ESET NOD32 Antivirus 3.0

Componente integrate:
ESET NOD32 Antivirus
ESET NOD32 Antispyware

Ghid de utilizare

noi vă protejăm universul digital

cuprins

1. ESET NOD32 Antivirus 3.0 4
1.1 Ce este nou 4
1.2 Cerințe de sistem 4

2. Instalare 5
2.1 Instalare tipică 5
2.2 Instalare personalizată 6
2.3 Utilizarea setărilor originale 7
2.4 Introducerea numelui de utilizator și a parolei 7
2.5 Scanarea calculatorului la cerere 8

3. Ghidul începătorului 9
3.1 Prezentarea designului interfeței pentru utilizator – moduri 9
3.1.1 Verificarea funcționării sistemului 9
3.1.2 Ce este de făcut dacă programul nu funcționează corect 10
3.2 Setarea actualizării 10
3.3 Setare server proxy 10
3.4 Protecția setărilor 11

4. Lucrul cu ESET NOD32 Antivirus 12
4.1 Protecția antivirus și antispyware 12
4.1.1 Protecția-protecție în timp real a sistemului de fișiere 12
4.1.1.1 Setarea controlului 12
4.1.1.1.1 Scanarea mediilor 12
4.1.1.1.2 Scanare declanșată de un eveniment 12
4.1.1.1.3 Verificarea fișierelor nou create 12
4.1.1.1.4 Setările avansate 12
4.1.1.2 Nivele de curățare 12
4.1.1.3 Când trebuie modificată configurația protecției în timp real Real 13
4.1.1.4 Verificarea protecției în timp real 13
4.1.1.5 Ce este de făcut dacă protecția în timp real nu funcționează 13
4.1.2 Protecția pentru email 13
4.1.2.1 Verificarea POP3 13
4.1.2.1.1 Compatibilitatea 13
4.1.2.2 Integrarea cu Microsoft Outlook, Outlook Express și Windows Mail 14
4.1.2.2.1 Adăugarea mesajelor etichetă la un corp de mesaj email 14
4.1.2.3 Eliminarea infiltrărilor 14
4.1.3 Protecția pentru acces Web 14
4.1.3.1 HTTP 15
4.1.3.1.1 Adrese blocate/excluse 15
4.1.3.1.2 Browsere Web 15
4.1.4 Scanarea calculatorului 16
4.1.4.1 Tipurile de scanare 16
4.1.4.1.1 Scanarea standard 16
4.1.4.1.2 Scanarea personalizată 16
4.1.4.2 Ținte de scanare 16
4.1.4.3 Profile de scanare 16
4.1.5 Setarea parametrilor pentru motorul ThreatSense 17
4.1.5.1 Setarea obiectelor 17
4.1.5.2 Opțiuni 17
4.1.5.3 Curățarea 18
4.1.5.4 Extensii 18
4.1.6 Se detectează o infiltrare 18
4.2 Actualizarea programului 19
4.2.1 Setarea actualizării 19
4.2.1.1 Profilele de actualizare 20
4.2.1.2 Setarea actualizării avansate 20
4.2.1.2.1 Modul de actualizare 20
4.2.1.2.2 Server proxy 20
4.2.1.2.3 Conectarea la LAN 21
4.2.1.2.4 Creare copii actualizare – oglindă 21
4.2.1.2.4.1 Actualizarea din oglindă 22
4.2.1.2.4.2 Depanarea problemelor la actualizarea din oglindă 23
4.2.2 Cum se creează sarcini de actualizare 23

ESET NOD32 Antivirus 3.0

Serviciu pentru clienți internațional: www.eset.eu/support
Serviciu pentru clienți din America de Nord: www.eset.com/support

REV.20080609-001

4.3 Planificatorul 23
4.3.1 Scopul sarcinilor planificate 23
4.3.2 Crearea de sarcini noi 23
4.4 Carantina 24
4.4.1 Plasarea fișierelor în carantină 24
4.4.2 Restaurarea din carantină 24
4.4.3 Trimiterea unui fișier din carantină 24
4.5 Fișierele log 25
4.5.1 Mentenanța fișierelor log 25
4.6 Interfața pentru utilizator 25
4.6.1 Alerte și notificări 26
4.7 ThreatSense.Net 27
4.7.1 Fișierele suspecte 27
4.7.2 Statisticile 28
4.7.3 Trimiterea 28
4.8 Administrarea la distanță 28
4.9 Licența 29

5. Utilizatorii avansați 30

5.1 Setarea serverului proxy 30
5.2 Importul/exportul setărilor 30
5.2.1 Exportul setărilor 30
5.2.2 Importul setărilor 30
5.3 Linia de comandă 31

6. Glosar 32

6.1 Tipuri de infiltrări 32
6.1.1 Viruși 32
6.1.2 Viermi 32
6.1.3 Troieni 32
6.1.4 Rootkit-uri 32
6.1.5 Adware 33
6.1.6 Spyware 33
6.1.7 Aplicații potențial periculoase 33
6.1.8 Aplicații potențial periculoase 33

1. ESET NOD32 Antivirus 3.0

ESET NOD32 Antivirus 3.0 este succesorul produsului premiat ESET NOD32 Antivirus 2.*. Produsul folosește viteza de scanare și precizia ESET NOD32 Antivirus, care sunt asigurate de cea mai recentă versiune a motorului de scanare ThreatSense®.

Tehnicile avansate implementate sunt capabile să blocheze proactiv viruși, spyware, troieni, viermi, adware și rootkit-uri fără a încetini sistemul și fără a vă deranja în timp ce lucrați sau vă jucați pe calculator.

1.1 Ce este nou

Experiența îndelungată a experților noștri în domeniul dezvoltării este demonstrată de arhitectura complet nouă a programului ESET NOD32 Antivirus, care garantează detecție maximă cu cerințe minime de sistem.

- **Antivirus și antispyware**

Acest modul se bazează pe centrul de scanare ThreatSense®, folosit pentru prima dată în sistemul premiat NOD 32 Antivirus. Centrul ThreatSense® este optimizat și îmbunătățit cu noua arhitectură ESET NOD32 Antivirus.

Caracteristică	Descriere
Curățare îmbunătățită	Sistemul antivirus curăță și șterge acum în mod inteligent majoritatea infiltrărilor detectate, fără a necesita intervenția utilizatorului.
Mod Scanare în fundal	Scanarea calculatorului poate fi lansată în fundal, fără a încetini performanțele sistemului.
Fișiere de actualizare de dimensiuni mai mici	Procesele de optimizare a centrului păstrează fișierele de actualizări la dimensiuni mai mici decât în versiunea 2.7. De asemenea, a fost îmbunătățită protecția fișierelor de actualizare împotriva deteriorărilor.
Protecție pentru clienții de email populari	Acum este posibil să scanați mesajele de corespondență primite nu numai în MS Outlook, dar și în Outlook Express și Windows Mail.
O varietate de alte îmbunătățiri minore	– Accesul direct la sisteme de fișiere, pentru viteză și rezultate ridicate. – Blocarea accesului la fișierele infectate – Optimizare pentru Windows Security Center, inclusiv pentru Vista.

1.2 Cerințe de sistem

Pentru funcționarea fără probleme a programului ESET NOD32 Antivirus, sistemul dvs. trebuie să îndeplinească următoarele cerințe hardware și software:

ESET NOD32 Antivirus:

Windows 2000, XP	400 MHz 32 de biți / 64 de biți (x86 / x64) 128 MB de RAM pentru memoria sistemului Spațiu disponibil 35 MB Super VGA (800 x 600)
Windows Vista	1 GHz 32 de biți / 64 de biți (x86 / x64) Memorie de sistem de 512 MO de RAM Spațiu disponibil 35 MB Super VGA (800 × 600)

ESET NOD32 Antivirus Business Edition:

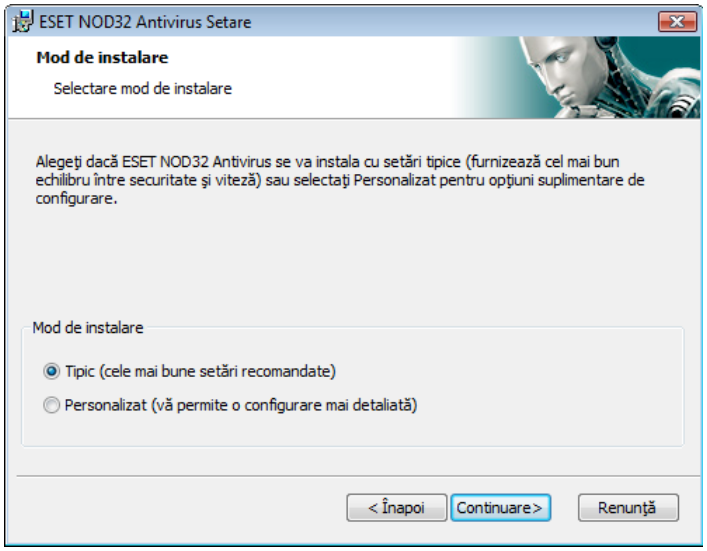
Windows 2000, 2000 Server, XP, 2003 Server	400 MHz 32 de biți / 64 de biți (x86 / x64) 128 MB de RAM pentru memoria sistemului Spațiu disponibil 35 MB Super VGA (800 x 600)
Windows Vista, Windows Server 2008	1 GHz 32 de biți / 64 de biți (x86 / x64) 512 MB de RAM pentru memoria sistemului Spațiu disponibil 35 MB Super VGA (800 x 600)

2. Instalare

După achiziționare, programul de instalare ESET NOD32 Antivirus se poate descărca de pe site-ul Web al ESET sub forma unui pachet .msi. Lansați programul de instalare și expertul de instalare vă va ghida prin procesul de setare elementară. Există două tipuri de instalare disponibile, cu niveluri diferite de detalii de setare:

1. Instalare tipică

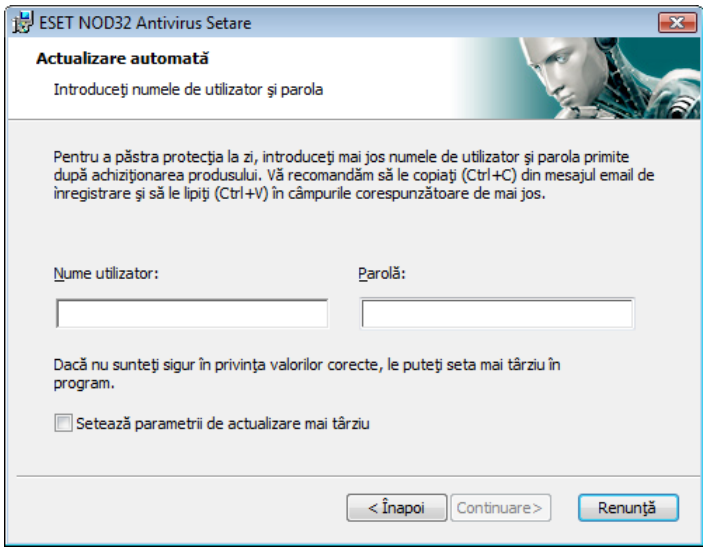
2. Instalare personalizată



2.1 Instalare tipică

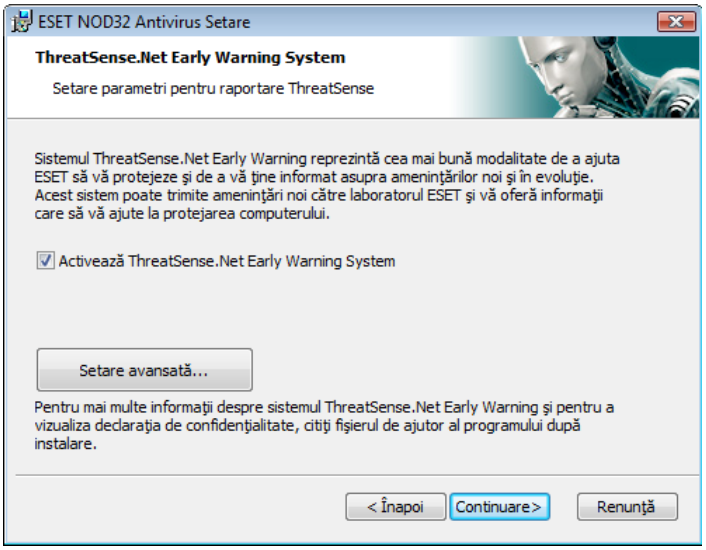
Instalarea tipică este recomandată pentru utilizatori care doresc să instaleze ESET NOD32 Antivirus cu setările implicite. Setările implicite ale programului oferă nivelul maxim de protecție; acest fapt este apreciat de utilizatorii care nu doresc să configureze setări detaliate.

Primul pas (foarte important) îl reprezintă introducerea numelui de utilizator și a parolei pentru actualizarea automată a programului. Acesta joacă un rol important în oferirea unei protecții constante sistemului.



Introduceți **numele dvs. de utilizator** și **parola**, adică datele de autentificare pe care le-ați primit după achiziționarea sau înregistrarea produsului, în câmpurile corespunzătoare. Dacă în momentul respectiv nu aveți la îndemână numele dvs. de utilizator și parola, selectați opțiunea **Setează parametrii de actualizare mai târziu**. Datele de autentificare pot fi introduse oricând ulterior, direct din program.

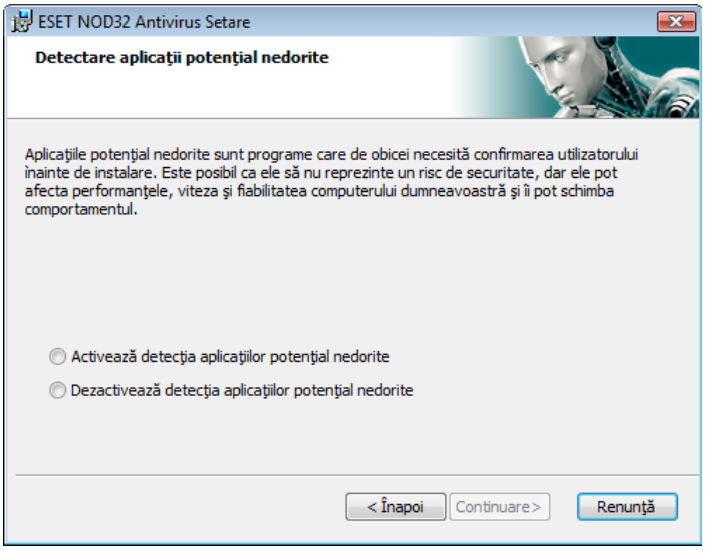
Următorul pas al instalării îl reprezintă configurarea ThreatSense. Net Early Warning System. ThreatSense.Net Early Warning System vă ajută să vă asigurați că ESET este informată imediat și în permanență despre infiltrări noi, pentru a-și proteja rapid clienții. Sistemul permite trimiterea de amenințări noi către laboratoarele ESET pentru viruși, în care acestea sunt analizate, procesate și adăugate la bazele de semnături.



În mod implicit, caseta de selectare **Enable ThreatSense.Net Early Warning System** este selectată pentru a se activa această caracteristică. Faceți clic pe **Setare avansată...** pentru a modifica setări avansate pentru trimiterea de fișiere suspecte.

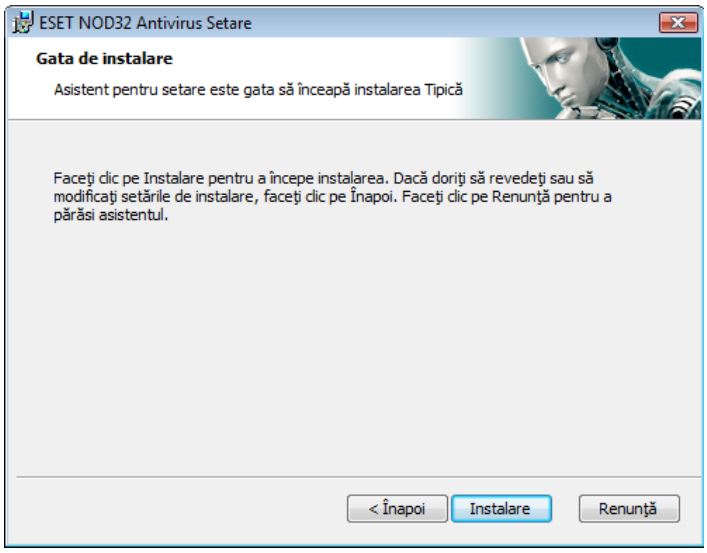
Următorul pas al procesului de instalare îl reprezintă configurarea **detectării aplicațiilor potențial nedorite**. Aplicațiile potențial nedorite nu sunt în mod obligatoriu menite să fie dăunătoare, dar ele pot adesea afecta în sens negativ comportamentul sistemului de operare.

Aceste aplicații sunt adesea împachetate cu alte programe și poate fi dificilă observarea lor în timpul procesului de instalare. Deși, de obicei, aceste aplicații afișează o notificare în timpul instalării, ele pot fi instalate cu ușurință fără permisiunea dvs.



Selectați opțiunea **Activează detecția aplicațiilor potențial nedorite** pentru a permite detectarea acestui tip de amenințare de către ESET NOD32 Antivirus (recomandat).

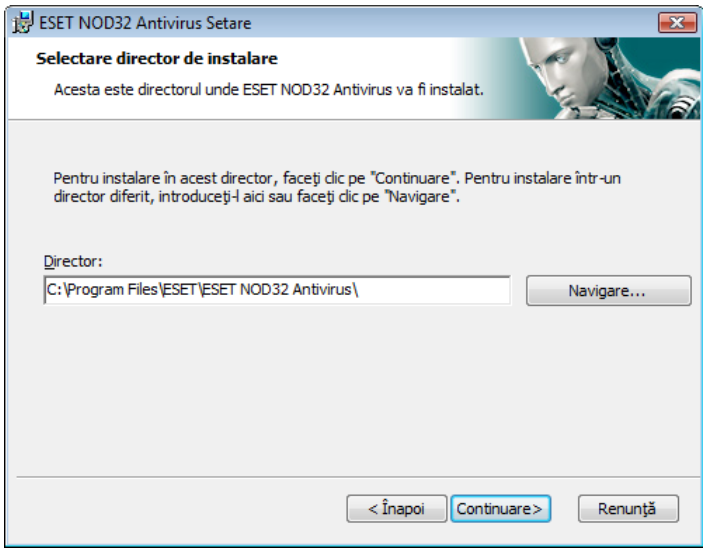
Ultimul pas în modul Instalare tipică îl reprezintă confirmarea instalării făcând clic pe butonul **Instalare**.



2.2 Instalare personalizată

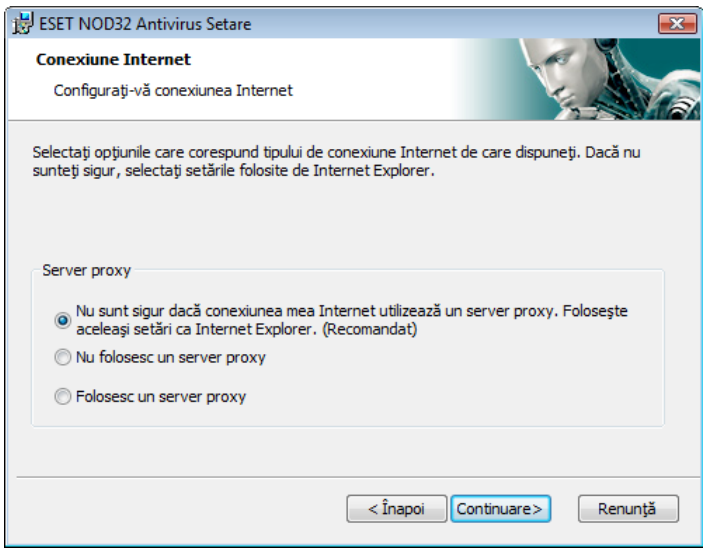
Personalizată Instalarea personalizată este concepută pentru utilizatori care au experiență setarea amănunțită a programelor și care doresc să modifice setări avansate în timpul instalării.

Primul pas îl reprezintă selectarea locației directorului de instalare. În mod implicit, programul se instalează în directorul C:\Fișiere program\ESET\ESET Smart Security\. Faceți clic pe **Răsfoiește...** pentru a schimba locația (nerecomandat).

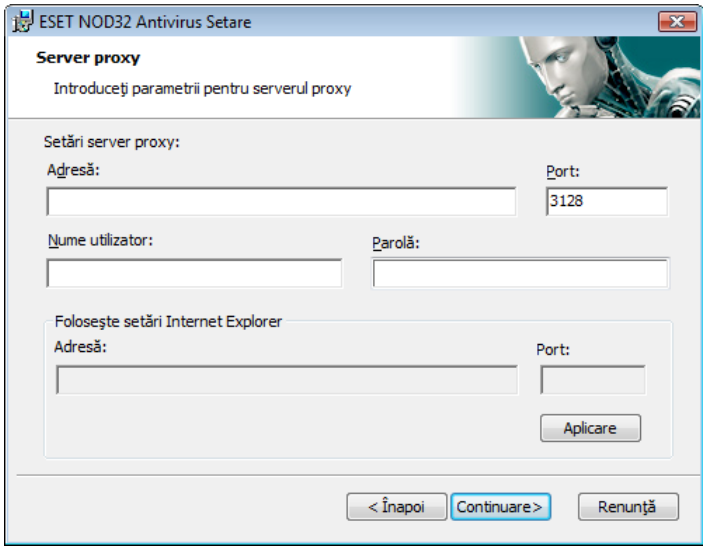


Apoi **introduceți numele dvs. de utilizator și parola**. Acest pas coincide cu cel din Instalare tipică (vezi pagina 5).

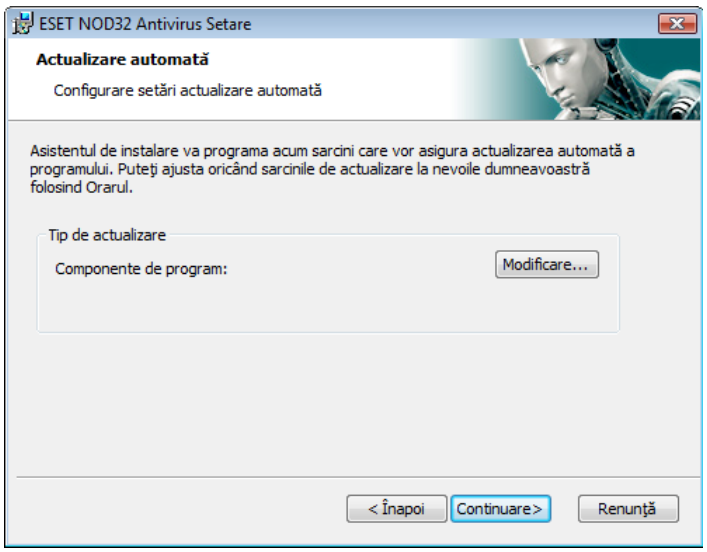
După ce introduceți numele dvs. de utilizator și parola, faceți clic pe **Următorul** pentru a **configura conexiunea dvs. Internet**.



Dacă utilizați un server proxy, acesta trebuie configurat corect pentru funcționarea corespunzătoare a actualizărilor de semnături. Dacă nu știți dacă folosiți un server proxy pentru a vă conecta la Internet, lăsați setarea implicită **Nu sunt sigur dacă conexiunea mea Internet folosește un server proxy. Folosește aceleași setări ca Internet Explorer** și faceți clic pe **Următorul**. Dacă nu utilizați un server proxy, selectați opțiunea corespunzătoare.

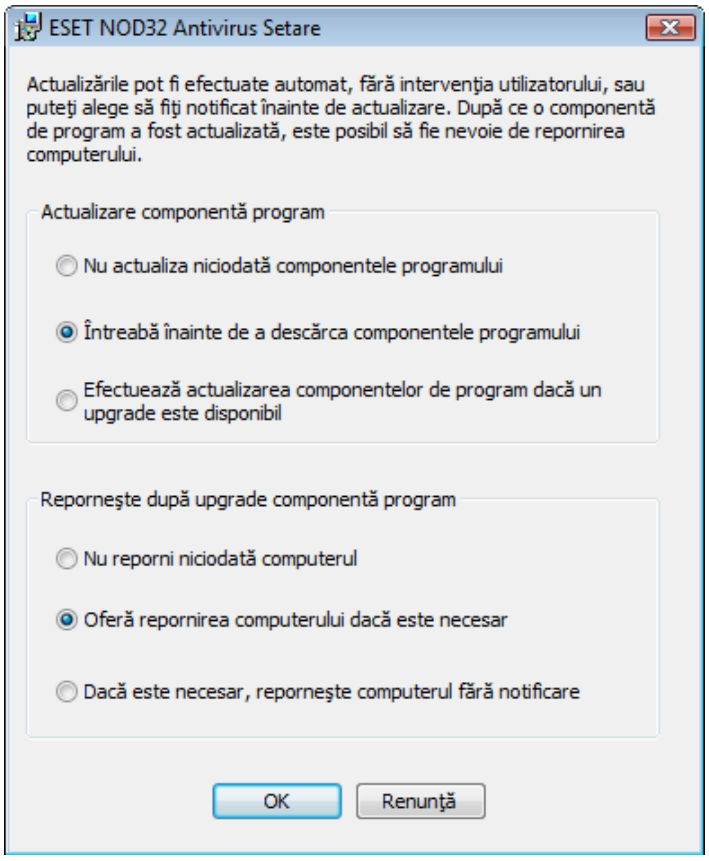


Pentru a configura setările pentru serverul dvs. proxy, selectați **Folosesc un server proxy** și faceți clic pe **Următorul**. Introduceți adresa IP sau adresa URL a serverului dvs. proxy în câmpul **Adresă.** În câmpul **Port**, specificați portul prin care serverul proxy acceptă conexiunile (în mod implicit, acesta este 3128). În eventualitatea în care serverul proxy necesită autentificare, trebuie introduse un nume de utilizator și o parolă valide, pentru a obține acces la serverul proxy. De asemenea, setările serverului pot fi copiate din Internet Explorer, dacă se dorește. Pentru a proceda astfel, faceți clic pe **Aplicare** și confirmați selecția.



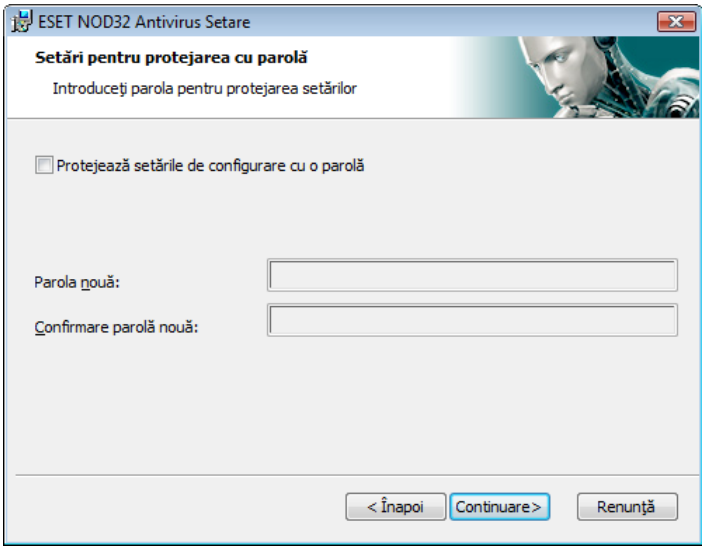
Faceţi clic pe **Următorul** pentru a trece la fereastra **Configurare setări actualizare automată**. Acest pas vă permite să desemnaţi modul în care vor fi tratate actualizările automate ale componentelor programului pe sistemul dvs. Faceţi clic pe **Modificare...** pentru a accesa setările avansate.

Dacă nu doriţi să fie actualizate componentele programului, selectaţi **Nu actualiza niciodată componentele programului**. Activarea opţiunii **Întreabă înainte de a descărca componentele programului** determină afişarea unei ferestre de confirmare înainte de descărcarea componentelor de program. Pentru a activa upgrade-ul automat pentru componentele programului fără a mai fi solicitat în acest sens, selectaţi opţiunea **Efectuează actualizarea componentelor de program dacă un upgrade este disponibil**.



NOTĂ: De obicei, după efectuarea unui upgrade pentru componentele programului, este necesară o repornire. Setarea recomandată este: **Dacă este necesar, reporneşte calculatorul fără notificare**.

Următorul pas al instalării este introducerea unei parole pentru protejarea parametrilor programului. Alegeţi o parolă cu care doriţi să protejaţi programul. Tastaţi din nou parola pentru confirmare.

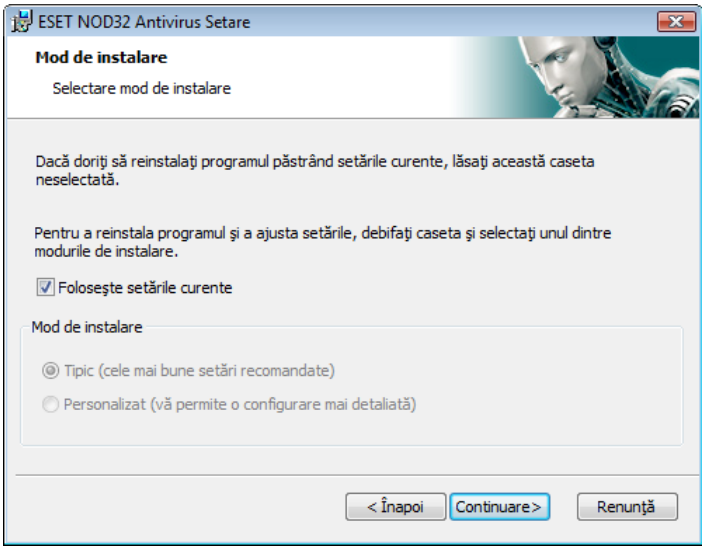


Paşii **Configurarea ThreatSense.Net Early Warning System** şi **Detectarea aplicaţiilor potenţial nedorite** coincid cu cei pentru Instalarea tipică şi nu sunt afişaţi aici (vezi pagina 5).

În ultimul pas se afişează o fereastră în care vi se solicită acordul pentru instalare.

2.3 Utilizarea setărilor originale

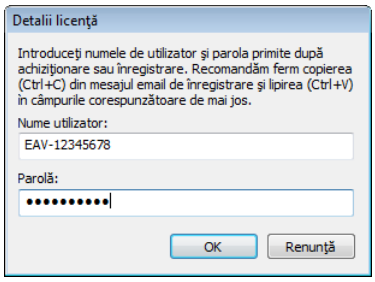
Dacă instalaţi din nou ESET NOD32 Antivirus, se afişează opţiunea **Foloseşte setările curente**. Selectaţi această opţiune pentru a transfera parametrii de setare din instalarea originală în cea nouă.



2.4 Introducerea numelui de utilizator şi a parolei

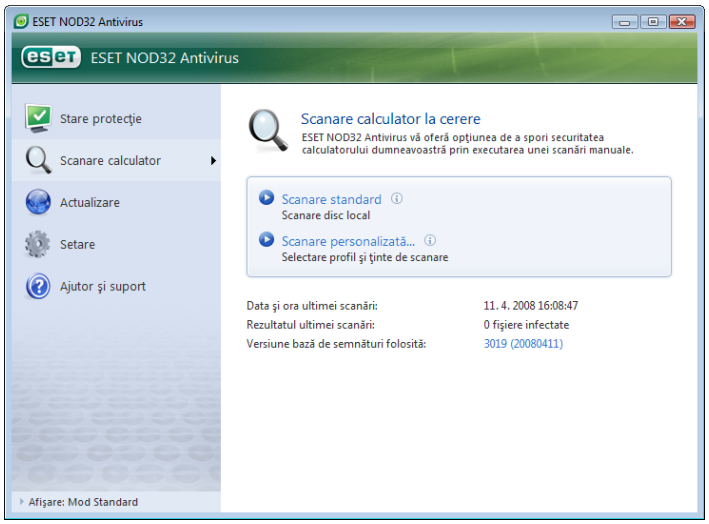
Pentru o funcţionalitate optimă, este important ca programul să fie actualizat automat. Acest lucru este posibil numai dacă în setarea de actualizare sunt introduse numele de utilizator şi parola corecte.

Dacă nu ați introdus numele dvs. de utilizator și parola în timpul instalării, puteți face acum acest lucru. În fereastra principală a programului, faceți clic pe **Actualizare** și apoi pe **Setare nume utilizator și parolă...** Introduceți datele primite împreună cu licența de produs în fereastra **Detalii licență**.



2.5 Scanarea calculatorului la cerere

După instalarea ESET NOD32 Antivirus, trebuie efectuată o scanare a calculatorului pentru detectarea prezenței codului malware. Pentru a lansa rapid o scanare, selectați **Scanare calculator** în meniul principal și apoi **Scanare standard** în fereastra principală a programului. Pentru mai multe informații despre caracteristica de scanare a calculatorului, consultați capitolul „Scanarea calculatorului”.



3. Ghidul începătorului

Acest capitol oferă o prezentare generală inițială a programului ESET NOD32 Antivirus și a setărilor de bază ale acestuia.

3.1 Prezentarea designului interfeței pentru utilizator – moduri

Fereastra principală a ESET NOD32 Antivirus este împărțită în două secțiuni principale. Coloana din stânga oferă acces la meniul principal prietenos. Fereastra principală a programului din dreapta servește în primul rând la afișarea informațiilor corespunzătoare opțiunii selectate în meniul principal.

În continuare sunt descrise butoanele din meniul principal:

Stare protecție – Într-o formă prietenoasă, aceasta oferă informații despre starea protecției ESET Smart Security. Dacă este activat modul Avansat, se afișează starea tuturor modulelor de protecție. Faceți clic pe un modul pentru a-i vizualiza starea curentă.

Scanare computer – această secțiune permite utilizatorului să configureze și să lanseze scanarea computerului la cerere.

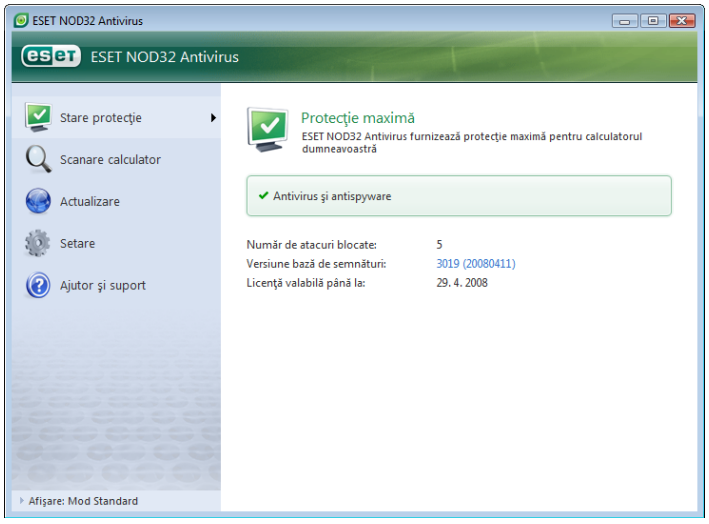
Actualizare – Selectați această opțiune pentru a accesa modulul de actualizare care gestionează actualizările bazei de date de semnături.

Setare – selectați această opțiune pentru a regla nivelul de securitate a calculatorului. Dacă este activat modul Avansat, se afișează submeniurile modulului Protecție antivirus și antispyware.

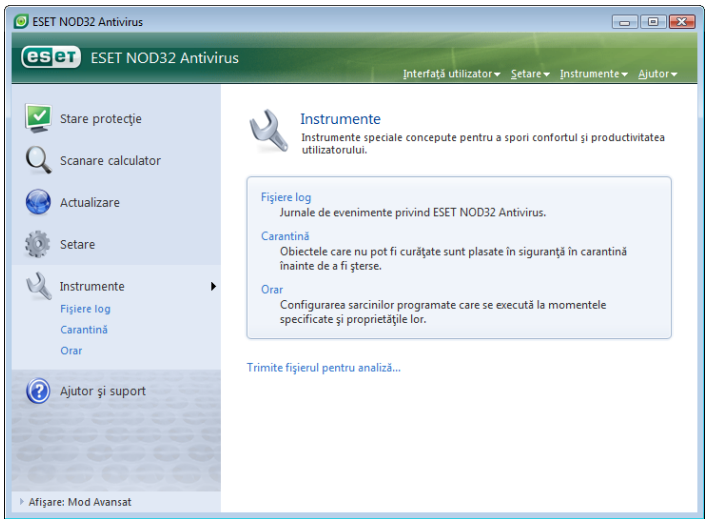
Instrumente – această opțiune este disponibilă numai în modul Avansat Asigură acces la Fișierele log, la Carantină și la Orar.

Ajutor și suport – Selectați această opțiune pentru a accesa fișiere de ajutor, Baza de cunoștințe ESET, site-ul Web ESET și o solicitare de asistență pentru serviciul pentru clienți.

Interfața pentru utilizator ESET NOD32 Antivirus permite utilizatorilor să comute între modurile Standard și Avansat. Pentru a comuta între moduri, accesați legătura **Afișare** amplasată în colțul din stânga-jos al ecranului principal al ESET NOD32 Antivirus. Faceți clic pe acest buton pentru a selecta modul de afișare dorit.



Modul Standard oferă acces la caracteristici necesare pentru operațiile obișnuite. Acesta nu afișează nicio opțiune avansată.

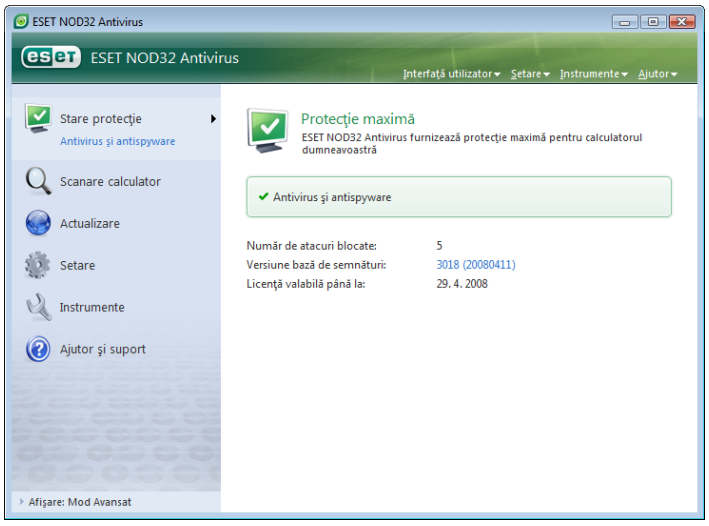


Dacă se comută la modul Avansat, la meniul principal se adaugă opțiunea **Instrumente**. Opțiunea Instrumente permite utilizatorului să acceseze Orarul și Carantina sau să vizualizeze Fișierele log ale ESET NOD32 Antivirus.

NOTĂ: Toate instrucțiunile prezentate în continuare în acest ghid se referă la modul Avansat.

3.1.1 Verificarea funcționării sistemului

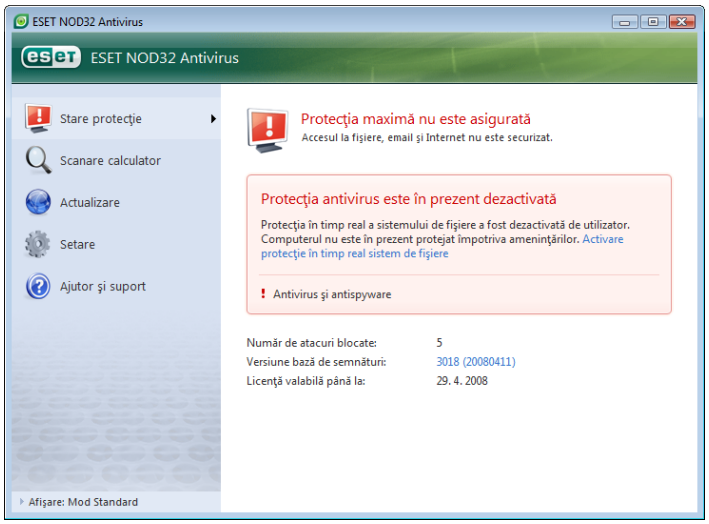
Pentru a vizualiza **Stare protecție**, faceți clic pe această opțiune din partea de sus a meniului principal. Submeniul **Antivirus și antispyware** va apărea imediat dedesubt, iar în fereastra principală a programului se va afișa un rezumat al stării funcționării ESET NOD32 Antivirus. Dacă faceți clic pe Antivirus și antispyware, în fereastra principală a programului se va afișa starea fiecărui modul de protecție



Dacă modulele activate funcționează corespunzător, acestora li se atribuie câte o bifă verde. În caz contrar, se afișează un semn de exclamare roșu sau o pictogramă de notificare portocalie și sunt prezentate informații suplimentare despre modul în partea de sus a ferestrei. De asemenea, se afișează o soluție sugerată pentru repararea modulului. Pentru a modifica starea unui anumit modul, faceți clic pe **Setare** în meniul principal și apoi pe modulul dorit.

3.1.2 Ce este de făcut dacă programul nu funcționează corect

Dacă ESET NOD32 Antivirus detectează o problemă în oricare dintre modulele sale de protecție, aceasta este raportată în fereastra **Stare protecție**. De asemenea, în acest ecran este oferită o posibilă soluție la problemă.

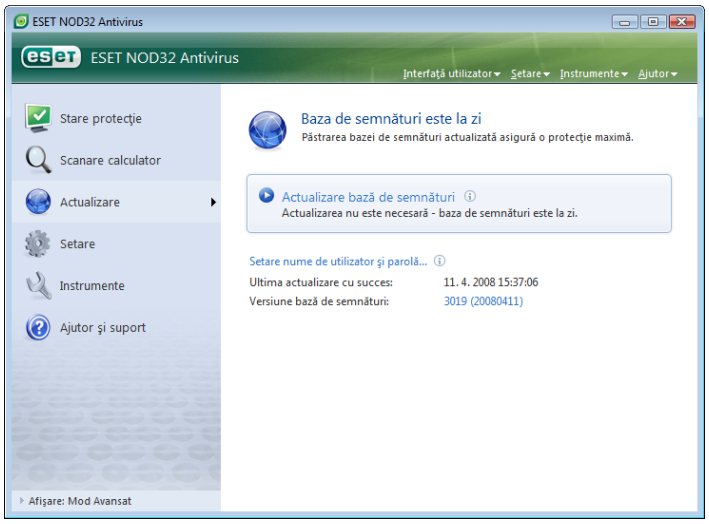


Dacă nu este posibilă rezolvarea unei probleme folosind lista de probleme și soluții cunoscute afișată, faceți clic pe **Ajutor și suport** pentru a accesa fișierele de ajutor sau căutați în Baza de cunoștințe. Dacă, în continuare, nu se poate găsi o soluție, puteți trimite o solicitare de asistență la Servicul pentru clienți ESET. Pe baza acestui feedback, specialiștii noștri pot răspunde prompt la întrebările dvs. și vă pot acorda sfaturi utile în legătură cu problema.

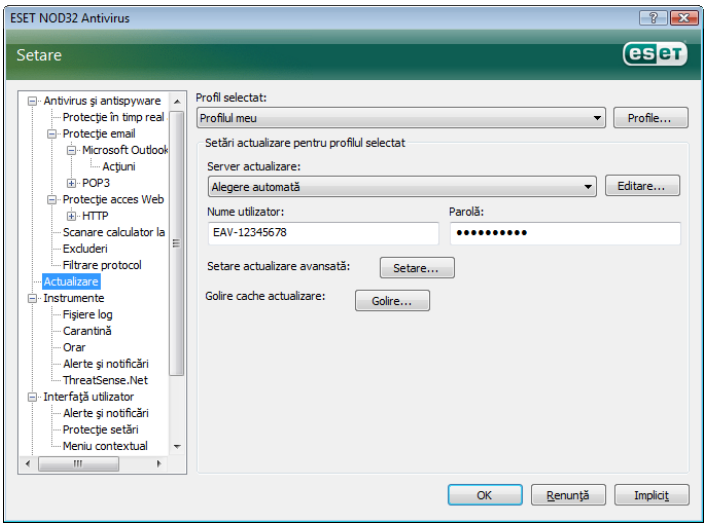
3.2 Setarea actualizării

Actualizarea bazei de semnături și actualizarea componentelor programului sunt aspecte importante în oferirea protecției complete împotriva codului malware. Acordați atenție specială configurării și funcționării acestora. Din meniul principal, selectați **Actualizare** și apoi faceți clic pe **Actualizare bază de semnături** în fereastra principală a programului pentru a verifica instantaneu disponibilitatea unei actualizări mai recente a bazei de date. **Setare nume utilizator și parolă...** afișează o casetă de dialog în care trebuie introduse numele de utilizator și parola primite în momentul achiziționării.

Dacă numele de utilizator și parola au fost introduse în timpul instalării ESET NOD32 Antivirus, nu vi se va solicita introducerea acestora în acest moment.

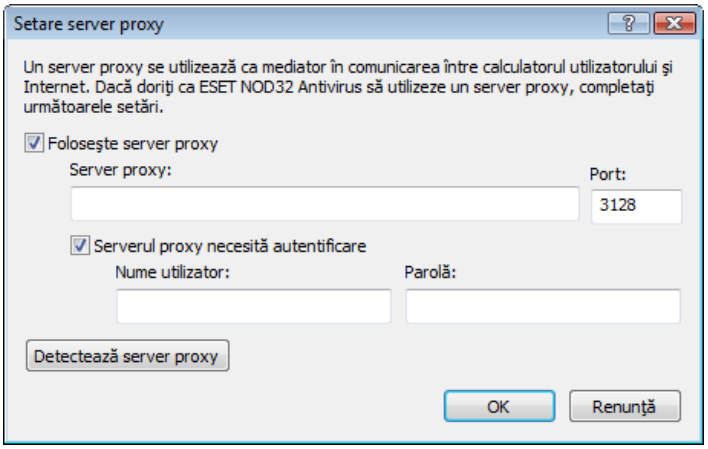


Fereastra **Setare avansată** (pentru a o accesa, apăsați pe F5) conține alte opțiuni detaliate pentru actualizare. **Serverul de actualizare:** meniul vertical trebuie setat la **Alegere automată**. Pentru a configura opțiuni de actualizare avansate precum modul de actualizare, accesul la serverul proxy, accesarea actualizărilor pe un server local și crearea de copii ale semnăturilor (ESET NOD32 Antivirus Business Edition), faceți clic pe butonul **Setare...**.



3.3 Setare server proxy

Dacă utilizați un server proxy pentru a media conexiunea la Internet pe un sistem care utilizează ESET Smart Security, acesta trebuie specificat în Setare avansată (F5). Pentru a accesa fereastra de configurare **Server proxy**, faceți clic pe **Diverse > Server proxy** în arborele de setare avansată. Selectați caseta de selectare **Folosește server proxy** și introduceți adresa IP și portul serverului proxy, împreună cu datele de autentificare pentru acesta.



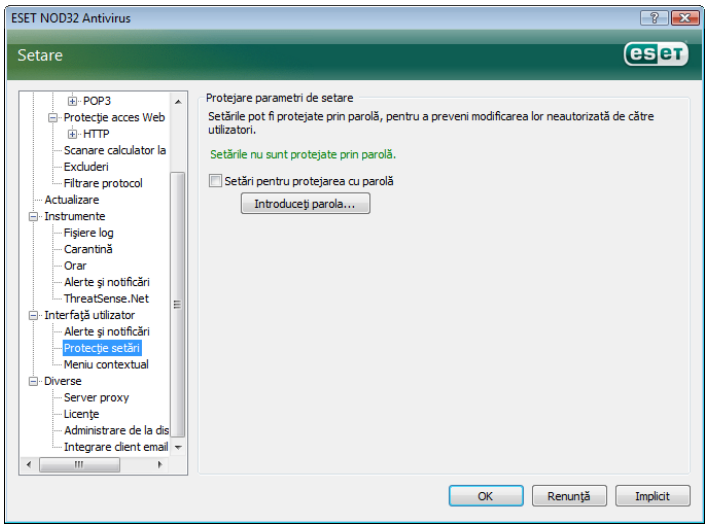
Dacă acest informații nu sunt disponibile, puteți încerca să detectați automat setările de server proxy pentru ESET NOD32 Antivirus făcând clic pe butonul **Detectează server proxy**.

NOTĂ: Este posibil ca opțiunile pentru serverul proxy să difere în funcție de profilul de actualizare. În acest caz, configurați serverul proxy în Setare actualizare avansată

3.4 Protecția setărilor

Setările ESET NOD32 Antivirus Settings pot fi foarte importante din punctul de vedere al politicii de siguranță a organizației dvs. Modificările neautorizate pot periclita stabilitatea și protecția sistemului dvs. Pentru a proteja prin parolă parametrii de setare, deschideți meniul principal și faceți clic pe **Setare > Intrare în tot arborele de setare avansată... > Interfață utilizator > Protecție setări** și faceți clic pe butonul **Introduceți parola...**.

Introduceți o parolă, introduceți-o din nou pentru a o confirma și faceți clic pe **OK**. Parola va fi necesară pentru oricare modificări ulterioare ale setărilor ESET NOD32 Antivirus.



4. Lucrul cu ESET NOD32 Antivirus

4.1 Protecția antivirus și antispyware

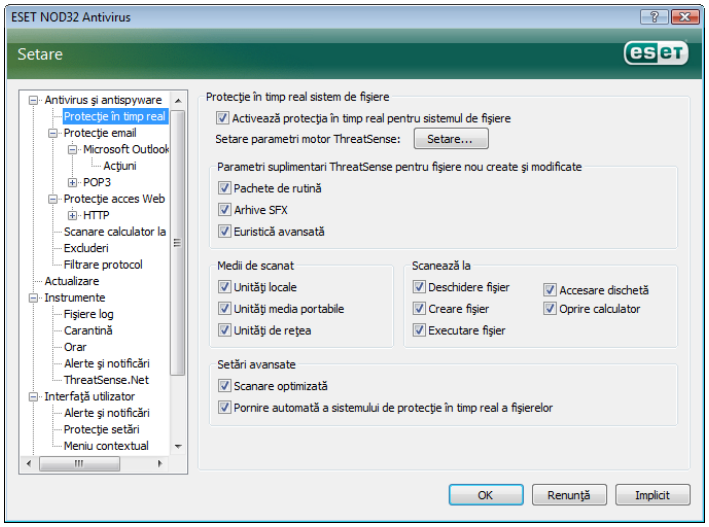
Protecția antivirus vă protejează împotriva atacurilor dăunătoare asupra sistemului prin controlarea fișierelor, mesajelor de email și comunicării Internet. Dacă se detectează o amenințare cu cod dăunător, modulul Antivirus o poate elimina mai întâi prin blocarea ei și apoi prin curățarea, ștergerea sau mutarea sa în carantină.

4.1.1 Protecția-protecție în timp real a sistemului de fișiere

Protecția în timp real pentru sistemul de fișiere controlează toate evenimentele din sistem legate deantivirus. Sunt scanate pentru cod dăunător toate fișierele în momentul în care ele sunt deschise, create sau rulate pe computer. Protecția în timp real pentru sistemul de fișiere este lansată la pornirea sistemului.

4.1.1.1 Setarea controlului

Personalizată Protecția în timp real a sistemului de fișiere verifică toate tipurile de medii, iar controlul este declanșat de diferite evenimente. Controlul utilizează metodele de detecție ale tehnologiei ThreatSense (așa cum se descrie în Setare parametri motor ThreatSense). Comportamentul controlului poate varia pentru fișierele nou create și pentru cele existente. Se poate aplica un nivel mai avansat de control pentru fișierele nou create.



4.1.1.1.1 Scanarea mediilor

În mod implicit, sunt scanate toate tipurile de medii pentru amenințări potențiale.

Unități locale – Controlează toate unitățile de disc locale
Medii amovibile – Dischete, dispozitive de stocare USB etc.
Unități de rețea – Scanează toate unitățile mapate

Vă recomandăm să păstrați setările implicite și să nu le modificați decât în cazuri specifice, cum ar fi atunci când scanarea anumitor medii încetinește semnificativ transferurile de date.

4.1.1.1.2 Scanare declanșată de un eveniment

În mod implicit, toate fișierele sunt scanate la deschidere, executare sau creare. Vă recomandăm să păstrați setările implicite, deoarece acestea oferă nivelul maxim de protecție în timp real pentru calculator.

Opțiunea **Acces dischetă** oferă control pentru sectorul de boot al dischetei la accesarea acestei unități. Opțiunea **Închidere calculator** oferă control pentru sectoarele de boot ale discului fix în timpul închiderii computerului. Deși virușii de boot sunt rari astăzi, vă recomandăm să lăsați aceste opțiuni activate, deoarece încă mai există posibilitatea infectării cu un virus de boot de la alte surse.

4.1.1.1.3 Verificarea fișierelor nou create

Probabilitatea de infectare este semnificativ mai mare la fișierele nou create decât la cele existente. Din acest motiv programul verifică aceste fișiere cu parametri de scanare suplimentari. Pe lângă metodele comune de scanarepe bază de semnături, se utilizează euristică avansată, ce îmbunătățește semnificativ ratele de detecție. În plus față de fișierele nou create, scanarea este efectuată și pentru arhivele SFX și pachetele de rutină (fișiere executabile comprimate intern).

4.1.1.1.4 Setările avansate

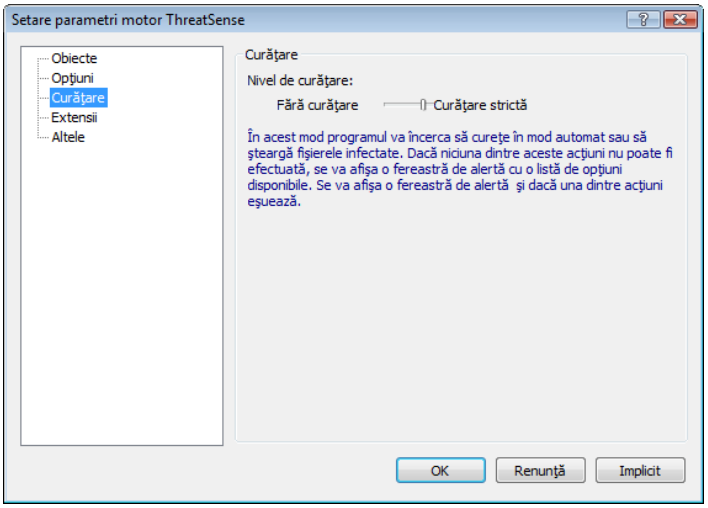
Pentru a furniza o amprentă minimă asupra sistemului la utilizarea protecției în timp real, fișierele care au fost deja scanate nu sunt scanate în mod repetat (decât dacă au fost modificate). Fișierele sunt scanate din nou imediat după fiecare actualizare a bazei de semnături. Acest comportament se configurează utilizând opțiunea **Scanare optimizată**. Dacă aceasta este dezactivată, sunt scanate toate fișierele de fiecare dată când sunt accesate.

În mod implicit, protecția în timp real este lansată în momentul pornirii sistemului de operare, furnizând scanare neîntreruptă. În cazuri deosebite (de ex. dacă există un conflict cu alt scanner în timp real), protecția în timp real poate fi terminată prin dezactivarea opțiunii **Pornire automată protecție în timp real sistem de fișiere**.

4.1.1.2 Nivele de curățare

PersonalizatăProtecția în timp real are trei nivele de curățare (pentru accesare, faceți clic pe butonul **Setare...** în secțiunea **Protecție în timp real sistem de fișiere** și apoi faceți clic pe ramificația **Curățare**).

- Primul nivel afișează o fereastră de alertă cu opțiuni disponibile pentru fiecare infiltrare găsită. Utilizatorul trebuie să aleagă o acțiune pentru fiecare infiltrare în parte. Acest nivel este conceput pentru utilizatorii mai avansați care știu cum să procedeze pentru fiecare tip de infiltrare.
- Nivelul mediu alege și efectuează automat o acțiune predefinită (în funcție de tipul de infiltrare). Detectarea și ștergerea unui fișier infectat este semnalată printr-un mesaj de informare localizat în colțul din dreapta jos al ecranului. Totuși, nu se efectuează automat o acțiune dacă infiltrarea este localizată într-o arhivă care conține și fișiere curate și acțiunea nu se efectuează la obiectele pentru care nu există o acțiune predefinită.
- Nivelul trei este cel mai „agresiv" – sunt curățate toate obiectele infectate. Deoarece acest nivel poate duce la pierderea de fișiere valabile, vă recomandăm să-l utilizați numai în situații specifice.



4.1.1.3 Când trebuie modificată configurația protecției în timp real Real

Protecția în timp real este componenta cea mai esențială pentru menținerea unui sistem sigur. Prin urmare, fiți atent atunci când modificați parametrii acesteia. Vă recomandăm să modificați parametrii acesteia numai în anumite cazuri. De exemplu, dacă există un conflict cu o anumită aplicație sau cu scannerul în timp real al unui alt program antivirus.

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 butonul **Implicit** amplasat în partea din dreapta-jos a ferestrei **Protecție în timp real sistem de fișiere** (**Setare avansată > Antivirus și antispyware > Protecție în timp real sistem de fișiere**).

4.1.1.4 Verificarea protecției în timp real

Pentru a verifica dacă protecția în timp real funcționează și detectează viruși, utilizați un fișier test de la eicar.com. Acest fișier test este un fișier special inofensiv, detectabil de către toate programele antivirus. Fișierul a fost creat de compania EICAR (Institutul european de cercetare antivirus pentru computer) pentru a testa funcționalitatea programelor antivirus. Fișierul eicar.com este disponibil pentru descărcare la adresa http://www.eicar.org/download/eicar.com

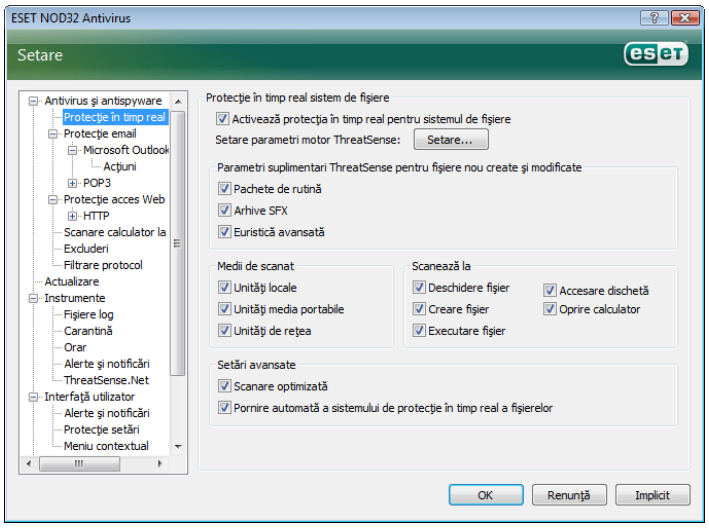
4.1.1.5 Ce este de făcut dacă protecția în timp real nu funcționează

În următorul capitol descriem situațiile problematice care pot să apară la utilizarea protecției în timp-real și modul de depanare a acestora.

Protecția în timp real este dezactivată

Dacă protecția în timpreal este dezactivată din neatenție de utilizator, ea trebuie reactivată. Pentru a reactiva protecția în timp real, navigați la **Setare > Antivirus și antispyware** și faceți clic pe **Activare** în secțiunea **Protecție în timp real sistem de fișiere** a ferestrei programului principal.

Dacă protecția în timp real nu este inițiată la pornirea sistemului, acest lucru se datorează probabil dezactivării opțiunii **Pornire automată protecție în timp real sistem de fișiere**. Pentru a activa această opțiune, navigați la **Setare avansată** (F5) și faceți clic pe **Protecție în timp real sistem de fișiere** în arborele de setare avansată. În secțiunea **Setare avansată** din partea de jos a ferestrei, asigurați-vă că este bifată caseta de selectare **Pornire automată protecție în timp real sistem de fișiere**.



Protecția în timp real nu detectează și nu curăță infiltrările

Asigurați-vă că pe computer nu mai sunt instalate alte programe antivirus. Dacă suntactivate simultan două scuturi de protecție antivirus, acestea pot intra în conflict. Vă recomandăm să dezinstalați orice alte programe antivirus de pe sistemul dvs.

Protecția în timp real nu pornește

Dacă protecția în timp real nu s-a inițiat la pornirea sistemului (iar opțiunea **Pornire automată protecție în timp real sistem de fișiere** este activată), aceasta se poate datora conflictelor cu alte programe. În acest caz contactați specialiștii de la departamentul de Asistență Clienți al ESET.

4.1.2 Protecția pentru email

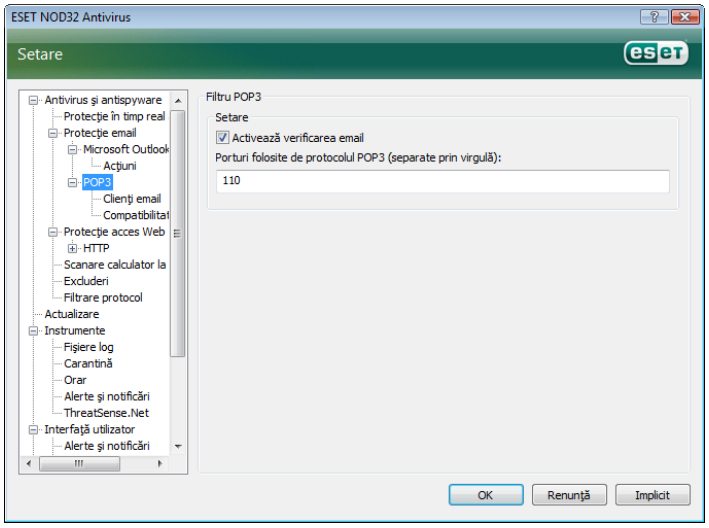
Protecția pentru email oferă controlul asupra comunicării prin mesaje email primite prin protocolul POP3. Utilizând programul insert pentru Microsoft Outlook, ESET NOD32 Antivirus oferă controlul asupra tuturor comunicărilor din clientul de email (POP3, MAPI, IMAP, HTTP). La examinarea mesajelor la intrare, programul utilizează toate metodele de scanare avansată oferite de motorul de scanare ThreatSense. Acest lucru înseamnă că detectarea programelor dăunătoare are loc chiar înainte de a fi comparate cu baza de semnături. Scanarea comunicărilor prin protocolul POP3 se face independent de clientul de email folosit.

4.1.2.1 Verificarea POP3

Protocolul POP3 este cel mai răspândit protocol utilizat pentru a primi comunicări prin email într-o aplicație de client email. ESET NOD32 Antivirus oferă protecție pentru acest protocol, indiferent de clientul de email utilizat.

Modulul care oferă acest control este inițiat automat în momentul pornirii sistemului de operare și este apoi activ în memorie. Pentru ca modulul să funcționeze corect, asigurați-vă că acesta este activat – verificarea 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 de porturi trebuie separate printr-o virgulă.

Comunicarea criptată nu este controlată.



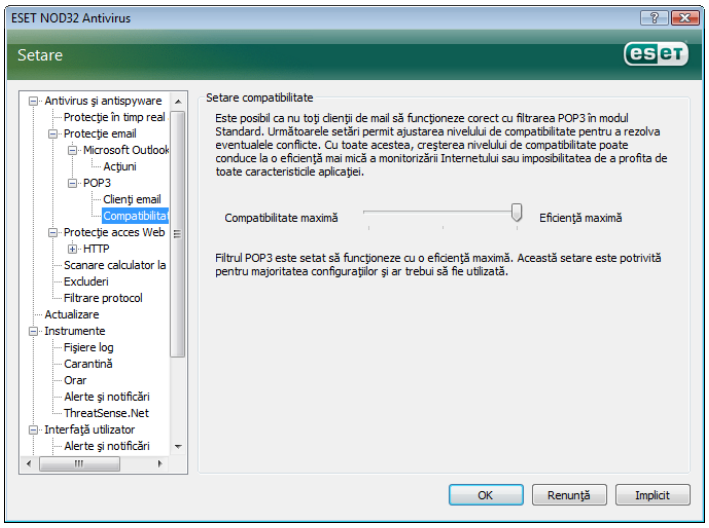
4.1.2.1.1 Compatibilitatea

La anumite programe de email puteți întâlni probleme la filtrarea POP3 (de ex. dacă primiți mesaje printr-o conexiune Internet lentă, pot apărea temporizări datorită verificării). În acest caz încercați să modificați modul în care se efectuează controlul. Micșorarea nivelului de control poate îmbunătăți viteza procesului de curățare. Pentru a regla nivelul de control al filtrării POP3, navigați la **Antivirus și antispyware > Protecție email > POP3 > Compatibilitate**.

Dacă este activată opțiunea **Eficiență maximă**, infiltrările sunt eliminate din mesajele infectate și informațiile despre infiltrare sunt introduse înainte de subiectul original al mesajului email (trebuie activate opțiunile **Ștergere** sau **Curățare** sau trebuie activat nivelul de curățare **maxim** sau **mediu**

Compatibilitatea medie modifică modul în care sunt primite mesajele. Mesajele sunt trimise către clientul de email în mod gradat – după ce s-a transferat și ultima parte a mesajului, acesta va fi scanat pentru infiltrări. Totuși, riscul de infectare crește la acest nivel de control. Nivelul de curățare și gestionare a mesajelor etichetă (alerte de notificări care sunt adăugate la linia de subiect și în corpul mesajelor email) este identic cu setarea pentru eficiență maximă.

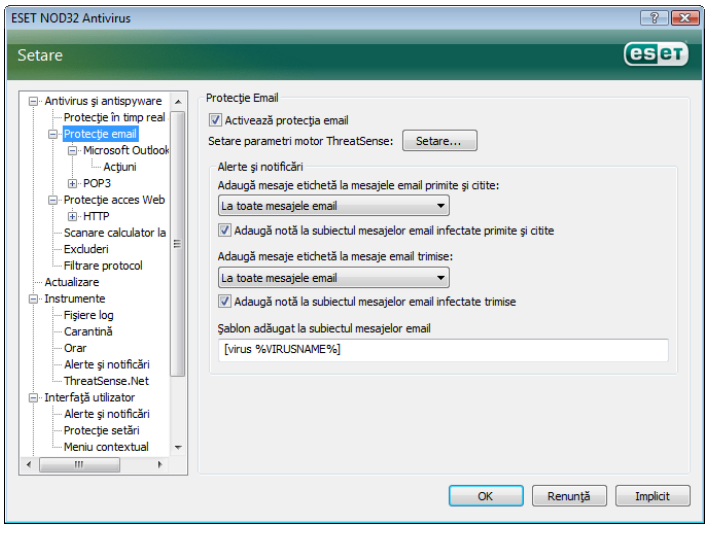
La nivelul **Compatibilitate maximă**, utilizatorul este avertizat printr-o fereastră de alertă care raportează primirea unui mesaj infectat. În linia de subiect sau în corpul mesajului pentru mesajele livrate nu sunt adăugate informații despre fișierele infectate, iar infiltrările nu sunt eliminate automat. Ștergerea infiltrărilor trebuie efectuată de către utilizator, din clientul de email.



4.1.2.2 Integrarea cu Microsoft Outlook, Outlook Express și Windows Mail

Integrarea ESET NOD32 Antivirus cu clienți de email sporește nivelul protecției active împotriva codului dăunător din mesajele de email. Dacă clientul dvs. de email este acceptat, această integrare se poate activa în ESET Smart Security. Dacă integrarea este activată, bara de instrumente ESET NOD32 Antivirus este introdusă direct în clientul de email, permițând o protecție mai eficientă a comunicării prin email. Setările de integrare sunt disponibile în secțiunea **Setare > Intrare în tot arborele de setare avansată... > Diverse > Integrare client email**. Această fereastră de dialog vă permite să activați integrarea cu clienții de email acceptați. Clienții de email acceptați actualmente includ Microsoft Outlook, Outlook Express și Windows Mail.

Protecția email se pornește prin activarea casetei de selectare **Activează protecția email** din ramificația **Setare avansată (F5) > Antivirus și antispyware** > **Protecție email**.



4.1.2.2.1 Adăugarea mesajelor etichetă la un corp de mesaj email

Fiecare email controlat de ESET NOD32 Antivirus poate fi marcat prin adăugarea unui mesaj etichetă la subiectul sau la corpul mesajului email. Această caracteristică sporește nivelul de credibilitate pentru destinatar și, dacă se detectează o infiltrare, aceasta oferă informații valoroase despre nivelul de amenințare al mesajului de email/ expeditorului respectiv.

Opțiunile pentru această funcționalitate sunt disponibile în secțiunea **Setare avansată > Protecție antivirus > Protecție email**. Programul poate **adăuga mesaje etichetă la mesajele email primite și citite**, dar și **adăuga mesaje etichetă la mesajele email trimise**. De asemenea, utilizatorul are posibilitatea să decidă dacă mesajele etichetă trebuie adăugate la toate mesajele de email, numai la cele infectate sau la niciunul.

În plus, ESET NOD32 Antivirus permite utilizatorului să adauge mesaje la subiectul original al mesajelor infectate. Pentru a activa adăugarea la subiect, selectați opțiunile **Adaugă notă la subiectul mesajelor email infectate primite și citite** și **Adaugă notă la subiectul mesajelor email infectate trimise**.

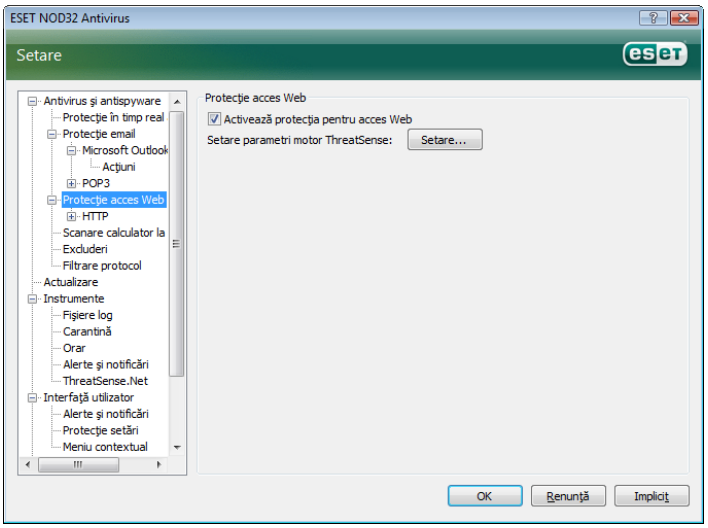
Conținutul notificărilor poate fi modificat în câmpul Șablon adăugat la subiectul mesajelor email infectate. Modificările menționate mai sus pot ajuta la automatizarea procesului de filtrare a mesajelor email infectate, deoarece vă permite să filtrați mesajele email cu un anumit subiect (presupunând că această opțiune este acceptată de clientul dvs. de email) într-un director separat.

4.1.2.3 Eliminarea infiltrărilor

Dacă se primește un mesaj de email infectat, este afișată o fereastră de alertă. Fereastra de alertă prezintă numele expeditorului, mesajul email și numele infiltrării. În partea de jos a ferestrei sunt disponibile următoarele opțiuni pentru obiectul detectat: **Curățare**, **Ștergere** și **Păstrare**. Pentru majoritatea cazurilor, vă recomandăm să selectați **Curățare** sau **Ștergere**. În situații deosebite, când doriți să primiți fișierul infectat, selectați **Păstrare**. Dacă este activat modul **Curățare strictă**, se afișează o fereastră de informare fără opțiuni disponibile pentru obiectele infectate.

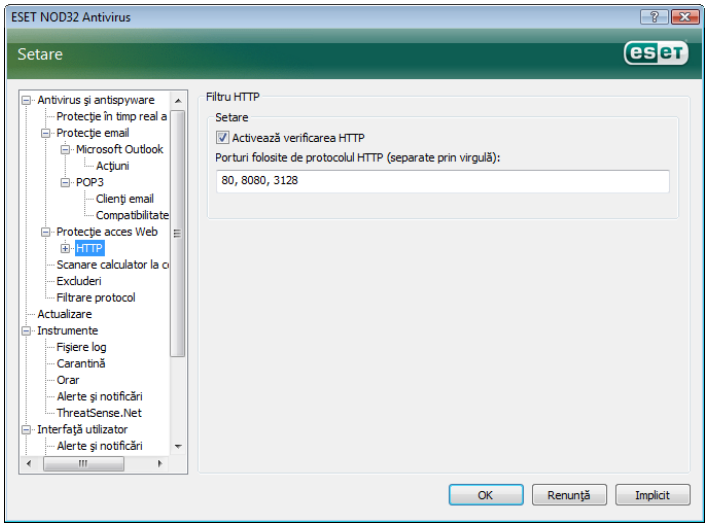
4.1.3 Protecția pentru acces Web

Conectivitatea Internet este o caracteristică standard într-un computer personal. Din păcate, aceasta a devenit, de asemenea, mijlocul principal de transferare a codului dăunător. Din această cauză, este esențial să acordați o atenție deosebită protecției pentru accesul Web. Recomandăm cu insistență ca opțiunea **Activează protecție acces Web** să fie activată. Această opțiune este amplasată în **Setare avansată (F5) > Protecție antivirus și antispyware > Protecție acces Web**.



4.1.3.1 HTTP

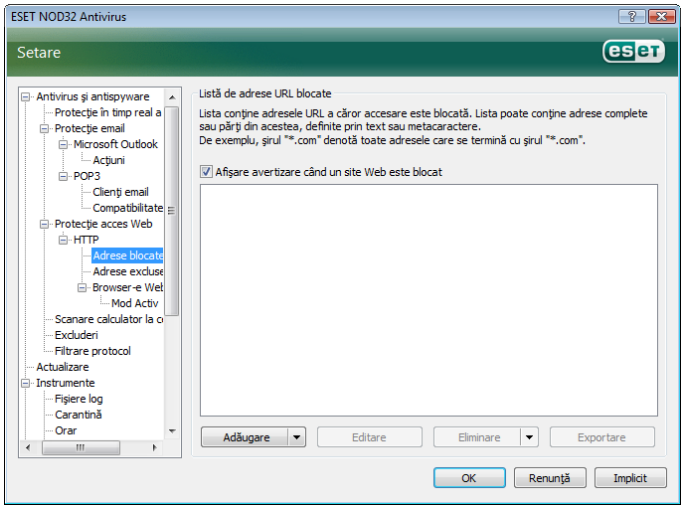
Funcția principală a protecției pentru accesul Web este monitorizarea comunicării dintre browserele Internet și serverele la distanță, care respectă regulile protocolului HTTP (Hypertext Transfer Protocol). ESET NOD32 Antivirus este configurat în mod implicit să folosească standardele HTTP pentru majoritatea browserelor Internet. Totuși, opțiunile de setare pentru verificarea HTTP pot fi modificate parțial în secțiunea **Protecție acces Web > HTTP**. În fereastra **Setare filtru HTTP** puteți activa sau dezactiva verificarea HTTP cu opțiunea **Activare verificare HTTP**. De asemenea, puteți defini numărul de porturi utilizate de sistem pentru comunicarea HTTP. În mod implicit, se utilizează numerele de porturi 80, 8080 și 3128. Traficul HTTP prin fiecare port se poate detecta și scana în mod automat prin adăugarea de numere de porturi suplimentare separate prin virgulă.



4.1.3.1.1 Adrese blocate/excluse

Setarea verificării HTTP vă permite să creați liste definite de utilizator cu liste **definite** de **adrese** URL (Uniform Resource Locator) **Blocate și Excluse**.

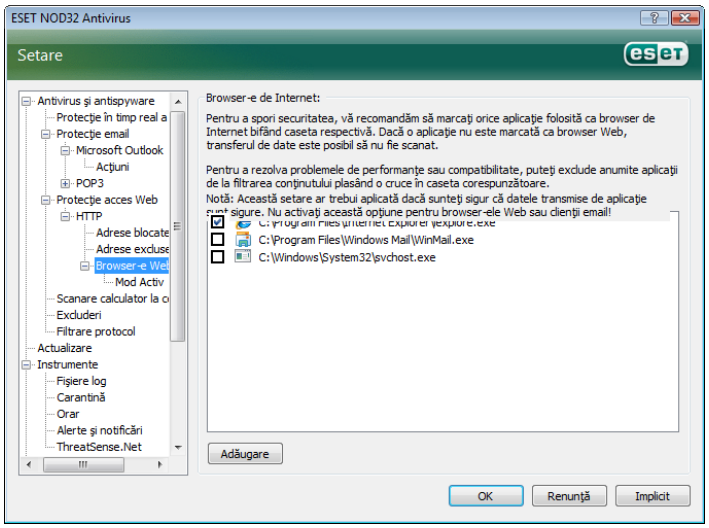
Ambele ferestre de dialog conțin butoanele **Adăugare**, **Editare**, **Eliminare** și **Export**, care vă permit să gestionați și să întrețineți cu ușurință listele de adrese specificate. Dacă o adresă cerută de utilizator este în lista de adrese blocate, accesarea acestei adrese nu va fi posibilă. Pe de altă parte, adresele din lista de adrese excluse sunt accesate fără a se face verificarea pentru cod dăunător. În ambele liste se pot utiliza simbolurile speciale * (asterisc) și **?** (semn de întrebare). 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.



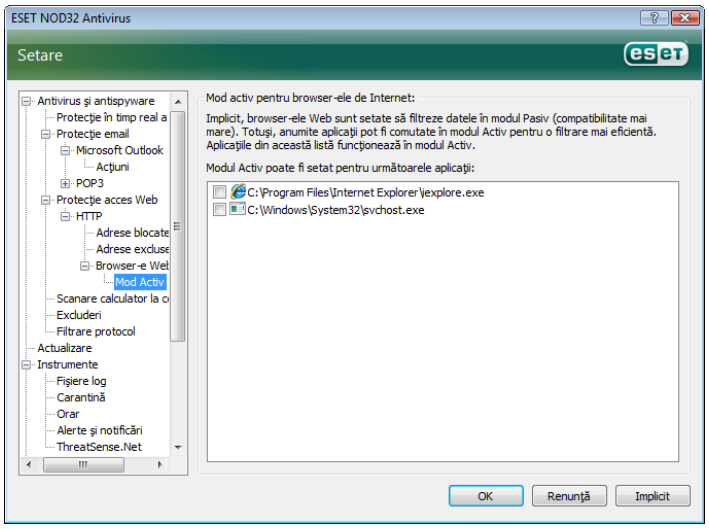
4.1.3.1.2 Browsere Web

ESET NOD32 Antivirus conține și caracteristica **Browsere Web**, care permite utilizatorului să definească dacă aplicația dată este sau nu este un browser. Dacă o aplicație este marcată ca browser de către utilizator, întreaga comunicație de la această aplicație este monitorizată, indiferent de numerele de porturi implicate în comunicare.

Caracteristica Browsere Web este complementară celei de verificare HTTP, deoarece verificarea HTTP are loc numai pentru porturi predefinite. Totuși, multe servicii Internet utilizează modificarea dinamică sau numere de porturi necunoscute. Ținând cont de acest lucru, caracteristica Browsere Web poate stabili controlul comunicărilor prin porturi indiferent de parametrii de conectare.



Lista de aplicații marcate ca browsere se poate accesa direct din submeniul **Browsere Web** a ramificației **HTTP**. Această secțiune mai conține submeniul **Mod Activ**, ce definește modul de verificare pentru browserele Internet. **Modul Activ** este util deoarece examinează datele transferate ca întreg. Dacă nu este activat, comunicarea aplicațiilor este monitorizată gradat, în loturi. Acest lucru diminuează eficiența procesului de verificare a datelor, dar oferă o compatibilitate sporită pentru aplicațiile listate. Dacă nu apar probleme la utilizarea acestuia, vă recomandăm să activați modul de verificare activă prin bifarea casetei de selectare de lângă aplicația dorită.



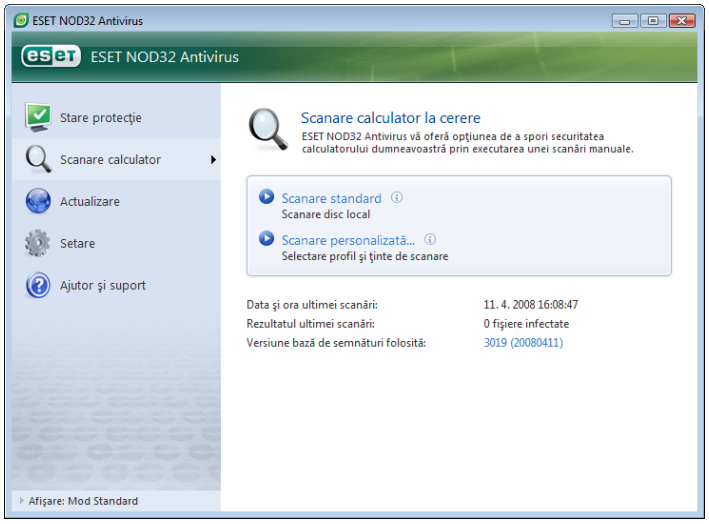
4.1.4 Scanarea calculatorului

Dacă bănuiți că vi s-a infectat calculatorul (acesta se comportă anormal), rulați o scanare de computer la cerere, pentru a examina computerul pentru infiltrări. Din punctul de vedere al securității, este esențial ca scanările de computer să ruleze nu numai când se suspectează o infiltrare, ci în mod regulat, ca parte a măsurilor de securitate de rutină. Scanările regulate oferă detectarea infiltrărilor care nu au fost detectate de scannerul în timp real în momentul salvării acestora pe disc. Acest lucru se poate întâmpla dacă scannerul în timp real era dezactivat în momentul infectării sau dacă baza de date de semnături era veche.

Vă recomandăm să rulați o scanare la cerere cel puțin o dată sau de două ori pe lună. Scanarea se poate configura ca o sarcină programată în **Instrumente > Orar**.

4.1.4.1 Tipurile de scanare

Sunt disponibile două tipuri. **Scanare standard** scanează rapid sistemul, fără a necesita configurarea suplimentară a parametrilor de scanare. **Scanare personalizată**... permite utilizatorului să selecteze oricare din profilele de scanare predefinite, dar și să aleagă obiecte de scanare din structura arbore.



4.1.4.1.1 Scanarea standard

Scanarea standard este o metodă prietenoasă pentru utilizator care-i permite să lanseze rapid o scanare de computer și să curețe fișiere infectate fără a necesita intervenția sa. Avantajele principale constau în funcționarea ușoară fără o configurare de scanare detaliată. Scanarea standard verifică toate fișierele de pe unitățile locale și curăță sau șterge automat infiltrările detectate. Nivelul de curățare este setat automat la valoarea implicită. Pentru mai multe informații detaliate despre tipurile de curățare, consultați secțiunea Curățarea.

Profilul de scanare standard este conceput pentru utilizatori care doresc să-și scaneze computerele rapid și ușor. Acesta oferă o soluție eficientă de scanare și curățare, fără a necesita un proces extins de configurare.

4.1.4.1.2 Scanarea personalizată

Scanarea personalizată este o soluție optimă dacă doriți să specificați parametri de scanare precum țintele și metodele de scanare. Avantajul scanării personalizate constă în capacitatea de a configura detaliat parametrii. Configurațiile se pot salva în profile de scanare definite de utilizator, care pot fi utile dacă scanarea se efectuează în mod repetat, cu aceiași parametri definiți de utilizator.

Pentru a selecta țintele de scanare, utilizați meniul verticalpentru caracteristica de selectare rapidă a țintei sau selectați ținte din structura arbore ce prezintă toate dispozitivele disponibile pe computer. În plus, puteți alege unul dintre cele trei niveluri de curățare executând clic pe **Setare... Î > Curățare**. Dacă vă interesează numai scanarea sistemului, fără efectuarea unor acțiuni suplimentare, bifați caseta de selectare **Scanare fără curățare**.

Efectuarea scanărilor de computer utilizând modul de scanare personalizată este adecvată pentru utilizatori avansați, ce au experiență anterioară în utilizarea programelor antivirus.

4.1.4.2 Ținte de scanare

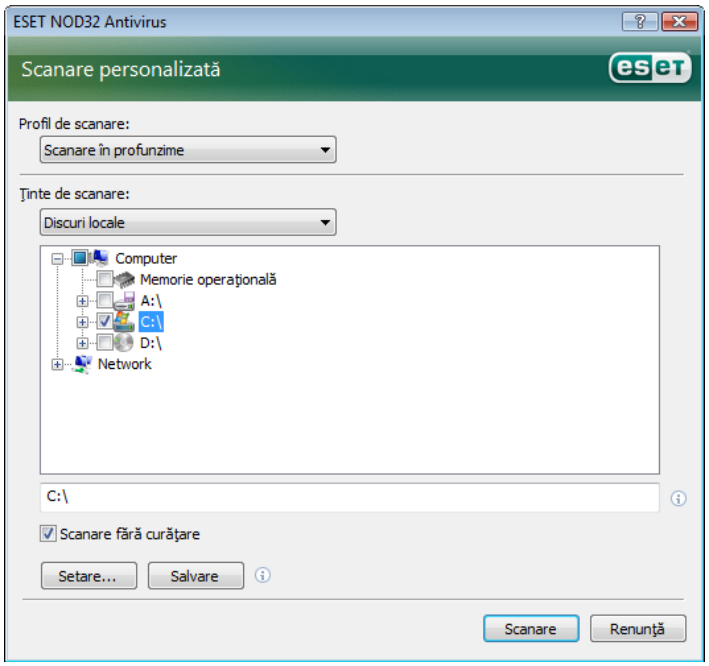
Meniul vertical Ținte de scanare vă permite să selectați fișiere, directoare și dispozitive (discuri) ce trebuie scanate pentru viruși.

Utilizând opțiunea de meniu pentru ținte de scanare rapidă, puteți selecta următoarele ținte:

Unități locale – controlează toate unitățile de disc locale

Medii amovibile – dischete, dispozitive de stocare USB, CD/DVD

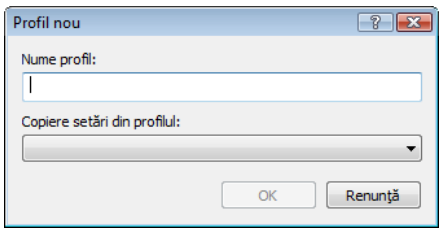
Unități de rețea – toate unitățile mapate



De asemenea, o țintă de scanare poate fi specificată mai precis introducând calea spre directorul sau fișierul/fișierele pe care doriți să îl/le includeți în scanare. Selectați țintele din structura arbore ce prezintă toate dispozitivele disponibile pe computer.

4.1.4.3 Profile de scanare

Parametrii de scanare computer preferați se pot salva în profile. Avantajul creării profilelor de scanare este că acestea pot fi utilizate în viitor în mod regulat pentru scanare. Vă recomandăm să creați atâtea profile (cu ținte de scanare diferite, metode de scanare diferite și alți parametri) câte folosește utilizatorul în mod regulat.



Pentru a crea un profil nou ce poate fi utilizat în mod repetat la scanările viitoare, navigați la **Setare avansată** (F5) **> Scanare computer la cerere**. Faceți clic pe butonul **Profile...** din dreapta pentru a afișa lista de profile de scanare existente și opțiunea de creare a unui profil nou. Următoarea opțiune **Setare parametri motor**

ThreatSense descrie fiecare parametru de setare scanare. Acest lucru vă va ajuta să creați un profil de scanare adecvat necesităților dvs.

Exemplu:
Să presupunem că doriți să creați propriul profil de scanare, iar configurarea atribuită profilului **Smart scan** este parțial adecvată. Dar nu doriți să scanați pachete de rutină sau aplicații potențial periculoase și doriți și să aplicați **curățarea strictă**. În fereastra **Profile de configurare**, faceți clic pe butonul **Adăugare...**. Introduceți numele profilului nou în câmpul **Nume profil** și selectați **Smart scan** din meniul vertical **Copiere setări din profilul:** meniu vertical. Ajustați apoi restul parametrilor pentru a corespunde cerințelor dvs.

4.1.5 Setarea parametrilor pentru motorul ThreatSense

ThreatSense este numele tehnologiei alcătuite din 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 mai multe metode (analiză de cod, emulare de cod, semnături generice, semnături de viruși) 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 rootkit-urile.

Opțiunile de setare a tehnologiei ThreatSense permit utilizatorului să specifice 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 butonul **Setare...** amplasat în fereastra de setare din oricare modul care folosește tehnologia ThreatSense (vezi mai jos). Este posibil ca diferite scenarii de securitate să necesite diferite configurații. Ținând cont de acest lucru, ThreatSense se poate configura individual pentru următoarele module de protecție:

- Protecție în timp real sistem de fișiere
- Verificare fișier la pornire sistem
- Protecție email
- Protecție acces Web
- Scanare computer la cerere

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

4.1.5.1 Setarea obiectelor

Secțiunea **Obiecte** vă permite să definiți ce componente de computer și fișiere vor fi scanate pentru infiltrări.

Memorie operațională – scanează pentru amenințări ce atacă memoria operațională a sistemului.

Sectoare de boot – scanează sectoare de boot pentru prezența virușilor în sectorul principal de încărcare

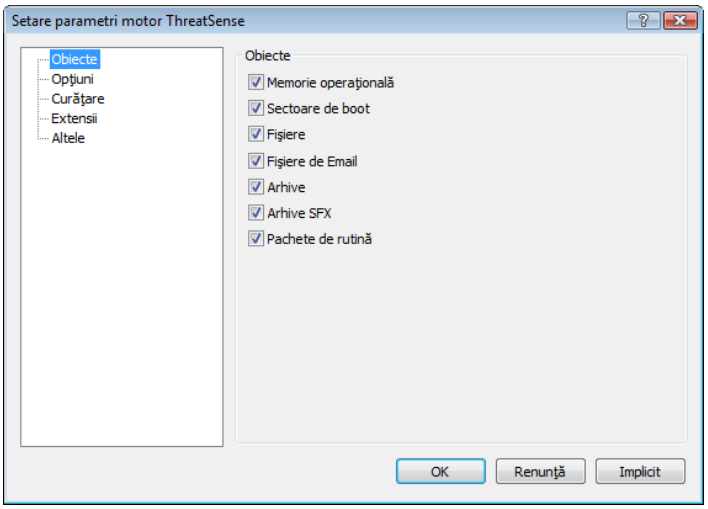
Fișiere – furnizează scanarea tuturor tipurilor comune de fișiere (programe, imagini, audio, fișiere video, fișiere de baze de date etc.)

Fișiere de email – scanează fișiere speciale în care sunt conținute mesaje de email

Arhive – furnizează scanarea fișierelor comprimate în arhive (.rar, .zip, .arj, .tar etc.)

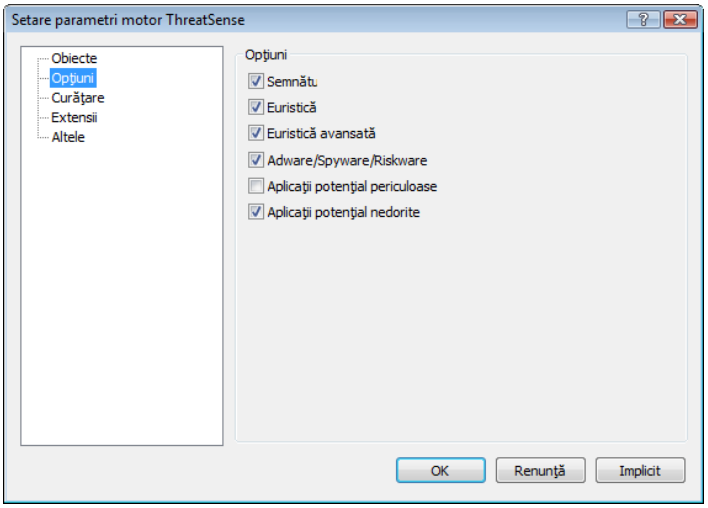
Arhive SFX – scanează fișiere care sunt cuprinse în fișierele arhivă SFX, dar care sunte prezentate de regulă cu o extensie .exe

Pachete de rutină – pachetele de rutină (spre deosebire de tipurile de arhivă standard) se decomprimă în memorie, în completare la pachetele standard statice (UPX, yoda, ASPack, FGS etc.).



4.1.5.2 Opțiuni

În secțiunea **Opțiuni**, utilizatorul poate selecta metodele de folosit la scanarea sistemului după infiltrări. Sunt disponibile următoarele opțiuni:



Semnături – Semnăturile pot detecta și identifica infiltrarea cu exactitate și credibilitate, după numele acestora, utilizând semnături de viruși.

Euristică – Euristica este un algoritm ce analizează activitatea (dăunătoare) a programelor. Avantajul principal al detecției euristice constă în capacitatea de a detecta software dăunător nou ce nu exista anterior sau care nu a fost inclus în lista de viruși cunoscuți (baza de semnături).

Euristică avansată – Euristica avansată cuprinde un algoritm euristic unic dezvoltat de ESET și optimizat pentru detectarea viermilor și troienilor scriși în limbaje de programare de nivel ridicat. Datorită euristicii avansate, detectarea inteligentă a programului este semnificativ mai ridicată.

Adware/Spyware/Riskware – Această categorie cuprinde software care colectează diferite informații sensibile despre utilizatori, fără consimțământul informat al acestora. Această categorie mai cuprinde software care afișează material publicitar.

Aplicații potențial periculoase – Aplicații potențial periculoase reprezintă clasificarea folosită pentru software comercial, legitim. Aici intră programe precum instrumente de acces la distanță, acesta fiind motivul pentru care opțiunea este dezactivată în mod implicit.

Aplicații potențial nedorite – Aplicațiile potențial nedorite nu sunt neapărat destinate să fie dăunătoare, dar ele pot afecta în mod negativ performanțele computerului. Aceste aplicații necesită, de obicei, permisiune pentru instalare. Dacă ele sunt prezente în calculator, sistemul se comportă diferit (comparativ cu starea anterioară instalării acestora). Modificările cele mai importante includ ferestre pop-up nedorite, activarea și rularea de procese ascunse, creșterea utilizării resurselor de sistem, modificări ale rezultatelor căutării și aplicații care comunică cu servere la distanță.

4.1.5.3 Curățarea

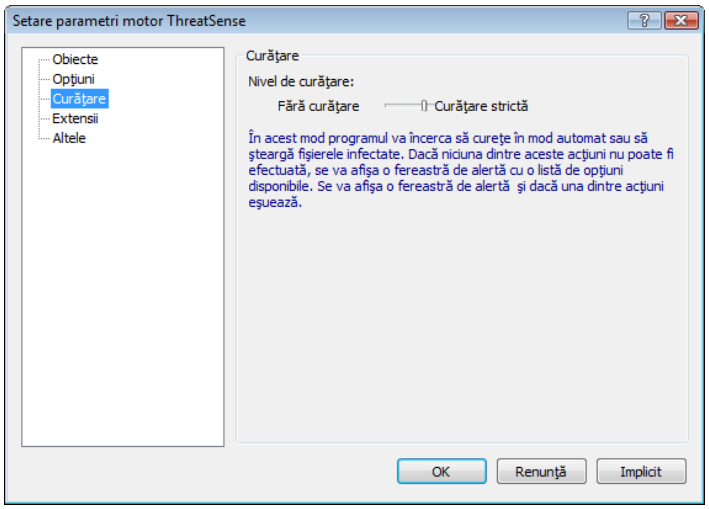
Setările de curățare determină comportamentul scannerului în timpul curățării fișierelor infectate. Există 3 niveluri de curățare:

Fără curățare
Fișierele infectate nu se curăță automat. Programul va afișa o fereastră de avertizare și va permite utilizatorului să aleagă o acțiune.

Nivel implicit
Programul va încerca curățarea sau ștergerea automată a unui fișier infectat. Dacă nu se poate selecta automat acțiunea corectă, programul va oferi o gamă de acțiuni de urmat. De asemenea, gama deacțiuni de urmat va fi afișată dacă o acțiune predefinită nu a putut fi terminată.

Curățare strictă
Programul va curăța sau va șterge toate fișierele infectate (inclusiv arhivele). Singura excepție o constituie fișierele de sistem. Dacă nu există posibilitatea de a le curăța, utilizatorului i se oferă o acțiune de urmat într-o fereastră de avertizare.

Avertisment:
În modul Implicit, fișierul de arhivă este șters în totalitate numai dacă acesta conține fișiere infectate. Dacă arhiva conține și fișiere legitime, aceasta nu va fi ștearsă. Dacă este detectat un fișier arhivă infectat în modul Curățare strictă, arhiva va fi ștearsă în întregime, chiar dacă sunt prezente și fișiere curate



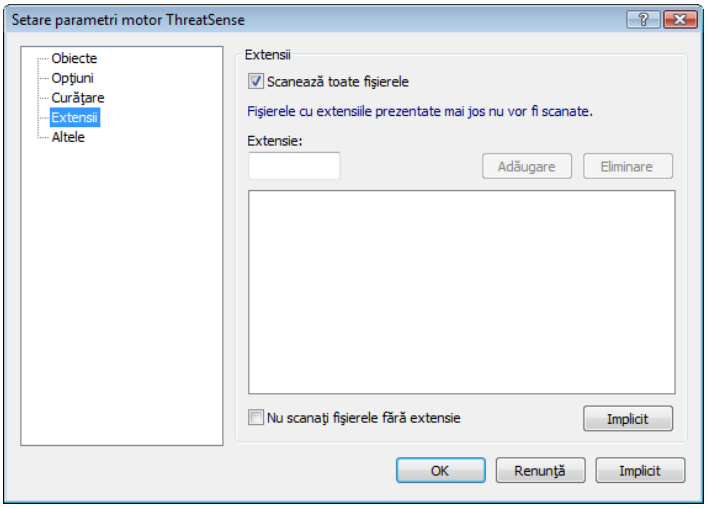
4.1.5.4 Extensii

O extensie este o parte din numele de fișier, delimitată prin punct. Extensia definește tipul și conținutul fișierului. Această secțiune din setarea parametrilor ThreatSense vă permite să definiți tipurile de fișiere de scanat.

În mod implicit, sunt scanate toate fișierele, indiferent de extensia acestora. În lista de fișiere excluse de la scanare se poate adăuga orice extensie. Dacă este debifată caseta de selectare **Scanează toate fișierele**, lista se modifică pentru a arăta toate extensiile de fișier scanate. Prin utilizarea butoanelor **Adăugare** și **Eliminare** puteți activa sau interzice scanarea extensiilor dorite.

Pentru a activa scanarea fișierelor fără extensie, selectați opțiunea **Scanare fișiere fără extensie**.

Excluderea fișierelor de la scanare are rolul său dacă scanarea anumitor tipuri de fișier duce la funcționarea incorectă a programului care utilizează extensiile. De exemplu, poate fi recomandabil să excludeți extensiile .edb, .eml și .tmp atunci când folosiți serverul MS Exchange.



4.1.6 Se detectează o infiltrare

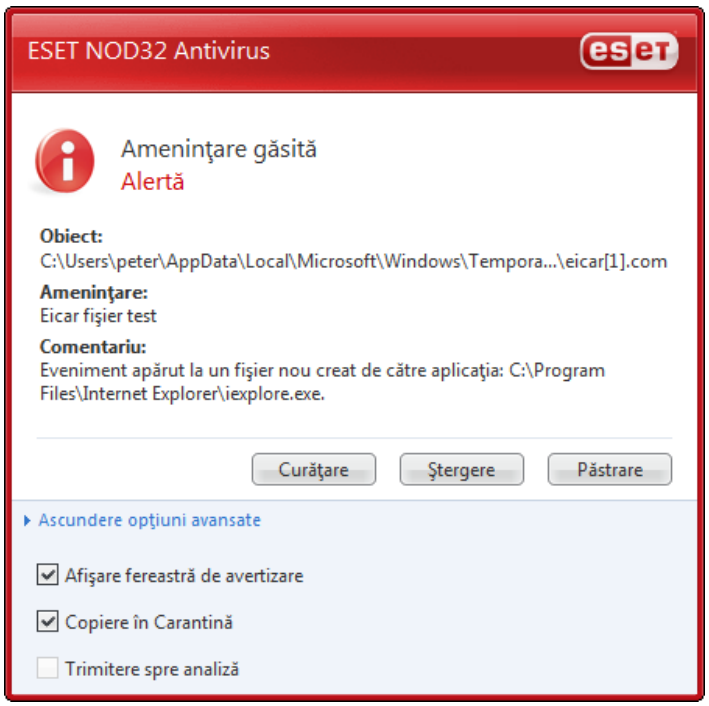
Infiltrările pot ajunge în sistem prin diverse puncte de intrare; pagini Web, directoare partajate, prin email sau de la dispozitivele de computer amovibile (USB, discuri externe, CD-uri, DVD-uri, dischete etc.).

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

- Deschideți ESET NOD32 Antivirus și faceți clic pe **Scanare calculator**
- Faceți clic pe **Scanare standard** (pentru informații suplimentare, consultați secțiunea Scanarea standard).
- 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.

Ca exemplu general despre cum sunt gestionate infiltrările în ESET Smart Security, să presupunem că este detectată o infiltrare de către monitorizarea în timp real a sistemului de fișiere, care utilizează nivelul de curățare implicit. Acesta va încerca să curețe sau să șteargă fișierul. Dacă nu există o acțiune predefinită de urmat pentru modulul de protecție în timp real, vi se va cere să selectați o opțiune într-o fereastră de alertă. De obicei, sunt disponibile opțiunile **Curățare**, **Ștergere** și **Păstrare**. Nu vă recomandăm să selectați **Păstarre**, deoarece fișierele infectate vor rămâne neatinse. Singura excepție este atunci când sunteți sigur că fișierul este inofensiv și a fost detectat din greșeală.



Curăţare şi ştergere
Aplicaţi curăţarea dacă un fişier curat a fost atacat de un virus care a ataşat cod dăunător fişierului curăţat. În acest caz, încercaţi mai întâi să curăţaţi fişierul infectat pentru a-l readuce la starea iniţială. Fişierul va fi şters dacă este format exclusiv din cod dăunător.

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

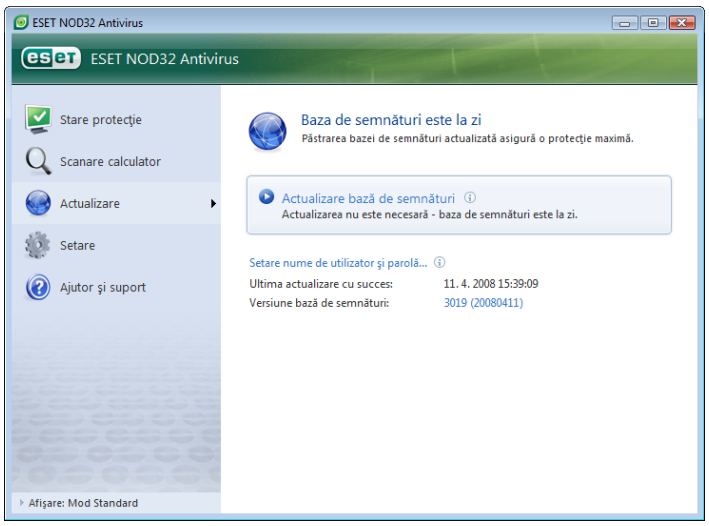
Ştergere fişiere în arhive
În modul de curăţare implicit, va fi ştearsă arhiva în totalitate numai dacă aceasta conţine fişiere infectate şi niciun fişier curat. Cu alte cuvinte, arhivele nu sunt şterse dacă ele conţin şi fişiere curate inofensive. Totuşi, acordaţi atenţie atunci când efectuaţi o scanare de curăţare strictă – la curăţarea strictă arhiva va fi ştearsă dacă aceasta conţine cel puţin un fişier infectat, indiferent de starea celorlalte fişiere din arhivă.

4.2 Actualizarea programului

Actualizarea regulată a sistemului constituie condiţia de bază pentru obţinerea nivelului maxim de securitate oferit de ESET Smart Security. Modulul actualizare asigură faptul că programul este întotdeauna la zi. Acest lucru se efectuează în două moduri – prin actualizarea bazei de semnături şi prin actualizarea componentelor sistemului.

Informaţiile despre starea actualizării curente pot fi găsite făcând clic pe **Actualizare** – inclusiv versiunea curentă a bazei de semnături şi informaţii despre necesitatea actualizării acesteia. În plus, este disponibilă opţiunea de activare imediată a procesului de actualizare – **Actualizare bază de semnături** – precum şi opţiunile de bază pentru setarea actualizării, cum ar fi numele de utilizator şi parola pentru accesarea serverelor de actualizare ale ESET.

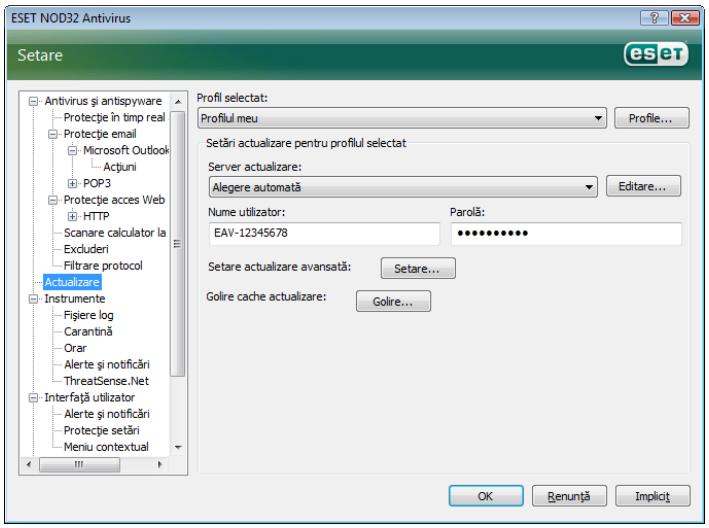
De asemenea, fereastra cu informaţii conţine detalii precum data şi ora celei mai recente actualizări reuşite şi numărul bazei de viruşi. Această indicaţie numerică este o legătură activă către site-ul Web ESET, care listează toate semnăturile adăugate în cadrul actualizării date.



NOTĂ: Numele de utilizator şi parola sunt furnizate de către ESET după achiziţionarea ESET Smart Security.

4.2.1 Setarea actualizării

Secţiunea de setare a actualizării specifică informaţiile despre sursa actualizării, precum serverele de actualizare şi datele de autentificare pentru aceste servere. În mod implicit, câmpul **Server actualizare:** este setat la **Alegere automată**. Această valoare asigură descărcarea automată a fişierelor de actualizare din serverul de actualizare ESET luând în considerare încărcarea cea mai redusă a traficului de reţea. Opţiunile pentru setarea actualizării sunt disponibile în arborele Setare avansată (F5), sub **Actualizare**.



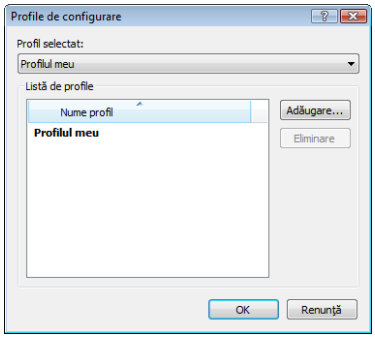
Lista de servere de actualizare existente curent poate fi accesată prin intermediul meniului vertical din **Server de actualizare:** meniu vertical. Pentru a adăuga un server de actualizare nou, faceţi clic pe **Editare...** în secţiunea **Setări actualizate pentru profilul selectat** şi apoi pe butonul **Adăugare**.

Autentificarea pentru serverele de actualizare se acordă prin **Numele de utilizator** şi **Parola** care au fost generate şi trimise utilizatorului de către ESET după achiziţionarea licenţei de produs.

4.2.1.1 Profilele de actualizare

Pentru diverse configurații de actualizare, puteți crea profile de actualizare definite de utilizator care pot fi folosite pentru o sarcină de actualizare dată. Crearea de profile de actualizare diverse este utilă în special pentru utilizatorii mobili, deoarece proprietățile conexiunii Internet se modifică în mod de regulat. Modificând sarcina de actualizare, utilizatorii mobili pot specifica faptul că dacă nu este posibilă actualizarea programului folosind configurația specificată în **Profilul meu**, actualizarea se va efectua folosind u profil alternativ.

Meniul vertical **Profil selectat** afișează profilul selectat curent. În mod implicit, această înregistrare este setată la opțiunea **Profilul meu**. Pentru a crea un profil nou, faceți clic pe butonul **Profile...**, apoi pe butonul **Adăugare...** și introduceți propriul dvs. **Nume de profil**. La crearea unui profil nou, puteți copia setări dintr-un profil existent selectându-l din meniul vertical **Copiere setări din profilul:**.



În cadrul setării profilului, puteți specifica serverul de actualizare la care programul se va conecta și va descărca actualizări; poate fi folosit orice server din lista de servere disponibile sau poate fi adăugat un server nou. Lista de servere de actualizare existente poate fi accesată prin intermediul meniului vertical din **Server de actualizare:** -. Pentru a adăuga un server de actualizare nou, faceți clic pe **Editare...** în secțiunea **Setări actualizate pentru profilul selectat** și apoi pe butonul **Adăugare**.

4.2.1.2 Setarea actualizării avansate

Pentru a vizualiza secțiunea **Setare actualizare avansată**, faceți clic pe butonul **Setare...**. Opțiunile pentru setarea actualizării avansate includ configurarea **modului de actualizare, a proxy-ului HTTP, a LAN-ului** și a **copiei fișierelor de actualizare**.

4.2.1.2.1 Modul de actualizare

Fila **Mod actualizare** conține opțiuni corelate cu actualizarea componentelor programului.

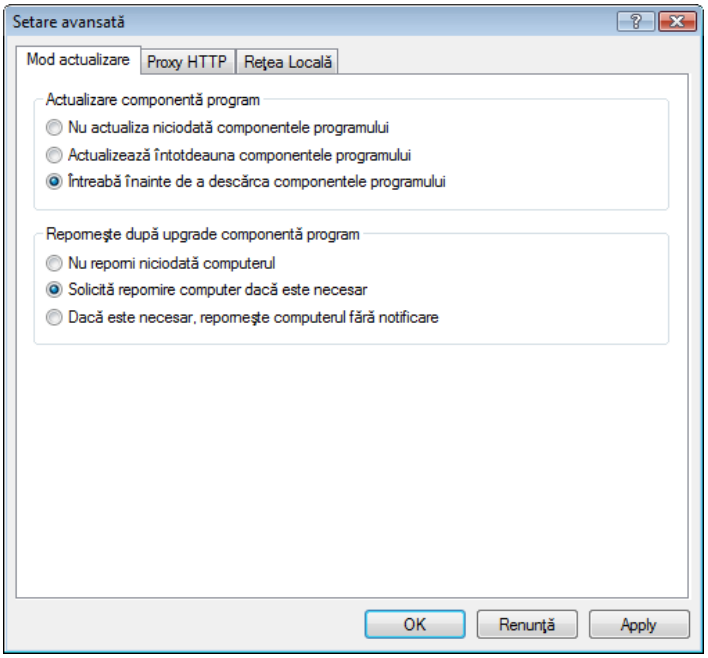
În secțiunea **Actualizare componentă program** sunt disponibile trei opțiuni:

- **Nu actualiza niciodată componentele programului**
- **Actualizează întotdeauna componentele programului**
- **Întreabă înainte de a descărca componentele programului**

Selectarea opțiunii **Nu actualiza niciodată componentele programului** asigură faptul că, după publicarea de către ESET a unei actualizări noi de componentă de program, aceasta nu va fi descărcată și nicio actualizare de componentă de program nu va avea loc pe stația de lucru dată. Opțiunea **Actualizează întotdeauna componentele programului** presupune faptul că actualizările componentelor programului vor fi efectuate ori de câte ori este disponibilă o actualizare nouă pe serverele de actualizare ESET și că se va face upgrade pentru componentele programului la versiunea descărcată.

Selectați a treia opțiune, **Întreabă înainte de a descărca componentele programului** pentru a vă asigura faptul că programul îi va solicita utilizatorului confirmarea de descărcare a actualizărilor componentelor programului în momentul în care astfel de actualizări sunt disponibile. În acest caz, va fi afișată o fereastră de dialog care conține informații despre actualizările de componente de program disponibile, cu opțiunea de confirmare sau refuzare a acestora. Dacă se confirmă, actualizările sunt descărcate și componentele de program noi vor fi instalate.

Opțiunea implicită pentru o actualizare a componentelor programului este **Întreabă înainte de a descărca componentele programului**.



După instalarea unei actualizări a componentelor programului, este necesar să reporniți computerul pentru a asigura funcționalitatea completă a tuturor modulelor. Secțiunea **Repornește după upgrade componentă program** vă permite să selectați una dintre următoarele trei opțiuni:

- **Niciodată nu reporni computerul**
- **Solicită repornire computer dacă este necesar**
- **Dacă este necesar, repornește computerul fără notificare**

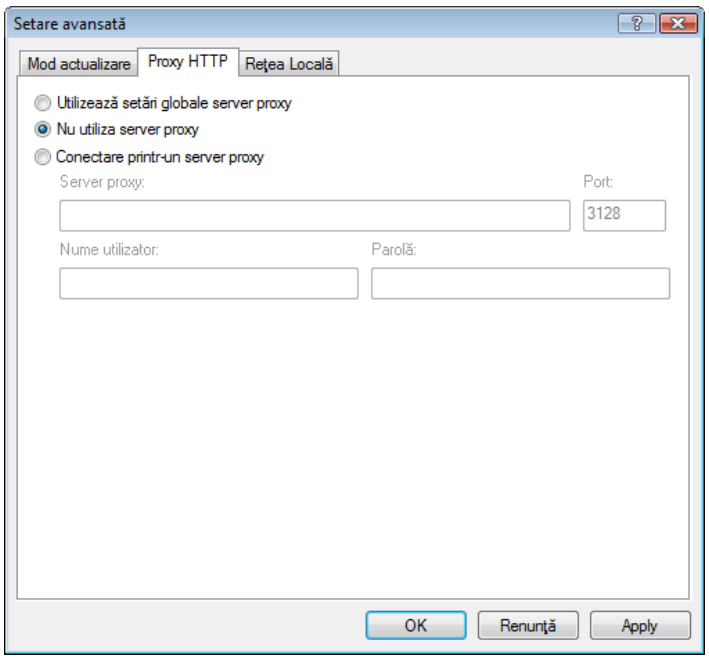
Opțiunea implicită pentru repornire este **Solicită repornire computer dacă este necesar**. Selectarea celor mai adecvate opțiuni pentru actualizările componentelor programului în cadrul filei **Mod actualizare** depinde de fiecare stație de lucru în parte, deoarece acesta este locul unde urmează să se aplice aceste setări. Luați în considerare faptul că există diferențe între stații de lucru și servere – de exemplu repornirea automată a serverului după un upgrade de program poate cauza dauna grave.

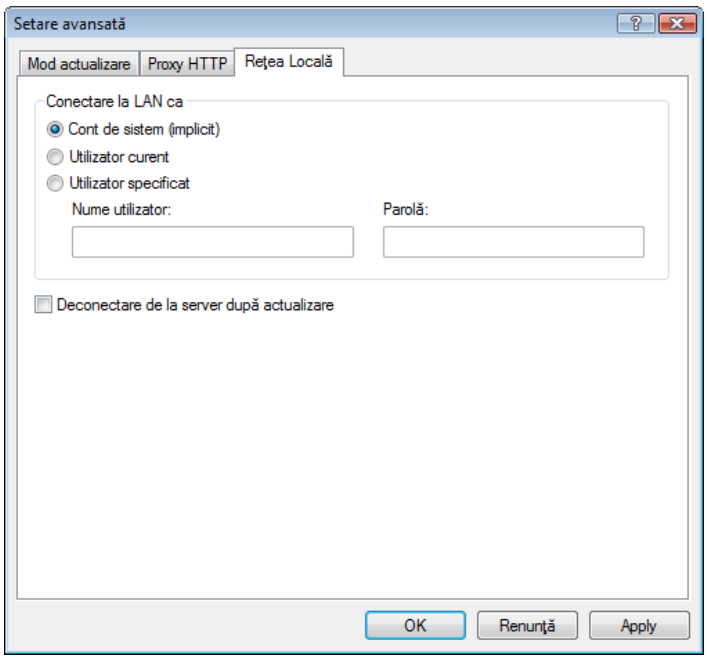
4.2.1.2.2 Server proxy

Pentru a accesa opțiunile serverului proxy pentru profilul de actualizare dat: Faceți clic pe **Actualizare** în arborele Setare avansată (F5) și apoi faceți clic pe butonul **Setare...** din dreapta secțiunii **Setare actualizare avansată.** Faceți clic pe fila **Proxy HTTP** și selectați una dintre următoarele trei opțiuni:

- **Utilizează setări globale server proxy**
- **Nu utiliza server proxy**
- **Conectare printr-un server proxy** (conexiune definită de proprietățile conexiunii)

Selectarea opțiunii **Utilizează setări globale server proxy** presupune aplicarea tuturor opțiunilor de configurare a serverului proxy deja specificate în ramificația **Diverse > Server proxy** a arborelui Setare avansată.





Selectați opțiunea **Nu utiliza server proxy** pentru a defini explicit nefolosirea niciunui server proxy pentru actualizarea ESET Smart Security.

Opțiunea **Conectare printr-un server proxy** trebuie aleasă dacă un server proxy urmează să fie folosit pentru actualizarea ESET NOD32 Antivirus și acesta este diferit de serverul proxy specificat în setările globale (**Diverse > Server proxy**). În acest caz trebuie specificate setări suplimentare: adresa **serverului proxy**, **portul** de comunicare plus **numele de utilizator** și **parola** pentru serverul proxy, dacă este necesar.

Această opțiune trebuie selectată și dacă serverul proxy nu a fost setat global, dar modulul de actualizare a ESET NOD32 Antivirus se va conecta la un server proxy.

Setarea implicită pentru serverul proxy este **Utilizează setări globale server proxy**.

4.2.1.2.3 Conectarea la LAN

Atunci când actualizați dintr un server local pe care se execută un sistem de operare bazat pe-NT, autentificarea pentru fiecare conexiune în parte este necesară în mod implicit. În majoritatea cazurilor, un cont de sistem local nu deține suficiente drepturi de acces pentru directorul oglindă (care conține copii ale fișierelor de actualizare). În acest caz, introduceți numele de utilizator și parola în secțiunea de setare a actualizării sau specificați un cont existent din care programul va accesa serverul de actualizare (oglindă).

Pentru a configura un astfel de cont, faceți clic pe fila **LAN**. Secțiunea **Conectare la LAN ca** oferă opțiunile **Cont de sistem (implicit)**, **Utilizator curent** și **Utilizator specificat**.

Selectați opțiunea **Cont de sistem** pentru a folosi contul de sistem pentru autentificare. În mod normal, nu are loc niciun proces de autentificare dacă nu există date de autentificare furnizate în secțiunea principală a setării de actualizare.

Pentru a vă asigura că programul se autorizează automat folosind contul unui utilizator conectat curent, selectați **Utilizator curent**. Dezavantajul acestei soluții este acela că programul nu se poate conecta la serverul de actualizare dacă nu există niciun utilizator conectat curent.

Selectați **Utilizator specificat** dacă doriți ca programul să folosească un anumit cont de utilizator pentru autentificare.

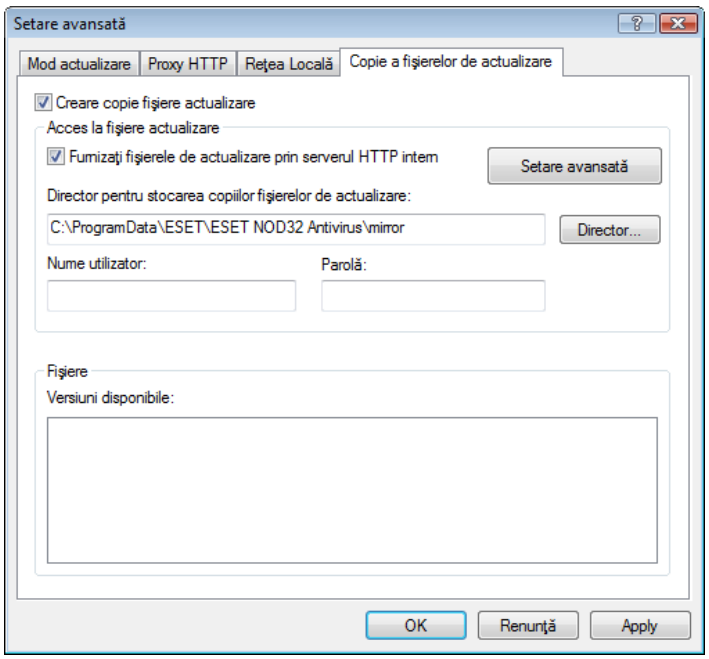
Opțiunea implicită pentru conexiunea LAN este **Cont de sistem**.

Avertisment:
Atunci când este activată fie opțiunea **Utilizator curent**, fie opțiunea **Utilizator specificat**, este posibil să apară o eroare la înlocuirea identității din program cu cea a utilizatorului dorit. Din acest motiv vă recomandăm să introduceți datele de autentificare în LAN în secțiunea principală a setării actualizării. În această secțiune a setării actualizării, datele de autentificare trebuie introduse după cum urmează: domeniu_nume\utilizator (dacă acesta este un grup de lucru, introduceți grupdelucru_nume\nume) și parola utilizatorului. Atunci când actualizați din versiunea HTTP a serverului local, nu este necesară nicio autentificare.

4.2.1.2.4 Creare copii actualizare – oglindă

ESET NOD32 Antivirus Business Edition permite utilizatorului să creeze copii ale fișierelor de actualizare care pot fi folosite pentru actualizarea altor stații de lucru din rețea. Actualizarea stațiilor de lucru client dintr-o oglindă optimizează raportul de încărcare și economisește lățimea de bandă a conexiunii Internet.

Opțiunile de configurare a oglinzii serverului local pot fi accesate (după adăugarea unei chei de licență valide în fereastra Manager de licențe, amplasată în secțiunea Setare avansată a ESET Smart Security Business Edition) din secțiunea **Setarea actualizării avansate:**. (Pentru a accesa această secțiune, apăsați pe F5 și faceți clic pe **Actualizare** în arborele Setare avansată. Faceți clic pe butonul **Setare...** de lângă **Setare actualizare avansată:** și selectați fila **Copie a fișierelor de actualizare**.)



Primul pas în configurarea oglinzii este bifarea casetei de selectare **Creare oglindă actualizare**. Selectarea acestei opțiuni activează alte opțiuni de configurare a oglinzii, precum modul de accesare a fișierelor de actualizare și calea de actualizare către fișierele oglindite.

Metodele de activare a oglinzii sunt descrise detaliat în capitolul următor, „Variante de accesare a oglinzii". Momentan, rețineți faptul că există două variante de bază pentru accesarea oglinzii – directorul cu fișiere de actualizare poate fi prezentat ca o oglindă a unui director partajat din rețea sau ca o oglindă a unui server HTTP.

Directorul dedicat stocării fișierelor de actualizare pentru oglindă este definit în secțiunea **Director pentru stocare fișiere oglindite**. Faceți clic pe **Director...** pentru a răsfoi până la un director dorit din computerul local sau până la un director partajat din rețea. Dacă este necesară autorizarea pentru directorul specificat, datele acesteia trebuie furnizate în câmpurile **Nume de utilizator** și **Parolă**. Numele de utilizator și parola trebuie introduse în formatul *domeniu/utilizator* sau *grup de lucru/utilizator*. Rețineți parolele corespunzătoare.

La specificarea configurației detaliate a oglinzii, puteți preciza, de asemenea, versiunile de limbă pentru care doriți să descărcați copiile de actualizare. Setarea versiunii de limbă poate fi accesată din secțiunea **Fișiere – Versiuni disponibile:**.

4.2.1.2.4.1 Actualizarea din oglindă

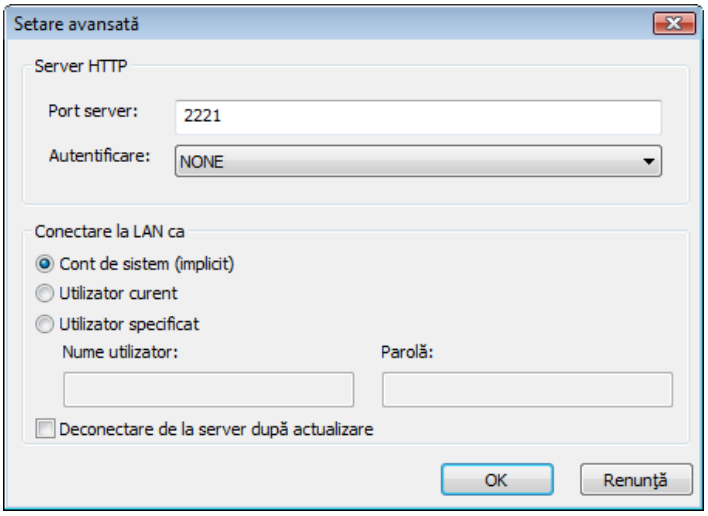
Există două metode de bază de configurare a oglinzii – directorul cu fișiere de actualizare poate fi prezentat ca o oglindă a unui director partajat din rețea sau ca o oglindă a unui server HTTP.

Accesarea oglinzii folosind un server HTTP intern

Această configurație este cea implicită și este specificată în configurația predefinită a programului. Pentru a permite accesarea oglinzii utilizând serverul HTTP, navigați la secțiunea **Setare actualizare avansată** (fila **Copie a fișierelor de actualizare**) și selectați opțiunea **Creare oglindă actualizare**.

În secțiunea **Setare avansată** a filei **Copie a fișierelor de actualizare** puteți specifica **Portul de server** unde va asculta serverul HTTP, precum și tipul de **Autentificare** folosit de serverul HTTP. În mod implicit, Portul de server este setat la valoarea **2221**. Opțiunea **Autentificare** definește metoda de autentificare folosită pentru accesarea fișierelor de actualizare. Sunt disponibile următoarele opțiuni: **NICIUNA, De bază** și **NTLM**. Selectați opțiunea **De bază** pentru a folosi codarea base64 împreună cu autentificarea de bază cu nume de utilizator și parolă. Opțiunea **NTLM** oferă o metodă de codificare sigură. Pentru autentificare se folosește numele de utilizator creat stația de lucru care partajează fișierele de actualizare. Setarea implicită este **NICIUNA**, care permite accesul la fișierele de actualizare fără a mai fi nevoie de autentificare.

Avertisment:
Dacă doriți să permiteți accesul la fișierele de actualizare prin intermediul serverului HTTP, directorul oglindă trebuie să fie amplasat pe același computer cu instanța ESET NOD32 Antivirus care îl creează.



După terminarea configurării oglinzii, accesați stațiile de lucru și adăugați un server de actualizare nou cu formatul **http://adresa_IP_a_serverului_dvs:2221**. Pentru a proceda astfel, urmați pașii de mai jos:

- Deschideți **Setare avansată ESET NOD32 Antivirus** și faceți clic pe ramificația **Actualizare**.
- Faceți clic pe **Editare...** din dreapta meniului vertical **Server de actualizare** și adăugați un server nou folosind următorul format: http://adresa_IP_a_serverului_dvs:2221
- Selectați acest server adăugat recent din lista de servere de actualizare.

Accesarea oglinzii prin intermediul partajărilor de sistem

Mai întâi trebuie creat un director partajat pe un dispozitiv local sau de rețea. La crearea directorului pentru oglindă, este necesar să furnizați acces la „scriere" utilizatorului care va salva fișierele în director și acces la „citire" tuturor utilizatorilor care vor actualiza ESET NOD32 Antivirus din directorul oglindă.

Continuați cu configurarea accesului la oglindă în secțiunea **Setare actualizare avansată** (fila **Copie a fișierelor de actualizare**) dezactivând opțiunea **Furnizați fișierele de actualizare prin serverul HTTP intern**. Această opțiune este activată implicit în pachetul de instalare a programului.

Dacă directorul partajat este amplasat pe un alt computer din rețea, trebuie să specificați date de autentificare pentru accesarea computerului respectiv. Pentru a specifica datele de autentificare, deschideți Setare avansată ESET NOD32 Antivirus (F5) și faceți clic pe ramificația **Actualizare**. Faceți clic pe butonul **Setare...** și apoi pe fila **LAN**. Această setare coincide cu cea pentru actualizare, care este descrisă în capitolul „Conectarea la LAN".

După finalizarea configurării oglinzii, continuați cu stațiile de lucru și setați \\UNC\CALE ca server de actualizare. Această operație poate fi efectuată după cum urmează:

- Deschideți Setare avansată ESET NOD32 Antivirus (F5) și faceți clic pe **Actualizare**.
- Faceți clic pe **Editare...** lângă Server de actualizare și adăugați un server nou utilizând formatul \\UNC\CALE.
- Selectați acest serveradăugat recent din lista de servere de actualizare.

NOTĂ: Pentru a asigura funcționarea corespunzătoare, calea către directorul oglindă trebuie specificată ca o cale UNC. Este posibil ca actualizările din unitățile mapate să nu funcționeze.

4.2.1.2.4.2 Depanarea problemelor la actualizarea din oglindă

În funcție de metoda de accesare a directorului oglindă, este posibil să apară diverse tipuri de probleme. În majoritatea cazurilor, problemele apărute în timpul unei actualizări dintr-un server oglindă sunt cauzate de următoarele: specificarea incorectă a opțiunilor directorului oglindă, date de autentificare incorecte pentru directorul oglindă, configurarea incorectă pe stații de lucru locale care încearcă să descarce fișiere de actualizare din oglindă sau o combinație a acestor cauze. Aici vă oferim o prezentare a celor mai frecvente probleme care pot apărea în timpul unei actualizări din oglindă:

- **ESET NOD32 Antivirus raportează o eroare la conectarea la serverul oglindă** – probabil cauzată de specificarea incorectă a serverului de actualizare (calea de rețea către directorul oglindă) din care stațiile de lucru locale descarcă actualizări. Pentru a verifica directorul, faceți clic (în Windows) pe meniul **Start**, apoi pe **Executare**, introduceți numele directorului și faceți clic pe **OK**. Trebuie să se afișeze conținutul directorului.

- **ESET NOD32 Antivirus solicită un nume de utilizator și o parolă** – probabil cauzată de introducerea incorectă a datelor de autentificare (nume de utilizator și parolă) în secțiunea de actualizare. Numele de utilizator și parola sunt folosite pentru a acorda acces la serverul de actualizare, din care programul se actualizează automat. Asigurați-vă că datele de autentificare sunt corecte și introduse în formatul corect. De exemplu *domeniu/nume de utilizator* sau *grup de lucru/nume de utilizator* plus parolele corespunzătoare. Dacă serverul oglindă poate fi accesat de „Oricine", luați în considerare faptul că aceasta nu presupune acordarea accesului absolut tuturor utilizatorilor. „Oricine" nu presupune orice utilizator neautorizat, ci numai faptul că directorul respectiv poate fi accesat de către toți utilizatorii domeniului. În concluzie, dacă directorul poate fi accesat de „Oricine", va trebui, în continuare, să se introducă un nume de utilizator și o parolă pentru domeniu în secțiunea de setare a actualizării.

- **ESET NOD32 Antivirus raportează o eroare la conectarea la serverul oglindă** – comunicarea prin portul definit pentru accesarea versiunii HTTP a oglinzii este blocată.

4.2.2 Cum se creează sarcini de actualizare

Actualizările pot fi declanșate manual selectând opțiunea **Actualizare bază de semnături** din fereastra cu informații care se afișează după ce faceți clic pe opțiunea **Actualizare** din meniul principal**.**

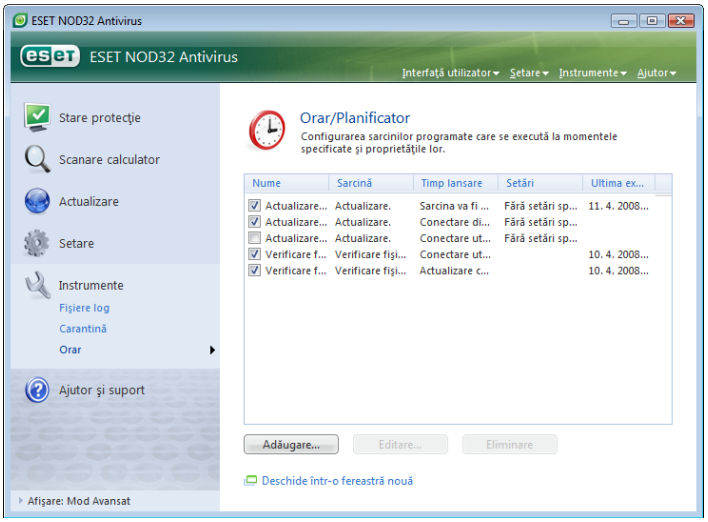
De asemenea, actualizările pot fi executate ca sarcini planificate – configurarea unei sarcini planificate se efectuează în **Instrumente > Planificator**. În mod implicit, următoarele sarcini sunt activate în ESET Smart Security:

- **Actualizare automată periodică**
- **Actualizare automată după conexiune dialup**
- **Actualizare automată după conectare utilizator**

Fiecare dintre sarcinile de actualizare menționate anterior pot fi modificate pentru a corespunde necesităților dvs. În afară de sarcinile de actualizare implicite, puteți crea noi sarcini de actualizare cu o configurație definită de utilizator. Pentru detalii suplimentare despre crearea și configurarea sarcinilor de actualizare, consultați capitolul „Planificatorul".

4.3 Planificatorul

Planificatorul este disponibil dacă modul Avansat din ESET NOD32 Antivirus este activat. **Planificatorul** poate fi găsit în meniul principal al ESET NOD32 Antivirus ca un submeniu al secțiunii **Instrumente**. Planificatorul conține un rezumat al tuturor sarcinilor planificate și proprietățile configurării acestora, precum data și ora predefinite și profilul de scanare folosit.



În mod implicit, în **Planificator** se afișează următoarele sarcini planificate:

- **Actualizare automată periodică**
- **Actualizare automată după conexiune dialup**
- **Actualizare automată după conectare utilizator**
- **Verificare fișiere cu pornire automată după conectare utilizator**
- **Verificare fișiere cu pornire automată după actualizare cu succes a bazei de semnături**

Pentru a edita configurația unei sarcini planificate existente (atât implicită, cât și definită de utilizator), faceți-clic dreapta pe sarcină și apoi clic pe **Editare...** sau selectați sarcina pe care doriți să o modificați și faceți clic pe butonul **Editare...**.

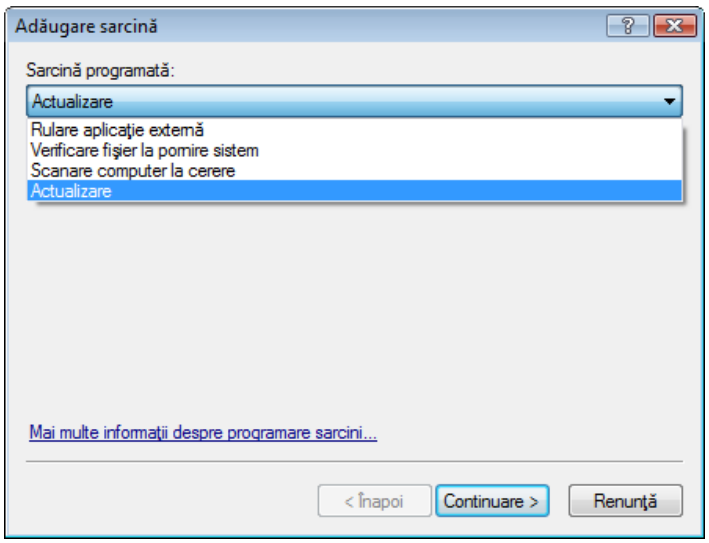
4.3.1 Scopul sarcinilor planificate

Planificatorul gestionează și lansează sarcini planificate cu configurații și proprietăți predefinite. Configurația și proprietățile conțin informații precum data și ora, precum și profile specificate pentru folosire în timpul executării sarcinii.

4.3.2 Crearea de sarcini noi

Pentru a crea o sarcină nouă în Planificator, faceți clic pe butonul **Adăugare...** sau faceți clic dreapta și selectați **Adăugare...** din meniul contextual. Sunt disponibile cinci tipuri de sarcini planificate:

- **Rulare aplicație externă**
- **Mentenanță fișiere log**
- **Verificare fișier la pornire sistem**
- **Scanare computer la cerere**
- **Actualizare**



Deoarece **Scanare computer la cerere** și **Actualizare** sunt sarcinile planificate utilizate cel mai frecvent, vom explica modul de adăugare a unei sarcini de actualizare noi.

În meniul vertical **Sarcină programată:** -selectați **Actualizare**. Faceți clic pe **Următorul** și introduceți numele sarcinii în câmpul **Nume sarcină:**. Selectați frecvența de efectuare a sarcinii. Sunt disponibile următoarele opțiuni: **O dată, Repetat, Zilnic**, **Săptămânal** și **Declanșat de eveniment**. În funcție de frecvența selectată, vi se vor solicita diverși parametri de actualizare. În continuare definiți acțiunea de efectuat în cazul în care sarcina nu poate fi efectuată sau finalizată la ora planificată. Sunt disponibile următoarele trei opțiuni:

- Așteaptă până la următoarea oră programată
- Execută sarcina cât de curând posibil
- Execută sarcina imediat dacă intervalul scurs de la ultima execuție a sarcinii depășește intervalul specificat (intervalul poate fi definit imediat utilizând caseta de defilare Interval sarcină)

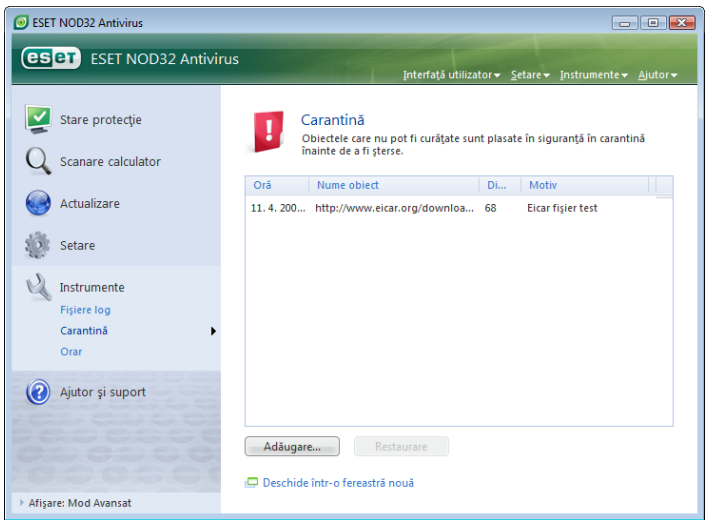
În pasul următor este afișată o fereastră cu un rezumat al informațiilor despre sarcina planificată curent; opțiunea Executare sarcină cu parametri specifici trebuie activată automat. Faceți clic pe butonul Terminare.

Va apărea o fereastră de dialog care vă permite să alegeți profile de utilizat pentru sarcina planificată. Aici puteți specifica un profil principal și unul profil alternativ; acesta din urmă se folosește în cazul în care sarcina nu poate fi finalizată folosind profilul principal. Confirmați făcând clic pe OK în fereastra Actualizare profile. Sarcina planificată nouă va fi adăugată la lista de sarcini planificate curente.

4.4 Carantina

Sarcina principală a carantinei este stocarea în siguranță a fișierelor infectate. Fișierele trebuie plasate în carantină dacă nu pot fi curățate, dacă ștergerea acestora nu prezintă siguranță sau nu este recomandată sau dacă acestea sunt detectate în mod fals de ESET Smart Security.

Utilizatorul poate alege să plaseze în carantină orice fișier dorește. Acest lucru se recomandă în cazul în care un fișier se comportă suspect, dar nu este detectat de scanner-ul antivirus. Fișierele plasate în carantină pot fi trimise pentru analiză către laboratoarele ESET de viruși.



Fișierele stocate în directorul carantinei pot fi vizualizate într-un tabel care afișează data și ora plasării în carantină, calea către locația inițială a fișierului infectat, dimensiunea acestora exprimată în octeți, motivul (**adăugat de utilizatorul...**) și numărul de amenințări (de exemplu dacă există o arhivă care conține mai multe infiltrări).

4.4.1 Plasarea fișierelor în carantină

Programul plasează automat în carantină fișiere șterse (dacă nu ați revocat această opțiune în fereastra de alertă). Dacă doriți, puteți plasa manual în carantină orice fișier suspect făcând clic pe butonul **Adăugare...**. În acest caz, fișierul inițial nu este eliminat din locația sa inițială. Meniul contextual poate fi folosit, de asemenea, în acest scop – faceți-clic dreapta în fereastra carantinei și selectați opțiunea **Adăugare...**.

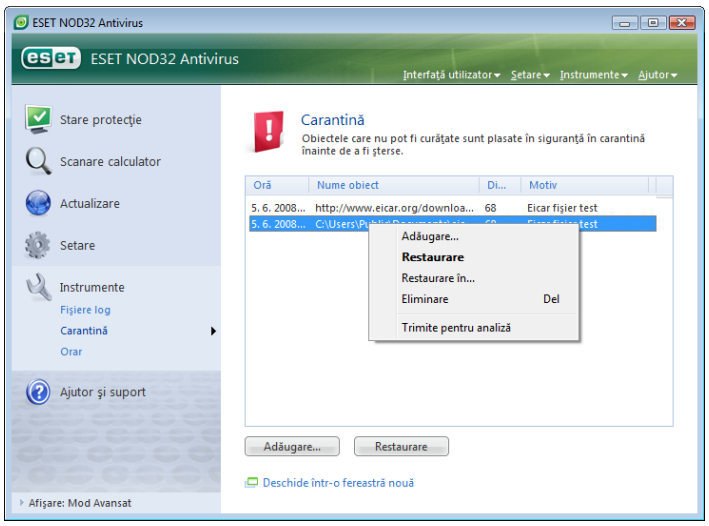
4.4.2 Restaurarea din carantină

Fișierele aflate în carantină pot fi ulterior restaurate în locația de origine. Folosiți caracteristica **Restaurare**; aceasta este disponibilă din meniul contextual făcând-clic dreapta pe fișierul dat în fereastra carantinei. De asemenea, meniul contextual oferă opțiunea **Restaurare în**, care vă permite să restaurați fișiere într-o altă locație decât cea din care au fost șterse.

NOTĂ:
Dacă programul a plasat din greșeală în carantină un fișier nepericulos, excludeți fișierul respectiv din procesul de scanare după restaurarea și trimiterea acestuia către Serviciul pentru clienți ESET.

4.4.3 Trimiterea unui fișier din carantină

Dacă ați plasat în carantină un fișier suspect care nu au fost detectate de program sau dacă un fișier a fost evaluat ca infectat în mod incorect (de exemplu prin analiza euristică a codului) și ulterior a fostplasat în carantină, trimiteți fișierul la laboratorul ESET de viruși. Pentru a trimite un fișier din carantină, faceți clic dreapta pe acesta și selectați **Trimitere spre analiză** din meniul contextual.



4.5 Fișierele log

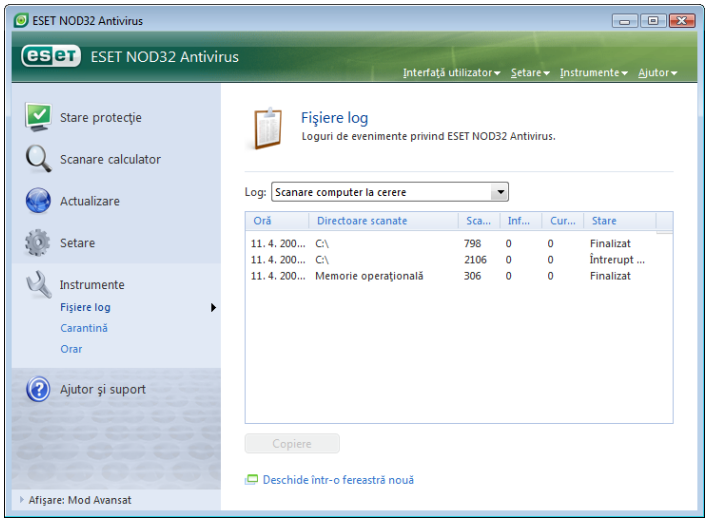
Fișierele log conțin informații despre toate evenimentele importante de program ce au avut loc și oferă o prezentare a amenințărilor detectate. Scrierea în log reprezintă un instrument esențial pentru analiza sistemului, detectarea amenințărilor și depanare. Scrierea în log se efectuează activ în fundal, fără interacțiunea utilizatorului. Informațiile sunt înregistrate în funcție de setările actuale privind detaliile de log. Este posibilă vizualizarea mesajelor text și a logurilor direct din mediul ESET NOD32 Antivirus, dar și în loguri arhivă.

Fișierele log sunt accesibile în fereastra principală a ESET NOD32 Antivirus, după ce faceți clic pe **Instrumente > Fișiere log**. Selectați tipul dorit de log utilizând meniul vertical **Log:** din partea de sus a ferestrei. Sunt disponibile următoarele loguri:

1. **Amenințări detectate –** Utilizați această opțiune pentru a vizualiza toate informațiile despre evenimente legate de detectarea infiltrărilor.

2. **Evenimente –** Această opțiune este concepută pentru administratori de sistem și utilizatori pentru a rezolva probleme. Toate acțiunile importante efectuate de ESET NOD32 Antivirus sunt înregistrate în logurile de evenimente.

3. **Scanare-computer la cerere –** în această fereastră sunt afișate rezultatele tuturor scanărilor finalizate. Faceți dublu-clic pe orice înregistrare pentru a vizualiza detaliidespre scanarea la cerere respectivă.

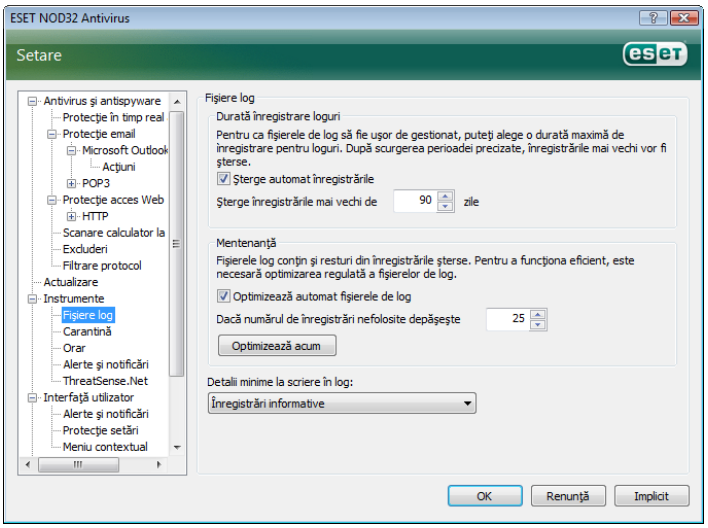


În fiecare secțiune, informațiile afișate pot fi copiate direct în clipboard selectând înregistrarea și făcând clic pe butonul **Copiere**. Pentru a selecta înregistrări multiple, folosiți tastele CTRL și SHIFT.

4.5.1 Mentenanța fișierelor log

Configurarea scrierii în log a ESET NOD32 Antivirus poate fi accesată din fereastra principală a programului. Faceți clic pe **Setare > Intrare în tot arborele de setare avansată... > Instrumente > Fișiere log**. Puteți specifica următoarele opțiuni pentru fișiere log:

- **Șterge automat înregistrările:** înregistrările din log mai vechi decât numărul de zile specificat se șterg automat
- **Optimizează automat fișierele de log:** activează defragmentarea automată a fișierelor log dacă se depășește procentajul de înregistrări nefolosite specificat
- **Detalii minime la scriere în log:** specifică nivelul de detaliere la scrierea în log. Opțiuni disponibile:
  - **Erori critice –** se scriu în log numai erorile critice (erori la pornirea protecției antivirus, a protecției firewall etc.)
  - **Erori –** se înregistrează numai mesaje „Eroare la descărcarea fișierului" plus erori critice
  - **Avertismente –** se înregistrează erori critice și mesaje de eroare și de avertisment
  - **Înregistrări de informare –** se înregistrează mesaje de informare, inclusiv mesaje de actualizare cu succes, plus toate înregistrările de mai sus
  - **Înregistrări de diagnosticare –** se scriu în log informații necesare pentru setarea amănunțită a programului și înregistrările de mai sus



4.6 Interfața pentru utilizator

Opțiunile de configurare a interfeței pentru utilizator din ESET NOD32 Antivirus pot fi modificate astfel încât să puteți adapta mediul de lucru la nevoile personale. Aceste opțiuni de configurare pot fi accesate din ramificația **Interfață utilizator** a arborelui Setare avansată ESET NOD32 Antivirus.

Secțiunea **Elemente interfață utilizator** permite utilizatorilor să comute, dacă doresc, la modul Avansat. Modul Avansat afișează setări mai detaliate și controale suplimentare din ESET Smart Security.

Opțiunea **Interfață grafică utilizator** trebuie dezactivată în cazul în care elementele grafice diminuează performanța computerului sau cauzează alte probleme. De asemenea, interfața grafică poate fi dezactivată pentru utilizatorii cu probleme de vedere, deoarece este posibil ca aceasta să intre în conflict cu aplicații speciale folosite pentru citirea textului afișat pe ecran.

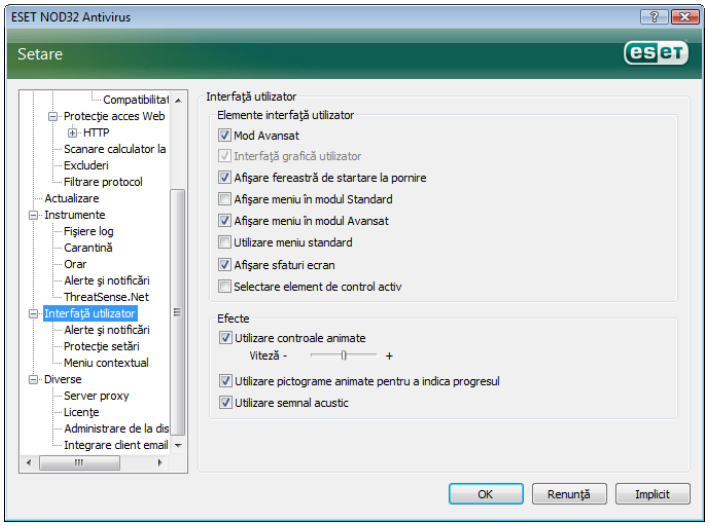
Dacă doriți să dezactivați fereastra de startare ESET NOD32 Antivirus, dezactivați opțiunea **Afișare fereastră de startare la pornire**.

În partea de sus a ferestrei principale a programului ESET NOD32 Antivirus există un meniu standard care poate fi activat sau dezactivat în funcție de opțiunea **Utilizare meniu standard**.

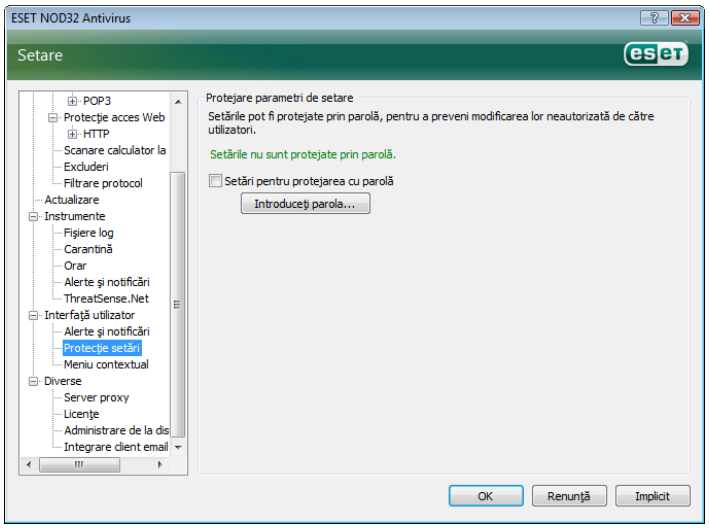
Dacă opțiunea **Afișare sfaturi ecran** este activată, se va afișa scurtă descriere a oricărei opțiuni dacă se va deplasa cursorul pe aceasta. Opțiunea **Selectare element de control activ** va determina evidențierea de către sistem a oricărui element care se află curent sub zona activă a cursorului mouse-ului. Elementul evidențiat va fi activat după un clic de mouse.

Pentru a scădea sau a crește viteza efectelor animate, selectați opțiunea **Utilizare controale animate** și deplasați bara de glisare **Viteză** spre stânga sau spre dreapta.

Pentru a activa utilizarea de pictograme animate pentru afișarea progresului diverselor operații, bifați caseta de selectare **Utilizare pictograme animate...**. Dacă doriți ca programul să emită un sunet dacă are loc un eveniment important, selectați opțiunea **Utilizare semnal acustic**.



Caracteristicile **interfeței pentru utilizator** includ, de asemenea, opțiunea de protejare prin parolă a parametrilor de setare ai programului ESET NOD32 Antivirus. Această opțiune este amplasată în submeniul **Protecție setări** din **interfața pentru utilizator**. Pentru a oferi securitate maximă sistemului dvs., este esențial ca programul să fie configurat corect. Modificările neautorizate pot cauza pierderea de date importante. Pentru a seta o parolă pentru protejarea parametrilor de setare, faceți clic pe **Introduceți parola...**



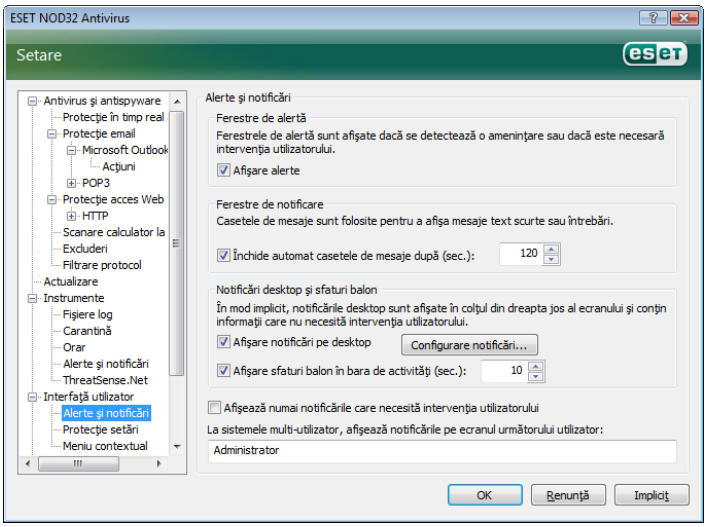
4.6.1 Alerte și notificări

Secțiunea **Setare alerte și notificări** din **interfața pentru utilizator** avă permite să configurați modul de tratare a mesajelor de alertă și a notificărilor de sistem în ESET Smart Security.

Primul element este **Afișare alerte**. Dezactivarea acestei opțiuni va revoca toate ferestrele de alertă; această acțiune este adecvată numai pentru un număr limitat de situații specifice. Pentru majoritatea utilizatorilor, recomandăm păstrarea opțiunii implicite (Activat).

Pentru a închide automat ferestre popup după o anumită perioadă de timp, selectați opțiunea **Închide automat casetele de mesaje după (sec.)**. Dacă nu sunt închise manual de către utilizator, ferestrele de alertă sunt închise automat după expirarea perioadei de timp specificate.

Notificările de pe desktop și sfaturile balon au rol exclusiv informativ și nu necesită sau oferă interacțiune cu utilizatorul. Acestea sunt afișate în zona de notificare din partea din dreapta-jos a ecranului. Pentru a activa afișarea notificărilor pe desktop, selectați opțiunea **Afișare notificări pe desktop**. Opțiuni mai detaliate – durata de afișare a notificărilor și transparența ferestrelor pot fi modificate făcând clic pe butonul **Configurare notificări...**. Pentru a previzualiza comportamentul notificărilor, faceți clic pe butonul **Previzualizare**. Pentru a configura durata de afișare a sfaturilor balon, accesați opțiunea **Afișare sfaturi balon în bara de activități (sec.)**.



În secțiunea de jos a ferestrei de setare **Alerte și notificări** există opțiunea **Afișează numai notificările care necesită intervenția utilizatorului**. Această opțiune vă permite să activați/dezactivați afișarea alertelor și a notificărilor care nu necesită intervenția utilizatorului. Cea din urmă caracteristică a acestei secțiuni este specificarea de adrese de notificări într-un mediu multi-utilizator.

Câmpul **La sistemele multi-utilizator, afișează notificările pe ecranul utilizatorului**: permite utilizatorului să definească numele persoanelor care vor primi notificări importante de la ESET Smart Security. În mod normal, acestea trebuie să fie administrator de sistem sau de rețea. Această opțiune este utilă în special pentru servere terminale, cu condiția ca toate notificările de sistem să fie trimise administratorului.

4.7 ThreatSense.Net

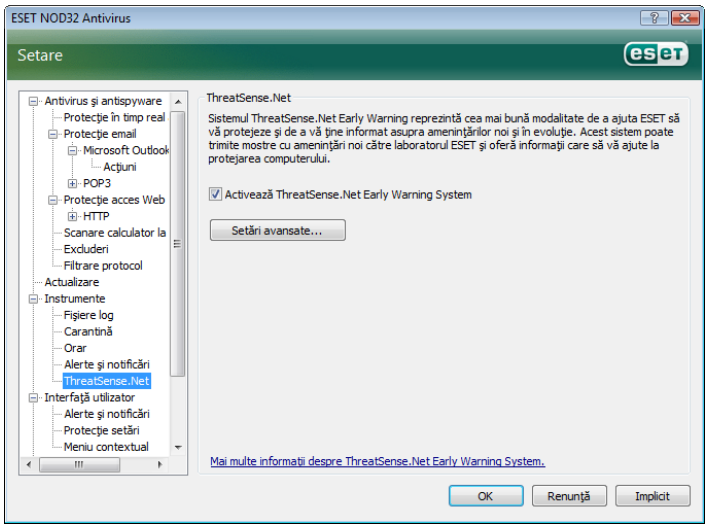
ThreatSense.Net Early Warning System este un instrument care informează imediat și în permanență compania ESET despre infiltrări noi. Instrumentul bidirecțional ThreatSense.Net Early Warning System are un singur scop – să îmbunătățească protecția pe care v-o putem oferi. Modul optim de a ne asigura că descoperim amenințări noi imediat ce apar este de a ne „conecta" la cât mai mulți clienți posibil și de a-i folosi ca pe „pionieri" în descoperirea amenințărilor. Există două opțiuni:

- Puteți decide să nu activați ThreatSense.Net Early Warning System. Nu veți pierde nicio funcționalitate din software și veți dispune în continuare de cea mai bună protecție pe care v-o putem oferi.
- Puteți configura Early Warning System pentru a trimite informații anonime despre amenințări noi și despre locația codului acestora într-un singur fișier. Fișierul poate fi trimis la ESET pentru analiză detaliată. Studierea acestor amenințări va ajuta ESET să își actualizeze propriile capacități de detectare. ThreatSense.Net Early Warning System va colecta informații despre calculatorul dvs. corelate cu amenințările nou detectate. Este posibil ca aceste informații să includă un eșantion sau o copie a fișierului în care apare amenințarea, calea către fișierul respectiv, numele fișierului, informații despre dată și oră, procesul cu ajutorul căruia amenințarea a apărut pe calculatorul dvs. și informații despre sistemul de operare al calculatorului. Este posibil ca unele dintre aceste informații să includă informații personale despre utilizatorul calculatorului, precum numele de utilizator dintr-o cale de director etc. Un exemplu de informații despre un fișier trimise este disponibil aici.

Deoarece există șansa ca în acest mod să se divulge ocazional unele informații despre dvs. și calculatorul dvs. laboratorului nostru de amenințări de la ESET, aceste informații nu vor fi folosite în NICIUN alt scop decât cel de a răspunde imediat la amenințări noi.

În mod implicit, ESET NOD32 Antivirus se configurează astfel încât să solicite acordul înainte de trimiterea fișierelor suspecte pentru analiză detaliată către laboratorul ESET de amenințări. Trebuie reținut faptul că fișierele cu anumite extensii, precum .doc sau .xls, sunt excluse întotdeauna din procesul de trimitere, chiar dacă este posibil ca în acestea să fie detectate amenințări. De asemenea, puteți adăuga alte extensii în cazul în care există anumite fișiere pe care dvs. sau compania dvs. dorește să evite să le trimită.

Setarea ThreatSense.Net este accesibilă din arborele de setare avansată, în **Instrumente > ThreatSense.Net**. Bifați caseta de selectare **Activează ThreatSense.Net Early Warning System**. Acest lucru vă va permite să activați instrumentul; apoi faceți clic pe butonul **Setare avansată...**.

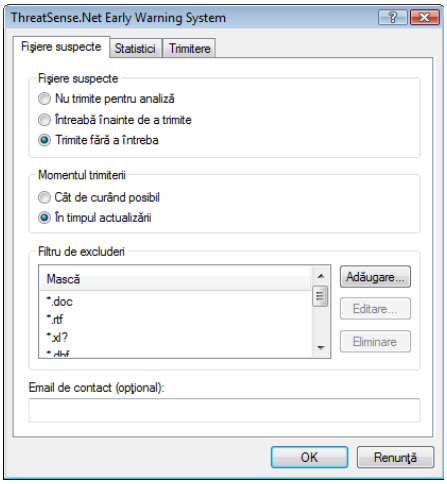


4.7.1 Fișierele suspecte

Fila **Fișiere suspecte** vă permite să configurați modul în care amenințările sunt trimise la laboratorul ESET pentru analiză.

Dacă găsiți un fișier suspect, îl puteți trimite pentru analiză la laboratoarele noastre de viruși. Dacă se dovedește că acesta este o aplicație malware, detectarea lui va fi adăugată la următoarea actualizare a semnăturilor.

Trimiterea de fișiere poate fi setată să fie efectuată automat, fără solicitare. Dacă această opțiune este selectată, fișierele suspecte sunt trimise în fundal. Dacă doriți să știți ce fișiere au fost trimise pentru analiză și să confirmați trimiterea, selectați opțiunea **Întreabă înainte de a trimite**.



Dacă nu doriți să fie trimis niciun fișier, selectați **Nu trimite pentru analiză**. Rețineți că netrimiterea fișierelor pentru analiză nu afectează trimiterea de informații statistice către ESET. Informațiile statistice sunt configurate în secțiunea de setare aferentă acestora, descrisă în capitolul următor.

Momentul trimiterii
Fișierele suspecte vor fi trimise către laboratoarele ESET pentru analiză cât mai curând posibil. Această acțiune este recomandată dacă este disponibilă o conexiune Internet permanentă; în această situație fișierele suspecte pot fi trimise fără întârziere. Cealaltă opțiune este trimiterea fișierelor suspecte **în timpul actualizării**. Dacă această opțiune este selectată, fișierele suspecte vor fi colectate și încărcate în serverele Early Warning System în timpul unei actualizări.

Filtrul de excluderi
Nu toate fișierele trebuie trimise pentru analiză. Filtrul de excluderi vă permite să excludeți anumite fișiere/directoare din procesul de trimitere. De exemplu, poate fi utilă excluderea fișierelor care pot cuprinde informații potențial confidențiale, precum documente sau foi de calcul. Cele mai obișnuite tipuri de fișiere sunt excluse în mod implicit (Microsoft Office, OpenOffice). Dacă doriți, puteți extinde lista de fișiere excluse.

Email-ul de contact
Email-ul de contact este trimis la ESET împreună cu fișierele suspecte și poate fi utilizat pentru a vă contacta, dacă pentru analiză sunt necesare informații suplimentare despre fișierele trimise. Rețineți că veți primi un răspuns de la ESET numai dacă sunt necesare informații suplimentare.

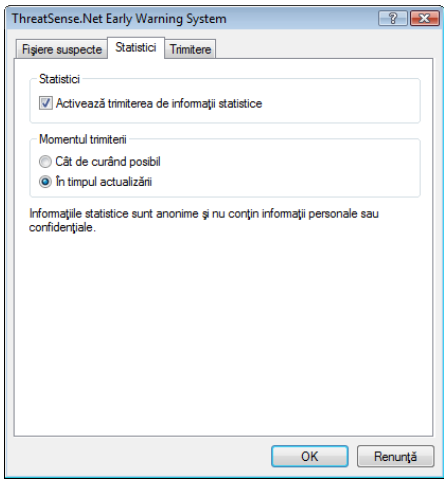
4.7.2 Statisticile

ThreatSense.Net Early Warning System colectează informații anonime despre computerul dvs. corelate cu amenințările recent detectate. Aceste informații pot include numele infiltrării, data și ora la care aceasta a fost detectată, versiunea de ESET NOD32 Antivirus, versiunea sistemului de operare al calculatorului dvs. și setările regionale. În mod normal, statisticile sunt trimise către serverele ESET o dată sau de două ori pe zi.

Un exemplu de pachet statistic trimis:

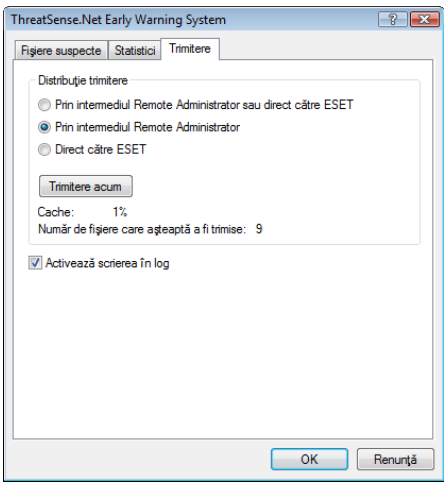
```
# utc_time=2005-0414 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\
Local Settings\Temporary Internet Files\Content.IE5\
C14J8NS7\rdgFR1463[1].exe
```

Momentul trimiterii
În secțiunea **Momentul trimiterii** puteți defini momentul în care vor fi trimise informațiile statistice. Dacă alegeți să trimiteți **Cât de curând posibil**, informațiile statistice vor fi trimise imediat după creare. Această setare este adecvată situației în care este disponibilă o conexiune Internet permanentă. Dacă se selectează **În timpul actualizării**, informațiile statistice vor fi păstrate și trimise împreună în timpul următoarei actualizări.



4.7.3 Trimiterea

În secțiunea Trimitere puteți alege mijloacele de trimitere a informațiilor statistice: prin Administrare la distanță ESET Remote Administrator sau direct la ESET. Dacă doriți să fiți sigur că fișierele suspecte și informațiile statistice sunt trimise la ESET, selectați opțiunea **Prin intermediul Administrare la distanță sau direct către ESET**. Dacă această opțiune este selectată, fișierele și statisticile sunt trimise prin toate mijloacele disponibile. Trimiterea fișierelor suspecte prin Administrare la distanță presupune trimiterea fișierelor și statisticilor către serverul de administrare la distanță, care ca asigura trimiterea ulterioară a acestora către laboratoarele ESET de viruși. Dacă este selectată opțiunea **Direct la ESET** toate fișierele suspecte și informațiile statistice sunt trimise la laboratorul ESET de viruși direct din program.



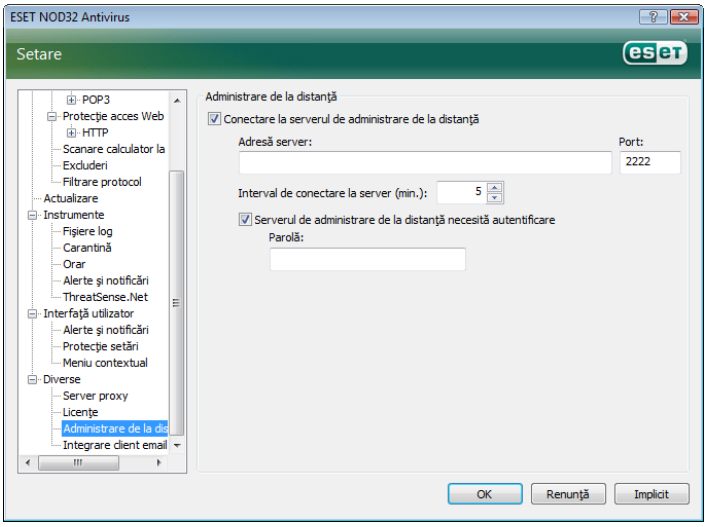
În cazul în care există fișiere care așteaptă să fie trimise, butonul **Trimitere acum** este activat în această fereastră de setare. Faceți clic pe acest buton dacă doriți să trimiteți imediat și informațiile statistice.

Bifați caseta de selectare **Activare înregistrare în jurnal** pentru a activa înregistrarea trimiterii de fișiere și informații statistice. După fiecare trimitere a unui fișier suspect sau a unei informații statistice, se creează o înregistrare în logul de evenimente.

4.8 Administrarea la distanță

Administrarea la distanță este un instrument eficient pentru întreținerea politicii de siguranță și pentru obținerea unei prezentări generale a gestionării securității în cadrul rețelei. Aceasta este utilă în special când este aplicată la rețele mai mari. Pe lângă faptul că administrarea la distanță sporește nivelul securității, aceasta facilitează folosirea administrării ESET NOD32 Antivirus pe stațiile de lucru client.

Opțiunile de setare pentru administrarea la distanță sunt disponibile în fereastra principală a programului ESET NOD32 Antivirus. Faceți clic pe **Setare > Intrare în tot arborele de setare avansată... > Diverse > Administrare la distanță**.



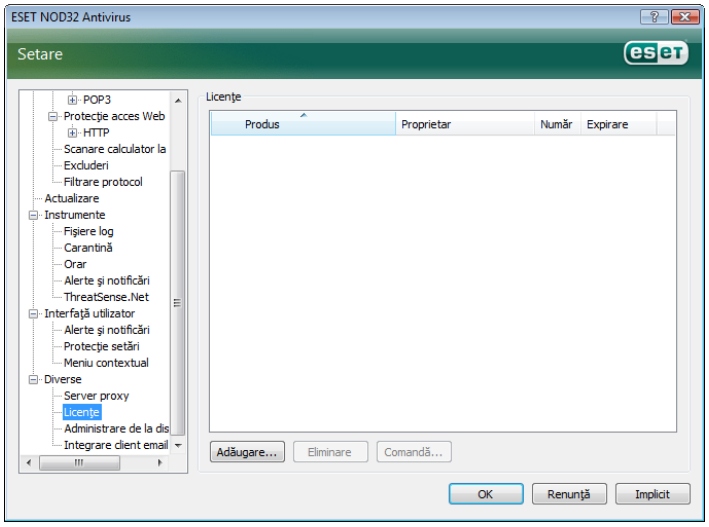
Fereastra Setare oferă activarea modului Administrare la distanță, care poate fi realizată selectând în prealabil caseta de selectare **Conectare la serverul de administrare la distanță**. Apoi puteți accesa celelalte opțiuni descrise mai jos:

- **Adresă server** – adresa de rețea a serverului pe care este instalată aplicația de server de administrare la distanță.
- **Port** – acest câmp conține un port de server predefinit utilizat pentru conexiune. Vă recomandăm să lăsați setarea de port predefinită, și anume 2222.
- **Interval între conexiuni la server (min.)** – Aceasta indică frecvența cu care ESET NOD32 Antivirus se va conecta la serverul ERA pentru a trimite datele. Cu alte cuvinte, informațiile sunt trimise la intervale de timp definite aici. Dacă aceasta este setată la 0, informațiile vor fi trimise la fiecare 5 secunde.
- **Administrare la distanță necesită autentificare** – Vă permite să introduceți o parolă pentru conectarea la serverul de administrare la distanță, dacă este necesar.

Faceți clic pe **OK** pentru a confirma modificările și pentru a aplica setările. ESET NOD32 Antivirus va utiliza aceste setări pentru a se conecta la serverul la distanță.

4.9 Licența

Ramificația **Licență** vă permite să gestionați cheile de licență pentru ESET NOD32 Antivirus și alte produse ESET. După achiziționare, cheile de licență sunt livrate împreună cu numele dvs. de utilizator și parola. Pentru a **adăuga/elimina** o cheie de licență, faceți clic pe butonul corespunzător din fereastra Manager de licențe. Managerul de licențe poate fi accesat din arborele Setare avansată, sub **Diverse > Licențe.**



Cheia de licență este un fișier text care conține informații despre produsul achiziționat: proprietarul acestuia, numărul de licențe și data expirării.

Fereastra Manager de licențe permite utilizatorului să încarce și să vizualizeze conținutul unei chei de licență folosind butonul **Adăugare**... – informațiile conținute sunt afișat în manager. Pentru a șterge fișiere de licență din listă, faceți clic pe **Eliminare**.

Dacă o cheie de licență a expirat și sunteți interesat să achiziționați o reînnoire, faceți clic pe butonul **Comandă...** – veți fi redirecționat către magazinul nostru online.

5. Utilizatorii avansați

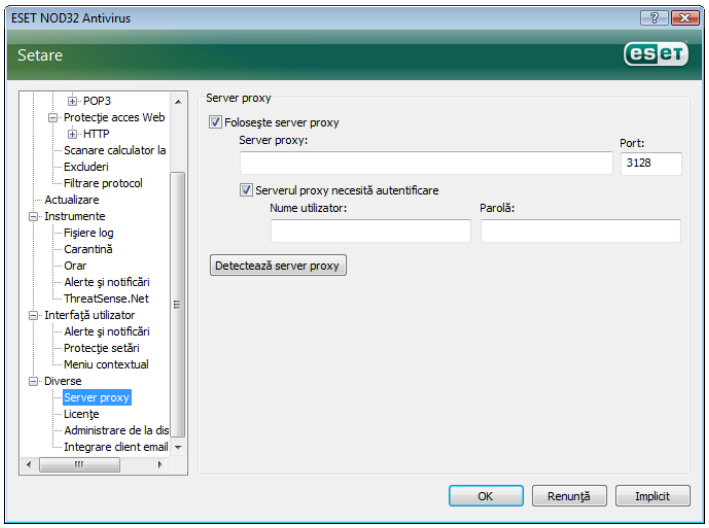
Acest capitol descrie caracteristicile ESET NOD32 Antivirus care se pot dovedi utile utilizatorilor mai avansați. Opțiunile de setare pentru aceste caracteristici pot fi accesate numai în modul Avansat. Pentru a comuta la modul Avansat, faceți clic pe **Comutare în modul Avansat** din colțul din stânga-jos al ferestrei principale a programului sau apăsați combinația de taste CTRL + M.

5.1 Setarea serverului proxy

În ESET Smart Security, setarea serverului proxy este disponibilă în două secțiuni diferite din structura arborelui Setare avansată.

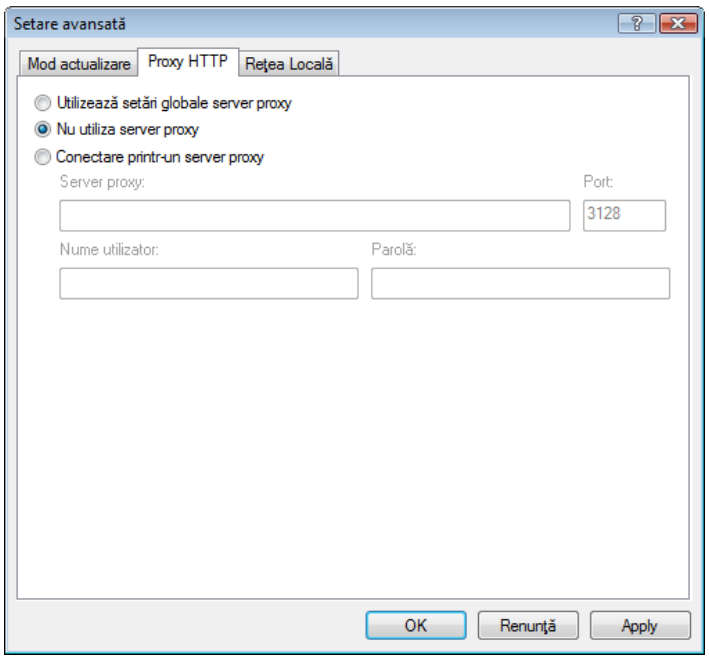
În primul rând, setările pentru serverul proxy pot fi configurate în **Diverse > Server proxy**. Specificând serverul proxy la acest nivel, definiți setările globale ale serverului proxy pentru toate componentele ESET Smart Security. Acești parametri vor fi utilizați de toate modulele care necesită conectare la Internet.

Pentru a specifica setările serverului proxy pentru acest nivel, bifați caseta de selectare **Utilizează server proxy** și apoi introduceți adresa serverului proxy în câmpul **Server proxy:** și numărul **portului** serverului proxy.



În cazul în care comunicarea cu serverul proxy necesită autentificare, bifați caseta de selectare **Serverul proxy necesită autentificare** și introduceți un **nume de utilizator** și o **parolă** valide în câmpurile respective. Faceți clic pe butonul **Detectează server proxy** pentru a detecta automat și introduce setările de server proxy. Parametrii specificați în Internet Explorer vor fi copiați. Rețineți că această caracteristică nu regăsește date de autentificare (nume de utilizator și parolă); acestea trebuie furnizate de către utilizator.

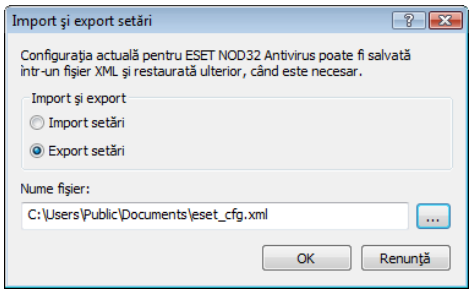
De asemenea, setările de server proxy pot fi stabilite în secțiunea **Setare actualizare avansată** (ramificația **Actualizare** a arborelui Setare avansată). Această setare se aplică pentru profilul de actualizare dat și este recomandat pentru laptopuri, deoarece acestea primesc adesea actualizări de semnături din diverse locații. Pentru mai multe informații despre această setare, consultați secțiunea 4.4, „Actualizarea sistemului".



5.2 Importul/exportul setărilor

Exportul și importul configurației curente a programului ESET NOD32 Antivirus sunt disponibile în meniul **Setare** din modul Avansat.

Exportul și importul utilizează tipul de fișier .xml. Exportul și importul sunt utile atunci când trebuie să efectuați backup pentru configurația curentă a programului ESET NOD32 Antivirus în vederea utilizării ulterioare (din diverse motive) a acestei configurații. De asemenea, opțiunea de export al setărilor va fi apreciată de persoanele care doresc să utilizeze configurațiile lor preferate pentru programul ESET NOD32 Antivirus pe mai multe sisteme – nu trebuie decât să importe propriul fișier .xml.



5.2.1 Exportul setărilor

Exportul configurației se efectuează foarte ușor. Dacă doriți să salvați configurația curentă a programului ESET Smart Security, faceți clic pe **Setare > Import și export setări...**. Selectați opțiunea **Export setări** și introduceți numele fișierului de configurare. Utilizați browser-ul pentru a selecta o locație de pe calculatorul dvs. unde doriți să salvați fișierul de configurare.

5.2.2 Importul setărilor

Pașii care trebuie urmați pentru importul setărilor sunt foarte similari. Din nou, selectați **Import și export setări** și apoi selectați opțiunea **Import setări**. Faceți clic pe butonul **...** și răsfoiți după fișierul de configurare pe care doriți să-l importați.

5.3 Linia 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").

Parametrii și butoanele următoare pot fi folosite la executarea scanner-ului la cerere din linia de comandă:

Opțiuni generale:

– help	afișare ajutor și părăsire
– version	afișare informații versiune și părăsire
– basedir = DIRECTOR	încărcare module din DIRECTOR
– quardir = DIRECTOR	DIRECTOR carantină
– aind	afișare indicator activitate
-- auto	scanează toate unitățile fixe în modul Curățare

Ținte:

– files	scanare fișiere (implicit)
– nofiles	nu se scanează fișiere
– boots	scanare sectoare de boot (implicit)
– noboots	nu se scanează sectoare de boot
– arch	scanare arhive (implicit)
– noarch	nu se scanează arhive
– maxarchivelevel = NIVEL	NIVEL maxim imbricare arhivă
– scantimeout = LIMITĂ	scanare arhivă cel mult LIMITĂ secunde. Dacă timpul de scanare atinge această limită, scanarea arhivei este oprită și scanarea va continua cu fișierul următor
– maxarchsize= DIMENSIUNE	scanează numai primii DIMENSIUNE bytes dinarhive (implicit 0 = nelimitat)
– mail	scanare fișiere email
– nomail	nu se scanează fișiere email
– sfx	scanare arhive SFX
– nosfx	nu se scanează arhive SFX
– rtp	scanare pachete de rutină
– nortp	nu se scanează pachete de rutină
– exclude = DIRECTOR	excludere DIRECTOR din proces de scanare
– subdir	scanare subdirectoare (implicit)
– nosubdir	nu se scanează subdirectoare
– maxsubdirlevel = NIVEL	NIVEL maxim de verificare in subdirector (implicit 0 = nelimitat)
– symlink	urmare legături simbolice (implicit)
– nosymlink	ignorare legături simbolice
– extremove = EXTENSII	
– extexclude = EXTENSII	excludere EXTENSIONS delimitate prin două puncte din procesul de scanare

Metode:

– adware	scanare pentru detectare adware/spyware/riskware
– noadware	nu se scanează pentru detectare adware/spyware/riskware
– unsafe	scanare pentru detectare aplicații potențial nesigure
– nounsafe	nu se scanează pentru detectare aplicații potențial nesigure
– unwanted	scanare pentru detectare aplicații potențial nedorite
– nounwanted	nu se scanează pentru detectare aplicații potențial nedorite
– pattern	folosire semnături
– nopattern	nu se folosesc semnături
– heur	activare euristică
– noheur	dezactivare euristică
– advheur	activare Euristică avansată
– noadvheur	dezactivare Euristică avansată

Curățare:

– action = ACȚIUNE	efectuare ACȚIUNE asupra obiectelor infectate. Acțiuni disponibile: none (niciuna), clean (curățare), prompt (atenționare)
– quarantine	copiere fișiere infectate în carantină (se adaugă la ACȚIUNE)
– noquarantine	nu se copiază fișiere infectate în Carantină

Loguri:

– log-file=FIȘIER	rezultat log în FIȘIER
– logrewrite	suprascriere fișier rezultat (valoarea implicită – adăugare)
– logall	scriere în log inclusiv fișiere curate
– nologall	nu se scriu în log fișiere curate (implicit)

Codurile de ieșire posibile ale scanării:

0 – nu a fost găsită nici o amenințare
1 – amenințare găsită, dar nu a fost curățată
10 – unele fișiere infectate nu au fost curățate
101 – eroare arhivă
102 – eroare accesare
103 – eroare internă

NOTĂ:
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.

6. Glosar

6.1 Tipuri de infiltrări

O infiltrare este un software dăunător care încearcă să pătrundă și/sau să deterioreze computerul unui utilizator.

6.1.1 Viruși

Un virus de computer este o infiltrare care corupe fișiere existente pe computerul dvs. Virușii sunt denumiți astfel după virușii biologici, deoarece ei folosesc tehnici asemănătoare pentru a se răspândi de la un computer la altul.

Virușii de computer atacă în special fișierele executabile și documentele. Pentru a se replica, un virus își atașează „corpul" la sfârșitul unui fișier țintă. Pe scurt, iată cum funcționează un virus de computer: după executarea fișierului infectat, virusul se activează (înaintea aplicației originale) și își execută sarcina predefinită. Numai după aceea este permisă execuția aplicației originale. Un virus nu poate infecta un computer decât dacă un utilizator (în mod accidental sau deliberat) execută sau deschide programul dăunător.

Virușii de computer pot varia în activitate și gravitate. Unii sunt extrem de periculoși, datorită capacității lor de a șterge în mod intenționat fișiere de pe un hard disk. Pe de altă parte, unii viruși nu provoacă nicio pagubă reală – ele servesc numai să îl enerveze pe utilizator și să demonstreze aptitudinile tehnice ale autorilor lor.

Este important să rețineți că virușii devin (în comparație cu troienii și cu programele spyware) tot mai mult o raritate, deoarece ei nu mai sunt atrăgători din punct de vedere comercial pentru autorii de software dăunător. De asemenea, termenul „virus" este adesea folosit incorect pentru a acoperi toate tipurile de infiltrări. În prezent, acesta este treptat înlocuit și este folosit termenul nou, mai corect, de „malware" (software dăunător).

În cazul în care computerul dvs. este infectat de un virus, este necesar să restaurați fișierele infectate la starea lor originală – de exemplu trebuie să le curățați folosind un program antivirus.

Exemple de viruși: OneHalf, Tenga și Yankee Doodle.

6.1.2 Viermi

Un vierme informatic este un program care conține cod dăunător ce atacă computerele gazdă și se răspândește într-o rețea. Diferența elementară între un virus și un vierme este aceea că viermii au capacitatea de a se replica și a călători singuri. Ele nu depinde de fișiere gazdă (sau de sectoare de boot).

Viermii proliferează prin intermediul mesajelor de email și pachetelor de rețea. Astfel, viermii pot fi împărțiți în două categorii:

- **Email** – se distribuie singuri la adresele de email găsite în lista de persoane de contact a unui utilizator și
- **Rețea** – exploatează vulnerabilitățile de securitate din diverse aplicații.

Prin urmare, viermii sunt mult mai viabili decât virușii de computer. Datorită disponibilității răspândite a Internetului, ei se pot răspândi pe tot globul în numai câteva ore de la lansare – în unele cazuri, chiar și în numai câteva minute. Această capacitate de a se replica în mod independent și rapid îi face mai periculoși decât celelalte tipuri de malware, cum ar fi virușii.

Un vierme activat într-un sistem poate determina o serie de neplăceri: poate șterge fișiere, poate reduce performanțele sistemului sau chiar poate dezactiva anumite programe. Natura viermilor de computer îi clasifică drept „mijloace de transport" pentru alte tipuri de infiltrări.

Dacă un vierme de computer v-a infectat computerul, vă recomandăm să ștergeți fișierele infectate, deoarece probabil ele conțin cod dăunător.

Exemple de viermi binecunoscuți: Lovsan/Blaster, Stration/Warezov, Bagle și Netsky.

6.1.3 Troieni

Din punct de vedere istoric, troienii de computer au fost definiți drept o clasă de infiltrări care încearcă să se prezinte drept programe utile, păcălindu-i astfel pe utilizatori să le permită executarea. Dar este important de reținut că acest lucru era valabil pentru troienii din trecut – în prezent nu mai este nevoie să se ascundă. Singurul lor scop este să se infiltreze cât mai ușor posibil și să își îndeplinească obiectivele dăunătoare. Termenul „troian" a devenit unul foarte general, el descriind orice infiltrare care nu se încadrează într-o anumită clasă de infiltrări.

Deoarece este o categorie foarte largă, ea este adesea împărțită în mai multe subcategorii. Cele mai bine cunoscute sunt:

- downloader – un program dăunător, care are capacitatea de a descărca alte infiltrări de pe Internet.
- dropper – un tip de troian conceput pentru a fixa alte tipuri de software dăunător pe computere compromise.
- backdoor – o aplicație care comunică cu atacatori la distanță, permițându-le să obțină acces la un sistem și să preia controlul asupra acestuia.
- keylogger – (program de înregistrare a apăsărilor de taste) – un program care înregistrează fiecare apăsare de tastă efectuată de un utilizator și trimite informațiile atacatorilor la distanță.
- program de apelare – programele de apelare sunt programe concepute pentru a se conecta la numere de telefon cu tarif special. Este aproape imposibil pentru un utilizator să observe că a fost creată o conexiune nouă. Programele de apelare pot provoca pagube numai utilizatorilor de modemuri pe linie comutată, care nu mai sunt utilizate cu regularitate.

Troienii iau de regulă forma unor fișiere executabile cu extensia .exe. Dacă pe computerul dvs. se detectează un fișier drept troian, este recomandat să-l ștergeți, deoarece foarte probabil acesta conține cod dăunător.

Exemple de troieni binecunoscuți: NetBus, Trojandownloader.Small.ZL, Slapper

6.1.4 Rootkit-uri

Rootkit-urile sunt programe dăunătoare care acordă atacatorilor de pe Internet acces nelimitat la un sistem, ascunzându-le în același timp prezența. Rootkit-urile, după ce accesează un sistem (de regulă exploatând o vulnerabilitate de sistem), folosesc funcții din sistemul de operare pentru a evita detectarea de către software antivirus: ele ascund procesele, fișierele și datele de regiștri Windows. Din acest motiv, este aproape imposibilă detectarea lor folosind tehnicile obișnuite de testare.

Atunci când vine vorba de prevenirea rootkit-urilor, rețineți că există două niveluri de detecție:

1. Atunci când acestea încearcă să acceseze un sistem. Ele încă nu sunt prezente, prin urmare sunt inactive. Majoritatea sistemelor antivirus pot elimina rootkit-urile la acest nivel (presupunând că ele detectează într-adevăr aceste fișiere ca fiind infectate).

2. Atunci când sunt ascunse de testarea normală. Utilizatorii sistemului antivirus ESET profită de avantajul tehnologiei AntiStealth care este de asemenea capabilă să detecteze și să elimine rootkit-urile active.

6.1.5 Adware

Adware este prescurtarea de la software ce este de bazează pe publicitate. În această categorie intră programele care afișează materiale publicitare. Adesea aplicațiile adware vor deschide automat întrun browser Internet o fereastră nouă pop-up ce conține reclame sau vor modifica pagina de pornire a browser-ului. Adesea aplicațiile adware sunt împachetate împreună cu programe freeware, permițând creatorilor acestora să acopere costurile de dezvoltare pentru aplicațiile lor (de obicei utile).

Aplicațiile adware în sine nu sunt periculoase – utilizatorii vor fi doar deranjați de reclame. Pericolul constă în faptul că aplicațiile adware pot executa și funcții de urmărire (precum procedează și aplicațiile spyware).

Dacă decideți să utilizați un produs freeware, acordați o atenție deosebită la instalarea programului. Cel mai probabil, programul de instalare vă va notifica despre instalarea unui program suplimentar adware. Cel mai adesea, vi se va permite să renunțați la acesta și să instalați programul fără adware. Pe de altă parte, unele programe nu se vor instala fără adware sau funcționalitatea lor va fi limitată. Acest lucru înseamnă că aplicația adware accesează adesea sistemul în mod „legal", deoarece utilizatorii și-au dat acceptul. În acest caz, este mai bine să fiți în siguranță decât să vă pară rău.

Dacă pe computerul dvs. există un fișier detectat ca adware, este recomandat să-l ștergeți, deoarece foarte probabil acesta conține cod dăunător.

6.1.6 Spyware

Această categorie acoperă toate aplicațiile care trimit informații private fără consimțământul/știința utilizatorului. Ele folosesc funcții de urmărire pentru a trimite diferite date statistice, cum ar fi o listă de site-uri Web vizitate, adrese email din lista de contacte a utilizatorului sau o listă de apăsări de taste introduse.

Autorii de spyware pretind că aceste tehnici sunt destinate să afle mai multe despre nevoile și interesele utilizatorilor și de a permite orientarea mai exactă a publicității. Problema este că nu există o diferență clară între aplicațiile folositoare și cele dăunătoare și nimeni nu poate fi sigur că informațiile recuperate nu vor fi utilizate incorect. Datele obținute de aplicațiile spyware pot conține coduri de securitate, coduri PIN, numere de conturi bancare etc. Aplicațiile spyware sunt adesea împachetate cu versiuni gratuite ale unui program de către autorul acestuia, pentru a genera venituri sau pentru a oferi o motivație pentru achiziționarea software-ului. Adesea utilizatorii sunt informați despre prezenta aplicației spyware în cursul instalării programului pentru a le oferi o motivație pentru a face un upgrade la o versiune plătită fără aplicația spyware respectivă.

Exemple de produse freeware bine cunoscute care sunt împachetate cu spyware sunt aplicațiile client pentru rețelele P2P (peer-to-peer). Spyfalcon sau Spy Sheriff (și multe alte aplicații) aparține unei subcategorii speciale de spyware – ele par a fi programe antispyware, dar de fapt sunt chiar ele programe spyware.

Dacă pe computerul dvs. există un fișier detectat ca spyware, este recomandat să-l ștergeți, deoarece foarte probabil acesta conține cod dăunător.

6.1.7 Aplicații potențial periculoase

Există multe programe legitime care servesc la simplificarea administrării computerelor legate în rețea. Cu toate acestea, în mâinile cui nu trebuie, ele pot fi folosite incorect pentru scopuri dăunătoare. De aceea ESET a creat această categorie specială. Clienții noștri au acum opțiunea de a alege dacă sistemul antivirus trebuie sau nu să detecteze aceste amenințări.

„Aplicațiile potențial periculoase" constituie clasificarea utilizată pentru software comercial legitim. Această clasificare cuprinde programe precum instrumente de acces la distanță, aplicații pentru spargerea parolelor și de înregistrare a tastelor (un program ce înregistrează fiecare tastă apăsată de un utilizator).

Dacă pe computerul dvs. există și se execută o aplicație potențial periculoasă (și nu ați instalat-o dvs.), consultați administratorul de rețea sau eliminați aplicația.

6.1.8 Aplicații potențial periculoase

Aplicațiile potențial nedorite nu sunt în mod obligatoriu menite să fie dăunătoare, dar ele pot afecta în sens negativ performanțele calculatorului. Aceste aplicații necesită, de obicei, permisiune pentru instalare. Dacă ele sunt prezente în calculator, sistemul se comportă diferit (comparativ cu starea anterioară instalării acestora). Modificările cele mai semnificative sunt:

- deschiderea de ferestre noi, pe care nu le-ați mai văzut
- activarea și rularea de procese ascunse
- creșterea utilizării resurselor de sistem
- modificări ale rezultatelor căutării
- aplicații care comunică cu servere la distanță