de licențiere și datele incluse în solicitările de asistență pot fi necesare pentru serviciul de asistență. În funcție de canalul pe care l-ați ales pentru a ne contacta, putem colecta adresa Dvs. de e-mail, numărul de telefon, informațiile despre licență, detaliile produsului și descrierea dosarului de asistență. Vi se poate solicita să ne furnizați și alte informații pentru a facilita asigurarea asistenței. Datele prelucrate pentru asistență tehnică sunt stocate timp de 4 ani.

Protecția împotriva utilizării necorespunzătoare a datelor. În cazul în care Contul ESET HOME este creat pe https://home.eset.com și funcția este activată de Utilizatorul final în legătură cu furtul computerului, vor fi colectate și prelucrate următoarele informații: datele despre locație, capturile de ecran, datele despre configurația computerului și datele înregistrate de camera computerului. Datele colectate sunt stocate pe serverele noastre sau pe serverele furnizorilor noștri de servicii și au o perioadă de păstrare de 3 luni.

Password Manager Dacă alegeți să activați funcția Password Manager, datele legate de detaliile dvs. de conectare sunt stocate într-o formă criptată numai pe computerul dvs. sau pe alt dispozitiv desemnat. Dacă activați serviciul de sincronizare, datele criptate sunt stocate pe serverele noastre sau pe cele ale furnizorilor noștri de servicii pentru a asigura acest serviciu. Nici ESET și nici furnizorul de servicii nu are acces la datele criptate. Numai Dvs. dețineți cheia de decriptare a datelor. Datele vor fi eliminate la dezactivarea funcției.

ESET LiveGuard. Dacă alegeți să activați funcția ESET LiveGuard, trebuie să se trimită mostre precum fișiere predefinite și selectate de Utilizatorul final. Mostrele pe care le alegeți pentru analiza la distanță vor fi încărcate în serviciul ESET, iar rezultatul analizei va fi trimis înapoi pe computerul dvs. Orice mostre suspecte sunt prelucrate la fel ca informațiile colectate de Sistemul de feedback ESET LiveGrid®.

Programul de îmbunătățire a experienței clienților. Dacă ați optat să activați Programul de îmbunătățire a experienței clienților , informațiile anonime de telemetrie referitoare la utilizarea produselor noastre vor fi colectate și utilizate, pe baza consimțământului dvs.

Rețineți că, în cazul în care persoana care utilizează produsele și serviciile noastre nu este Utilizatorul final care a achiziționat produsul sau serviciul și a încheiat cu noi Acordul de licență pentru utilizatorul final (de exemplu, un angajat al Utilizatorului final, un membru al familiei sau o persoană autorizată în alt mod să utilizeze produsul sau serviciul de către Utilizatorul final în conformitate cu Acordul de licență pentru utilizatorul final, prelucrarea datelor se efectuează în interesul legitim al ESET în sensul art. 6 (1) f) din GDPR pentru a permite utilizatorului

autorizat de Utilizatorul final să utilizeze produsele și serviciile furnizate de Noi în conformitate cu Acordul de licență pentru utilizatorul final.

Informații de contact

Dacă doriți să vă exercitați dreptul în calitate de subiect al datelor sau dacă aveți întrebări sau preocupări, trimiteți-ne un mesaj la adresa:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk